

ZyWALL/USG/ATP Series

ATP200/ ATP500/ ATP800

USG20-VPN / USG20W-VPN / USG40 / USG40W /
USG60 / USG60W / USG110 / USG210 / USG310/
USG1100 /USG1900 / USG2200-VPN

Security Firewalls

Firmware Version 4.35
Edition 3, 10/2019

Handbook

Default Login Details

| | |
|---------------------|---------------------|
| LAN Port IP Address | https://192.168.1.1 |
| User Name | admin |
| Password | 1234 |

Table of Content

| | |
|---|-----------|
| How to Configure Site-to-site IPSec VPN with Amazon VPC..... | 18 |
| Set Up the IPSec VPN Tunnel on the Amazon VPC..... | 19 |
| Set Up the IPSec VPN Tunnel on the ZyWALL/USG..... | 23 |
| Test the IPSec VPN Tunnel..... | 29 |
| What Could Go Wrong?..... | 30 |
| How to Configure Site-to-site IPSec VPN with Microsoft (MS) Azure | 31 |
| Set Up the IPSec VPN Tunnel on the ZyWALL/USG..... | 32 |
| Set Up the IPSec VPN Tunnel on the MS Azure | 37 |
| Test the IPSec VPN Tunnel..... | 44 |
| What Could Go Wrong? | 47 |
| How to Configure GRE over IPSec VPN Tunnel..... | 48 |
| Set Up the ZyWALL/USG GRE over IPSec VPN Tunnel of Corporate Network (HQ)..... | 49 |
| Set Up the ZyWALL/USG GRE over IPSec VPN Tunnel of Corporate Network (Branch) | 54 |
| Test the GRE over IPSec VPN Tunnel | 58 |
| What Could Go Wrong?..... | 59 |
| How to Configure Site-to-site IPSec VPN Where the Peer has a Static IP Address | 61 |
| Set Up the ZyWALL/USG IPSec VPN Tunnel of Corporate Network (Branch)..... | 66 |
| Test the IPSec VPN Tunnel..... | 70 |
| What Could Go Wrong? | 71 |
| How to Configure Site-to-site IPSec VPN Where the Peer has a Dynamic IP Address | 73 |
| Set Up the ZyWALL/USG IPSec VPN Tunnel of Corporate Network (HQ) | 73 |
| Set Up the ZyWALL/USG IPSec VPN Tunnel of Corporate Network (Branch has a Dynamic IP Address) | 77 |
| Test the IPSec VPN Tunnel..... | 81 |

| | |
|---|------------|
| What Could Go Wrong? | 83 |
| How to Configure IPSec Site to Site VPN while one Site is behind a NAT router | 85 |
| Set Up the ZyWALL/USG IPSec VPN Tunnel of Corporate Network (HQ) | 85 |
| Set Up the ZyWALL/USG IPSec VPN Tunnel of Corporate Network (Branch)..... | 89 |
| Set Up the NAT Router (Using ZyWALL USG device in this example) | 93 |
| Test the IPSec VPN Tunnel | 95 |
| What Could Go Wrong? | 96 |
| How to Configure Hub-and-Spoke IPSec VPN | 97 |
| Set Up the IPSec VPN Tunnel on the ZyWALL/USG by Using VPN Concentrator Hub_HQ-to-Branch_A | 98 |
| Hub_HQ-to-Branch_B | 102 |
| Hub_HQ Concentrator | 106 |
| Spoke_Branch_A | 107 |
| Spoke_Branch_B..... | 112 |
| Test the IPSec VPN Tunnel | 117 |
| What Could Go Wrong? | 121 |
| Set Up the IPSec VPN Tunnel of ZyWALL/USG without Using VPN Concentrator Hub_HQ-to-Branch_A | 123 |
| Hub_HQ-to-Branch_B | 126 |
| Spoke_Branch_A | 129 |
| Spoke_Branch_B..... | 132 |
| Test the IPSec VPN Tunnel | 135 |
| What Could Go Wrong? | 138 |
| How to Use Dual-WAN to Perform Fail-Over on VPN Using the VPN Concentrator | 140 |
| Set Up the IPSec VPN Tunnel on the ZyWALL/USG Hub_HQ-to-Branch_A..... | 141 |
| Hub_HQ-to-Branch_B | 144 |
| Hub_HQ Concentrator | 147 |
| Spoke_Branch_A | 148 |
| Spoke_Branch_B..... | 151 |

| | |
|---|------------|
| Test the IPsec VPN Tunnel..... | 155 |
| What Could Go Wrong? | 158 |
| How to Configure IPsec VPN with ZyWALL IPsec VPN Client | 159 |
| Set Up the ZyWALL/USG IPsec VPN Tunnel | 160 |
| Set Up the ZyWALL IPsec VPN Client | 164 |
| Test the IPsec VPN Tunnel | 167 |
| What Can Go Wrong? | 169 |
| How to Configure Site-to-site IPsec VPN with FortiGate..... | 171 |
| Set Up the IPsec VPN Tunnel on the ZyWALL/USG | 172 |
| Set Up the IPsec VPN Tunnel on the FortiGate..... | 175 |
| Test the IPsec VPN Tunnel | 180 |
| What Could Go Wrong? | 181 |
| How to Configure Site-to-site IPsec VPN with WatchGuard | 183 |
| Set Up the IPsec VPN Tunnel on the ZyWALL/USG | 184 |
| Set Up the IPsec VPN Tunnel on the WatchGuard | 187 |
| Test the IPsec VPN Tunnel | 193 |
| What Could Go Wrong? | 194 |
| How to Configure Site-to-site IPsec VPN with Cisco..... | 196 |
| Set Up the IPsec VPN Tunnel on the ZyWALL/USG | 197 |
| Set Up the IPsec VPN Tunnel on the Cisco | 202 |
| Test the IPsec VPN Tunnel | 207 |
| What Could Go Wrong? | 209 |
| How to Configure Site-to-site IPsec VPN with a SonicWALL router | 210 |
| Set Up the IPsec VPN Tunnel on the ZyWALL/USG | 211 |
| Set Up the IPsec VPN Tunnel on the SonicWALL | 218 |
| Test the IPsec VPN Tunnel | 222 |
| What Could Go Wrong? | 224 |
| How to Configure IPsec VPN Failover | 227 |
| Set Up the ZyWALL/USG IPsec VPN Tunnel of Corporate Network (HQ) | 228 |
| Set Up the ZyWALL/USG IPsec VPN Tunnel of Corporate Network (Branch)..... | 231 |
| Set up the WAN Trunk (ZyWALL/USG_HQ) | 236 |

| | |
|---|------------|
| Set up the Failover Command Line (ZyWALL/USG HQ) | 237 |
| Test the IPsec VPN Tunnel | 238 |
| What Could Go Wrong? | 240 |
| How to Configure L2TP over IPsec VPN while the ZyWALL/USG is behind a NAT router | 242 |
| Set Up the L2TP VPN Tunnel on the ZyWALL/USG_HQ | 243 |
| Set Up the NAT Router (Using ZyWALL USG device in this example) | 247 |
| Test the L2TP over IPsec VPN Tunnel | 250 |
| What Could Go Wrong? | 253 |
| How to Configure L2TP VPN with Android 5.0 Mobile Devices | 255 |
| Set Up the L2TP VPN Tunnel on the ZyWALL/USG | 256 |
| Set Up the L2TP VPN Tunnel on the Android Device | 260 |
| Test the L2TP over IPsec VPN Tunnel | 263 |
| What Could Go Wrong? | 265 |
| How to Configure L2TP VPN with iOS 8.4 Mobile Devices..... | 267 |
| Set Up the L2TP VPN Tunnel on the ZyWALL/USG | 267 |
| Set Up the L2TP VPN Tunnel on the iOS Device | 273 |
| Test the L2TP over IPsec VPN Tunnel | 274 |
| What Could Go Wrong? | 277 |
| How to Import ZyWALL/USG Certificate for L2TP over IPsec in Windows 10 | 279 |
| Set Up the L2TP VPN Tunnel on the ZyWALL/USG | 279 |
| Export a Certificate from ZyWALL/USG and Import it to Windows 10 Operating System | 284 |
| Set Up the L2TP VPN Tunnel on the Windows 10..... | 290 |
| Test the L2TP over IPsec VPN Tunnel | 294 |
| What Could Go Wrong? | 296 |
| How to Import ZyWALL/USG Certificate for L2TP over IPsec in IOS mobile phone..... | 298 |
| Set Up the L2TP VPN Tunnel on the ZyWALL/USG | 298 |
| Export a Certificate from ZyWALL/USG and Import it to iOS Mobile Phone | 303 |

| | |
|--|------------|
| Set Up the L2TP VPN Tunnel on the iOS Mobile Device | 303 |
| Test the L2TP over IPsec VPN Tunnel | 306 |
| What Could Go Wrong? | 308 |
| How to Configure 2 factor for VPN connection?..... | 309 |
| Set up the ZyWALL/USG IPsec VPN Tunnel..... | 310 |
| Set up the ZyWALL IPsec VPN Client | 315 |
| Set up notification for 2 factor authentication | 319 |
| Set up authentication for 2 factor VPN connection | 320 |
| Test the Result | 321 |
| What could went wrong | 324 |
| How to Import ZyWALL/USG Certificate for L2TP over IPsec in Android mobile phone | 324 |
| Set Up the L2TP VPN Tunnel on the ZyWALL/USG | 325 |
| Export a Certificate from ZyWALL/USG and Import it to Android Mobile Phone | 329 |
| Set Up the L2TP VPN Tunnel on the Android Mobile Device | 330 |
| Test the L2TP over IPsec VPN Tunnel | 334 |
| What Could Go Wrong? | 336 |
| How to Configure the L2TP VPN with Apple MAC OS X 10.11 Operating System | 338 |
| Set Up the L2TP VPN Tunnel on the ZyWALL/USG | 338 |
| Set Up the L2TP VPN Tunnel on the Apple MAC OS X 10.11 El Capitan Operating System | 343 |
| Test the L2TP over IPsec VPN Tunnel | 346 |
| What Could Go Wrong? | 348 |
| How to configure if I want user can only see SSL VPN Login button in web portal login page..... | 350 |
| Set Up the DNS Service | 351 |
| Set Up the ZyWALL/USG SSL VPN Setting | 351 |
| Set Up the ZyWALL/USG System Setting | 352 |
| Test the SSL VPN | 353 |
| How to Deploy SSL VPN with Apple Mac OS X 10.10 Operating System | 357 |

| | |
|--|------------|
| Set Up the SSL VPN Tunnel on the ZyWALL/USG | 358 |
| Set Up the SSL VPN Tunnel on the Apple MAC OS X 10.10 Operating System..... | 361 |
| Test the SSL VPN Tunnel..... | 365 |
| What Could Go Wrong? | 368 |
| How To Configure SSL VPN for Remote Access Mobile Devices | 370 |
| Set Up the SSL VPN Tunnel on the ZyWALL/USG | 371 |
| Test the SSL VPN Tunnel..... | 374 |
| What Could Go Wrong? | 376 |
| How to Configure an SSL VPN Tunnel (with SecuExtender version 4.0.0.1) on the Windows 10 Operating System | 377 |
| Set up the SSL VPN Tunnel with Windows 10 | 377 |
| What Can Go Wrong? | 381 |
| How to redirect multiple LAN interface traffic to the VPN tunnel | 383 |
| Set Up the ZyWALL/USG IPsec VPN Tunnel of Corporate Network (HQ) | 384 |
| Set Up the ZyWALL/USG IPsec VPN Tunnel of Corporate Network (Branch)..... | 387 |
| Set up the Policy Route (ZyWALL/USG_HQ) | 391 |
| Set up the Policy Route (ZyWALL/USG_Branch) | 392 |
| Test the IPsec VPN Tunnel | 394 |
| What Could Go Wrong? | 395 |
| How to Create VTI and Configure VPN Failover with VTI..... | 397 |
| VTI Deployment Flow | 397 |
| Set Up the ZyWALL/USG VTI of Corporate Network (HQ) | 398 |
| Set Up the ZyWALL/USG VTI of Corporate Network (Branch) | 403 |
| Test the IPsec VPN Tunnel | 409 |
| What Can Go Wrong? | 411 |
| How to configure the USG when using a Cloud Based SIP system | 413 |
| Set Up the SIP ALG..... | 414 |
| Test result | 414 |
| What could go wrong? | 415 |

| | |
|---|------------|
| How to block HTTPS websites by Domain Filter without applying SSL Inspection | 415 |
| Set Up the Content Filter on the ZyWALL/USG | 416 |
| Set Up the Security Policy on the ZyWALL/USG | 419 |
| Set Up the System Policy on the ZyWALL/USG | 419 |
| Test the Result | 419 |
| How to Configure Content Filter 2.0 with Geo IP Blocking | 422 |
| Set Up the Address Objet with Geo IP on the ZyWALL/USG | 423 |
| Set Up the Security Policy on the ZyWALL/USG | 423 |
| Test the Result | 424 |
| What Could Go Wrong? | 425 |
| How to Configure Content Filter 2.0 with HTTPs Domain Filter | 426 |
| Application Scenario | 426 |
| Set Up the Content Filter on the ZyWALL/USG | 427 |
| Set Up the Security Policy on the ZyWALL/USG | 429 |
| Set Up the System Policy on the ZyWALL/USG | 430 |
| Test the Result | 431 |
| What Could Wrong? | 431 |
| How to block the client accessing to certain country using Geo IP and Content Filter | 432 |
| Check Geo IP License Status on the ZyWALL/USG | 433 |
| Set Up the Address Objet with Geo IP on the ZyWALL/USG | 434 |
| Set Up the Security Policy on the ZyWALL/USG | 435 |
| Test the Result | 436 |
| How to Restrict Web Portal access from the Internet | 439 |
| Set Up the ZyWALL/USG System Setting | 439 |
| Test the Web Access | 440 |
| How to Setup and Configure Daily Report | 443 |
| Set Up the ZyWALL/USG Email Daily Report Setting | 444 |
| Test the Daily Log Report | 445 |
| What Could Go Wrong? | 447 |
| How to Setup and Configure Email Logs | 448 |

| | |
|--|------------|
| Set Up the ZyWALL/USG Email Logs Setting..... | 449 |
| Test the Email Log | 450 |
| What Could Go Wrong? | 451 |
| How to Setup and send logs to a Syslog Server..... | 452 |
| Set Up the Syslog Server (Use Papertrail syslog in this example) | 452 |
| Set Up the ZyWALL/USG Remote Server Setting | 455 |
| Test the Remote Server | 456 |
| What Could Go Wrong? | 457 |
| How to Setup and send logs to a Vantage Reports Server..... | 458 |
| Set Up the VRPT Server | 459 |
| Set Up the ZyWALL/USG Remote Server Setting | 462 |
| Test the Remote Server | 463 |
| What Could Go Wrong? | 463 |
| How to Setup and send logs to the USB storage | 464 |
| Set Up the USB System Settings | 465 |
| Set Up the USB Log Storage | 466 |
| Check the USG Log Files | 467 |
| How to Activate a Free Access Hotspot | 467 |
| Set up the Free Access Hotspot | 469 |
| Test the User Agreement and Advertisement Webpage | 470 |
| What could Go Wrong? | 472 |
| Set up Enable the Free Time Feature..... | 472 |
| Test Free Time Feature | 478 |
| What Can Go Wrong? | 481 |
| How to Setup IPv6 Interfaces for Pure IPv6 Routing | 483 |
| Setting Up the IPv6 Interface | 484 |
| Set up the Prefix Delegation and Router Advertisement | 486 |
| Test | 490 |
| What Can Go Wrong? | 491 |
| Test | 493 |
| How to Perform and Use the Packet Capture Feature on the ZyWALL/USG | 493 |
| Set Up the Packet Capture Feature..... | 494 |

| | |
|---|------------|
| Check the Capture Files..... | 497 |
| How to Automatically Reboot the ZyWALL/USG by Schedule..... | 498 |
| Set Up the Shell Script | 499 |
| Set Up the Schedule Run..... | 500 |
| Check the Reboot Status | 502 |
| How To Schedule YouTube Access..... | 504 |
| Set Up the Schedule on the ZyWALL/USG..... | 504 |
| Create the Application Objects on the ZyWALL/USG | 505 |
| Set Up SSL Inspection on the ZyWALL/USG | 505 |
| Set Up the Security Policy on the ZyWALL/USG..... | 506 |
| Export Certificate from ZyWALL/USG and Import it to Windows 7 Operation System | 507 |
| Test the Result | 513 |
| What Could Go Wrong? | 513 |
| How to continuously run a ZySH script..... | 515 |
| Set Up the Shell Script | 515 |
| Set Up the Schedule Run..... | 517 |
| Check the Result | 517 |
| How To Register Your Device and Services at myZyXEL.com | 518 |
| Account Creation | 519 |
| Device Registration..... | 521 |
| Service Registration (In the Case of Standard License) | 522 |
| Device Management (In the Case of Registering Bundled Licenses) | 523 |
| Refresh Service | 524 |
| What Could Go Wrong? | 524 |
| How To Exempt Specific Users From Security Control | 526 |
| Set Up the Security Policy on the ZyWALL/USG for Employees | 527 |
| Set Up the Security Policy on the ZyWALL/USG for Executives..... | 529 |
| Test the Result | 531 |
| What Could Go Wrong? | 532 |
| How To Detect and Prevent TCP Port Scanning with ADP | 533 |
| Set Up the ADP Profile on the ZyWALL/USG | 534 |

| | |
|---|------------|
| Test the Result | 537 |
| What Could Go Wrong? | 538 |
| How To Block Facebook | 539 |
| Set Up the Content Filter on the ZyWALL/USG | 540 |
| Set Up the SSL Inspection on the ZyWALL/USG | 540 |
| Set Up the Security Policy on the ZyWALL/USG | 542 |
| Export Certificate from ZyWALL/USG and Import it to Windows 7 Operation System | 543 |
| Test the Result | 548 |
| What Could Go Wrong? | 549 |
| How To Exempt Specific Users From a Blocked Website | 550 |
| Set Up the Security Policy on the ZyWALL/USG for Employees | 551 |
| Set Up the Security Policy on the ZyWALL/USG for Executives | 553 |
| Test the Result | 556 |
| What Could Go Wrong? | 557 |
| How To Control Access To Google Drive | 558 |
| Set Up the SSL Inspection on the ZyWALL/USG | 559 |
| Set Up the Security Policy on the ZyWALL/USG | 560 |
| Export Certificate from ZyWALL/USG and Import it to Windows 7 Operation System | 560 |
| Test the Result | 566 |
| What Could Go Wrong? | 567 |
| How To Block HTTPS Websites Using Content Filtering and SSL Inspection | 568 |
| Set Up the Content Filter on the ZyWALL/USG | 569 |
| Set Up SSL Inspection on the ZyWALL/USG | 570 |
| Set Up the Security Policy on the ZyWALL/USG | 572 |
| Export Certificate from ZyWALL/USG and Import it to Windows 7 Operation System | 573 |
| Test the Result | 578 |
| What Could Go Wrong? | 579 |
| How To Block the Spotify Music Streaming Service | 580 |
| Set Up IDP Profile on the ZyWALL/USG | 581 |

| | |
|---|------------|
| Test the Result | 582 |
| What Could Go Wrong? | 583 |
| How does Anti-Malware work | 584 |
| Enable Anti-Malware function to protecting your traffic | 585 |
| Test the result | 586 |
| Additional configuration | 586 |
| What can go wrong | 587 |
| How to Configure an Email Security Policy with Mail Scan and DNSBL | 588 |
| Set Up the Email Security on ATP Series | 588 |
| Test the result | 591 |
| What can go wrong | 592 |
| How to Configure Botnet Filter on ATP series? | 593 |
| Prerequisites before setting up Botnet Filter function | 594 |
| License activation..... | 594 |
| Update Botnet Filter Signatures | 594 |
| Set Up the IP Blocking on the ATP series | 596 |
| Test the Result | 596 |
| Set up the URL Blocking on the ATP series | 597 |
| Test the Result | 597 |
| How to Use Sandboxing to Detect Unknown Malware | 599 |
| Set Up Sandboxing on ATP | 600 |
| Test the Result | 602 |
| What Can Go Wrong? | 605 |
| How to Configure Bandwidth Management for FTP and HTTP Traffic .. | 606 |
| Set Up the Bandwidth Management for FTP on the ZyWALL/USG | 607 |
| Set Up the Bandwidth Management for HTTP on the ZyWALL/USG | 608 |
| Set Up the Bandwidth Management Global Setting on the ZyWALL/USG..... | 610 |
| Test the Result | 611 |
| What Could Go Wrong? | 612 |
| How to Limit BitTorrent or Other Peer-to-Peer Traffic | 613 |
| Set Up the Application Patrol Profile on the ZyWALL/USG | 614 |

| | |
|--|------------|
| Set Up the Bandwidth Management for BitTorrent on the ZyWALL/USG..... | 615 |
| Set Up the Bandwidth Management Global Setting on the ZyWALL/USG..... | 617 |
| Test the Result | 617 |
| What Could Go Wrong? | 618 |
| How to Configure a Trunk for WAN Load Balancing with a Static or Dynamic IP Address..... | 619 |
| Set Up the Available Bandwidth on WAN1 Interfaces on the ZyWALL/USG..... | 620 |
| Set Up the Available Bandwidth on WAN2 Interfaces on the ZyWALL/USG..... | 621 |
| Set Up the WAN Trunk on the ZyWALL/USG | 621 |
| Test the Result | 622 |
| What Could Go Wrong? | 623 |
| How to Configure DNS Inbound Load Balancing to balance DNS Queries Among Interfaces | 624 |
| Set Up the DNS Inbound Load Balancing on the ZyWALL/USG | 625 |
| Set Up the NAT Rule on the ZyWALL/USG | 626 |
| Test the Result | 627 |
| What Could Go Wrong? | 628 |
| How to Manage Voice Traffic | 629 |
| Set Up the SIP ALG on the ZyWALL/USG | 630 |
| Set Up the Bandwidth Management for SIP on the ZyWALL/USG | 630 |
| Set Up the Bandwidth Management for P2P on the ZyWALL/USG | 631 |
| Set Up the Bandwidth Management for FTP on the ZyWALL/USG | 632 |
| Test the Result | 634 |
| What Could Go Wrong? | 635 |
| How to Manage ZyWALL/USG Configuration Files | 636 |
| Rename the Configuration Files from the ZyWALL/USG | 637 |
| Download the Configuration Files on the ZyWALL/USG | 637 |
| Copy the Configuration Files on the ZyWALL/USG | 638 |
| Apply the Configuration Files on the ZyWALL/USG | 639 |

| | |
|---|------------|
| Upload the Configuration Files from the ZyWALL/USG | 640 |
| What Could Go Wrong? | 640 |
| How to Manage ZyWALL/USG Firmware | 641 |
| Download the Current Firmware Version from ZyXEL.com | 642 |
| Upload the Firmware on the ZyWALL/USG | 643 |
| What Could Go Wrong? | 646 |
| How to Get Started Using the Wizards..... | 647 |
| Set Up the Internet Access (Ethernet) Wizard on the ZyWALL/USG | 647 |
| Set Up the Internet Access (PPPoE) Wizard on the ZyWALL/USG .. | 651 |
| Set Up the Internet Access (PPTP) Wizard on the ZyWALL/USG | 654 |
| Set Up the Wireless Settings Wizard on the ZyWALL/USG | 658 |
| Set Up the Device Registration on the ZyWALL/USG | 660 |
| How to Configure the 3G/LTE Interface on the ZyWALL/USG as a WAN | |
| Backup..... | 662 |
| Set Up the 3G/LTE Interface on the ZyWALL/USG | 663 |
| Set Up the Trunk on the ZyWALL/USG | 664 |
| Test the Result | 665 |
| What Could Go Wrong? | 666 |
| How to Configure Two Different WAN Interfaces with Different IP | |
| Addresses in the Same VLAN..... | 667 |
| Set Up the Port Grouping on the ZyWALL/USG | 668 |
| Set Up the VLAN on the ZyWALL/USG | 668 |
| Set Up the Routing on the ZyWALL/USG | 670 |
| Test the Result | 670 |
| What Could Go Wrong? | 671 |
| How to Let a Server Use the Same Public IP Address as the WAN | |
| Interface Using the Bridge Interface | 671 |
| Set Up the Bridge Interface on the ZyWALL/USG | 672 |
| Test the Result | 674 |
| What Could Go Wrong? | 675 |
| How to Allow Public Access to a Server Behind ZyWALL/USG | 675 |
| Set Up the NAT on the ZyWALL/USG | 676 |

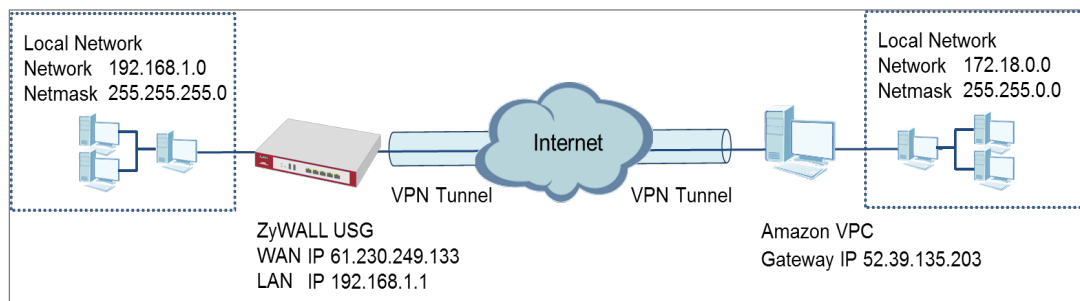
| | |
|--|------------|
| Set Up the Security Policy on the ZyWALL/USG | 677 |
| Test the Result | 678 |
| What Could Go Wrong? | 678 |
| How to Set Up a WiFi Network with ZyXEL APs | 680 |
| Set Up the AP Management on the ZyWALL/USG | 681 |
| Test the Result | 683 |
| What Could Go Wrong? | 684 |
| How to Set Up Guest WiFi Network Accounts..... | 685 |
| Set Up the WiFi Guest Account, Address Range and Service Rule on the ZyWALL/USG | 686 |
| Set Up the Web Authentication on the ZyWALL/USG | 688 |
| Set Up the Security Policy on the ZyWALL/USG | 689 |
| Test the Result | 690 |
| What Could Go Wrong? | 693 |
| How to create a Wi-Fi VLAN interfaces to separate staff network and Guest network | 695 |
| Set up Wi-Fi VLAN interfaces | 696 |
| Test result | 706 |
| What could go wrong | 708 |
| How to Set Up WiFi Networks with Microsoft Active Directory Authentication..... | 710 |
| Set Up the Wi-Fi Guest Account and Authentication Method on the ZyWALL/USG..... | 711 |
| Set Up the Active Directory Server Account on the ZyWALL/USG | 712 |
| Set Up the Security Policy on the ZyWALL/USG | 713 |
| Test the Result | 714 |
| What Could Go Wrong? | 716 |
| How to Set Up IPv6 Interfaces for Pure IPv6 Routing | 717 |
| Enable the IPv6 on the ZyWALL/USG | 718 |
| Set Up the WAN IPv6 Interface on the ZyWALL/USG..... | 719 |
| Set Up the LAN IPv6 Interface on the ZyWALL/USG | 719 |
| Test the Result | 720 |
| What Could Go Wrong? | 722 |

| | |
|--|------------|
| How to Set Up an IPv6 6to4 Tunnel | 722 |
| Set Up the LAN IPv6 Interface on the ZyWALL/USG | 723 |
| Set Up the 6to4 Tunnel on the ZyWALL/USG | 725 |
| Test the Result | 726 |
| What Could Go Wrong? | 727 |
| How to Set Up an IPv6-in-IPv4 Tunnel..... | 727 |
| Set Up the LAN IPv6 Interface on the ZyWALL/USG | 728 |
| Set Up the 6to4 Tunnel on the ZyWALL/USG | 729 |
| Set Up the Policy Route on the ZyWALL/USG..... | 730 |
| Test the Result | 731 |
| What Could Go Wrong? | 732 |
| How to Update Firmware Automatically from a USB Storage..... | 733 |
| Automatic USB Firmware Upgrade Flow | 733 |
| Enable the USB Firmware Upgrade Function by CLI Command... | 734 |
| Save the Firmware on the USB..... | 734 |
| Plug the USB into the Device | 735 |
| The Device Checks Running Partition for the Model ID and the Firmware Version | 735 |
| Check Firmware Status..... | 736 |
| What Can Go Wrong?..... | 737 |
| How to Configure DHCP Option 60 – Vendor Class Identifier | 739 |
| DHCP Option 60 Deployment Flow..... | 740 |
| Setting Up DHCP Option 60 on the Web GUI..... | 740 |
| Setting Up DHCP Option 60 on the CLI..... | 741 |
| Test DHCP Option 60..... | 742 |
| What Can Go Wrong? | 742 |
| How to Configure Device HA Pro | 743 |
| Device HA Pro License | 744 |
| Behavior of the Device HA Pro | 744 |
| Device-HA Pro Setting Screen | 744 |
| Suggestions | 746 |
| How do I Configure Device HA Pro in My Current Environment? . | 747 |
| What can go wrong? | 751 |

| | |
|---|------------|
| How to setup Two-Factor Authentication for admin login | 752 |
| Setup SMTP function on your device | 752 |
| Create admin type user on device | 753 |
| Setup Two-Factor Authentication for admin on your device | 754 |
| Test the Result | 755 |
| What Can Go Wrong? | 757 |
| How to configure Email Security for Phishing mail? | 759 |
| How it works | 759 |
| Set up Phishing on ATP | 760 |
| Test the Result | 761 |
| What Can Go Wrong? | 761 |
| How to setup Email to SMS | 763 |
| Setup SMTP function on your device | 763 |
| Setup Email to SMS Provider configuration | 764 |
| Create admin type user on device | 765 |
| Setup Two-Factor Authentication for admin on your device | 765 |
| Test the Result | 766 |
| What Can Go Wrong? | 768 |
| How to Use IP Reputation to Detect Threats | 769 |
| Activating Reputation Filter Service | 770 |
| Enabling IP Blocking on ATP | 770 |
| Selecting specific type of IP addresses to block | 771 |
| Adding IP addresses to white list and black list | 771 |
| Monitoring statistics for IP detection | 772 |
| Test the Result | 772 |
| What Can Go Wrong? | 774 |

How to Configure Site-to-site IPSec VPN with Amazon VPC

This example shows how to use the VPN Setup Wizard to create a site-to-site VPN between a ZyWALL/USG and an Amazon VPC platform. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



ZyWALL/USG Site-to-site IPSec VPN with Amazon VPC



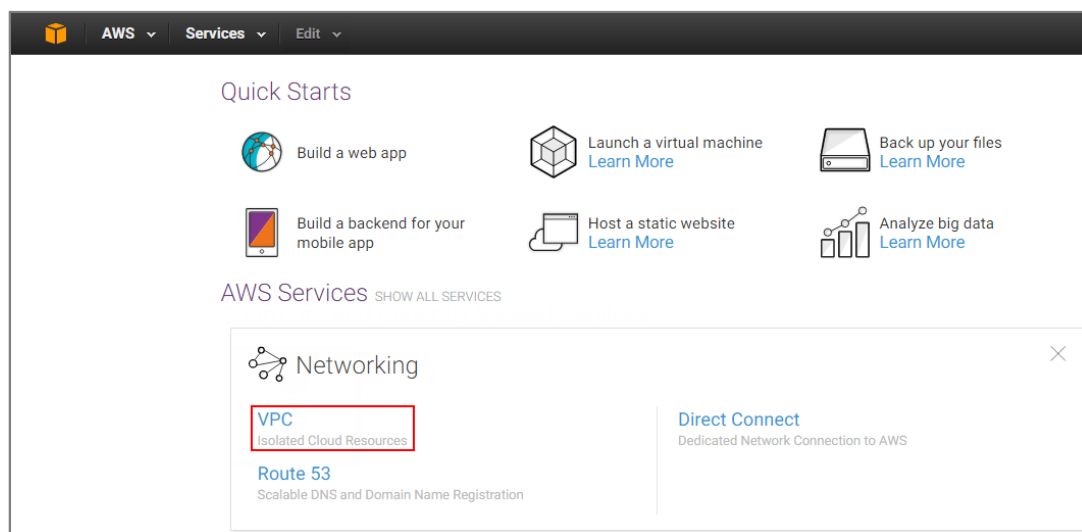
Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG110 (Firmware Version: ZLD 4.25) and Amazon VPC (June, 2016).

Set Up the IPSec VPN Tunnel on the Amazon VPC

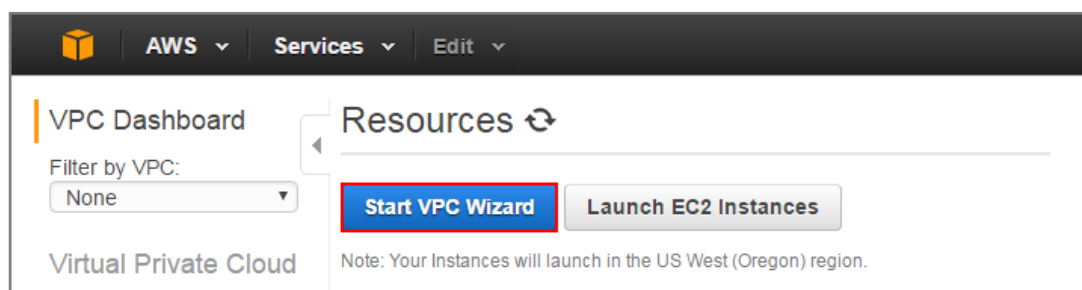
- 1 Sign into the Amazon AWS Management Console. Go to Networking > VPC.

Amazon AWS Management Console > Networking > VPC



- 2 In the upper left-hand of the screen, click **Start VPC Wizard**.

Amazon VPC Management Console > Networking > VPC > Start VPC Wizard



- 3 Select a VPC Configuration, select VPC with a Private Subnet Only and Hardware VPN Access, and then click Select.

Select a VPC Configuration > VPC with a Private Subnet Only and Hardware VPN Access

Step 1: Select a VPC Configuration

VPC with a Single Public Subnet

VPC with Public and Private Subnets

VPC with Public and Private Subnets and Hardware VPN Access

VPC with a Private Subnet Only and Hardware VPN Access

Your instances run in a private, isolated section of the AWS cloud with a private subnet whose instances are not addressable from the Internet. You can connect this private subnet to your corporate data center via an IPsec Virtual Private Network (VPN) tunnel.

Creates:

A /16 network with a /24 subnet and provisions an IPsec VPN tunnel between your Amazon VPC and your corporate network. (VPN charges apply.)

Select

Amazon Virtual Private Cloud Subnet

VPN

Corporate Data Center

- 4 VPC with a Private Subnet Only and Hardware VPN, add your **IP CIDR block** and **Private subnet**. Click **Next**.

VPC with a Private Subnet Only and Hardware VPN

Step 2: VPC with a Private Subnet Only and Hardware VPN Access

IP CIDR block:* **172.18.0.0/16** (65531 IP addresses available)

VPC name:

Private subnet:* **172.18.0.0/24** (251 IP addresses available)

Availability Zone:*

Private subnet name:

You can add more subnets after AWS creates the VPC.

Add endpoints for S3 to your subnets

Subnet:


Enable DNS hostnames:* ☒ Yes ☐ No

Hardware tenancy:*

Next

- 5 Configure your VPN, add your ZyWALL/USG public IP address into **Customer Gateway IP**. Name your **Customer Gateway name** and **VPN Connection name**.
Click **Create VPC** at the bottom of the blade.

Configure your VPN



Step 3: Configure your VPN

Specify the public IP Address of your VPN router (Customer Gateway)

Customer Gateway IP:* 61.230.249.133

Customer Gateway name: GW_to_ZyWALL/USG

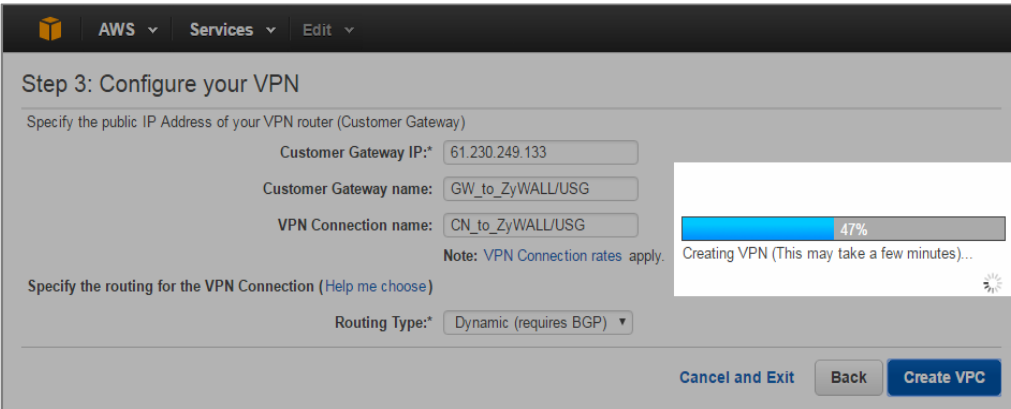
VPN Connection name: CN_to_ZyWALL/USG

Note: VPN Connection rates apply.

Specify the routing for the VPN Connection ([Help me choose](#))

Routing Type:* Dynamic (requires BGP) ▼

[Cancel and Exit](#) [Back](#) [Create VPC](#)



Step 3: Configure your VPN

Specify the public IP Address of your VPN router (Customer Gateway)

Customer Gateway IP:* 61.230.249.133

Customer Gateway name: GW_to_ZyWALL/USG

VPN Connection name: CN_to_ZyWALL/USG

Note: VPN Connection rates apply.

Specify the routing for the VPN Connection ([Help me choose](#))

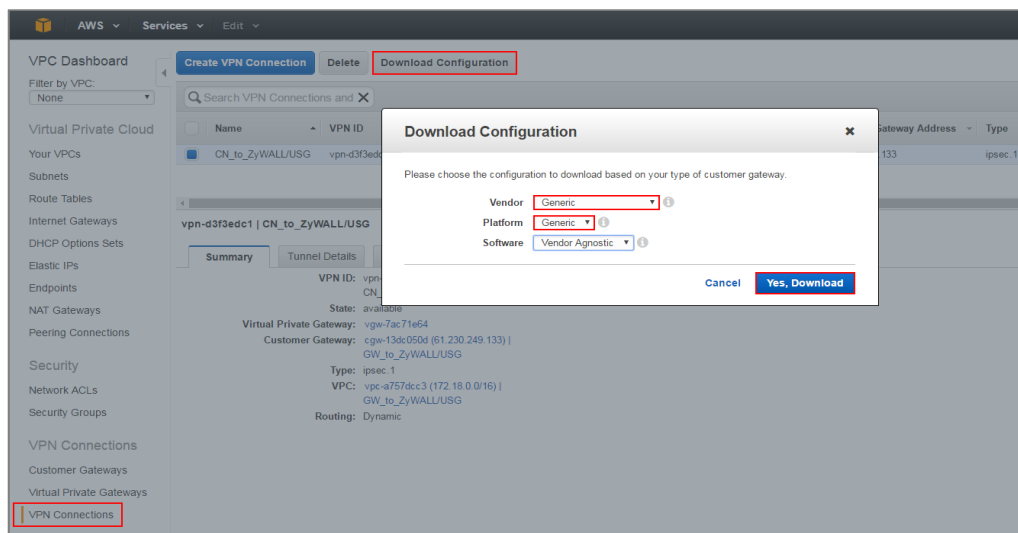
Routing Type:* Dynamic (requires BGP) ▼

[Cancel and Exit](#) [Back](#) [Create VPC](#)

47%
Creating VPN (This may take a few minutes)...

- 6 In the VPC Dashboard, go to VPN Connections. Select Download Configuration from the upper bar. Select Vendor and Platform to be Generic. Click Yes, Download.

VPC Dashboard > VPN Connections



- 7 Open the downloaded configuration txt. file, it displays IKE SA, IPsec SA and Gateway IP address. Please make sure all the settings match your ZyWALL/USG's setting.

Configuration txt. File

```
IPSec Tunnel #1
=====
#1: Internet Key Exchange Configuration
Configure the IKE SA as follows:
- Authentication Method      : Pre-Shared Key
- Pre-Shared Key            : 2EHrEA5WT6QFMEBaaPZT1bBmnoUaCLhW
- Authentication Algorithm   : sha1
- Encryption Algorithm       : aes-128-cbc
- Lifetime                   : 28800 seconds
- Phase 1 Negotiation Mode   : main
- Perfect Forward Secrecy    : Diffie-Hellman Group 2

#2: IPSec Configuration
Configure the IPSec SA as follows:
- Protocol                   : esp
- Authentication Algorithm    : hmac-sha1-96
- Encryption Algorithm        : aes-128-cbc
- Lifetime                   : 3600 seconds
- Mode                       : tunnel
- Perfect Forward Secrecy     : Diffie-Hellman Group 2

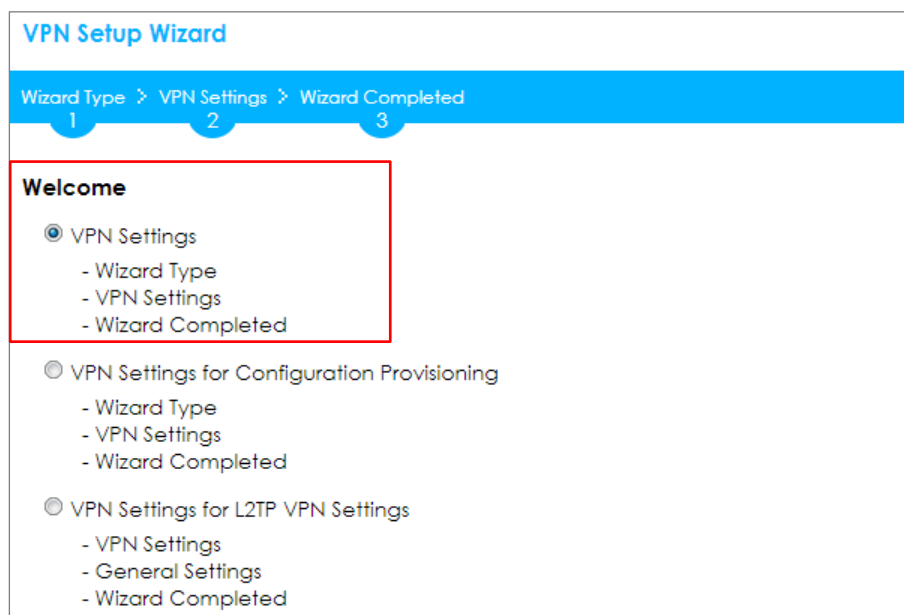
IPSec Dead Peer Detection (DPD) will be enabled on the AWS Endpoint. We
recommend configuring DPD on your endpoint as follows:
- DPD Interval               : 10
- DPD Retries                 : 3

#3: Tunnel Interface Configuration
Outside IP Addresses:
- Customer Gateway           : 61.230.249.133
- Virtual Private Gateway    : 52.39.135.203
```

Set Up the IPSec VPN Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the Amazon VPC. Click **Next**.

Quick Setup > **VPN Setup Wizard > Welcome**



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

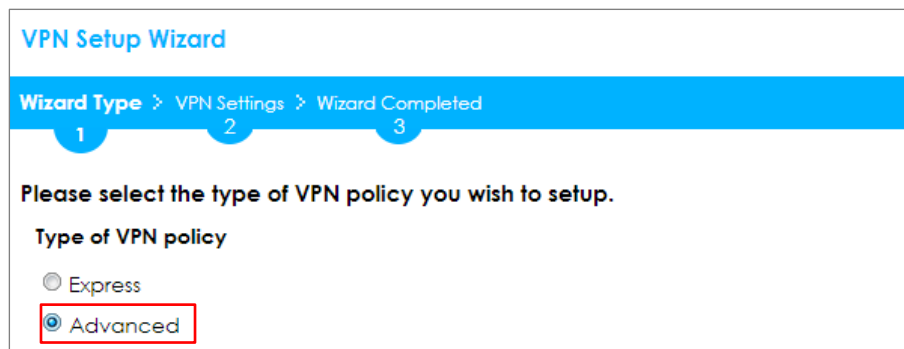
1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

Choose **Advanced** to create a VPN rule with the customize phase 1, phase 2 settings and authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Please select the type of VPN policy you wish to setup.

Type of VPN policy

- ☐ Express
- ☒ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Advanced Settings

IKE Version

☒ IKEv1
☐ IKEv2

Scenario

Rule Name:

☒ Site-to-site
☐ Site-to-site with Dynamic Peer
☐ Remote Access (Server Role)
☐ Remote Access (Client Role)

Then, configure the **Secure Gateway** IP as the peer Amazon VPC's Gateway IP address (in the example, 52.39.135.203); select **My Address** to be the interface connected to the Internet.

Set the **Negotiation**, **Encryption**, **Authentication**, **Key Group** and **SA Life Time** which Amazon VPC supports. Type a secure **Pre-Shared Key**.

Quick Setup > **VPN Setup Wizard** > **Welcome** > **Wizard Type** > **VPN Settings (Phase 1 Setting)**

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Advanced Settings

Phase 1 Setting

Secure Gateway: 52.39.135.203 (IP or FQDN)

My Address (interface): ge1

Negotiation Mode: Main

Encryption Algorithm: AES128

Authentication Algorithm: SHA1

Key Group: DH2

SA Life Time: 86400 (180 - 3000000 seconds)

☒ NAT Traversal

☒ Dead Peer Detection (DPD)

Authentication Method

☒ Pre-Shared Key 12345678

☐ Certificate default

Continue to Phase 2 Settings to select the **Encapsulation**, **Encryption**, **Authentication**, and **SA Life Time** settings which Amazon VPC supports.

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the Amazon VPC. Click **OK**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings

(Phase 2 Setting)

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

123

Advanced Settings

Phase 2 Setting

Active Protocol: ESP
Encapsulation: Tunnel
Encryption Algorithm: AES128
Authentication Algorithm: SHA1
SA Life Time: 86400 (180 - 3000000 seconds)
Perfect Forward Secrecy (PFS): None

Policy Setting

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask): 172.18.0.0 / 255.255.0.0

Property

☒ Nailed-Up

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings
(Summary)

Wizard Type > **VPN Settings** > Wizard Completed

123

Advanced Settings

Summary

| | |
|--------------------------|-----------------------------|
| Rule Name: | VPN_to_VPC |
| Secure Gateway: | 52.39.135.203 |
| Pre-Shared Key: | 12345678 |
| Local Policy (IP/Mask): | 192.168.1.0 / 255.255.255.0 |
| Remote Policy (IP/Mask): | 172.18.0.0 / 255.255.255.0 |

Phase 1

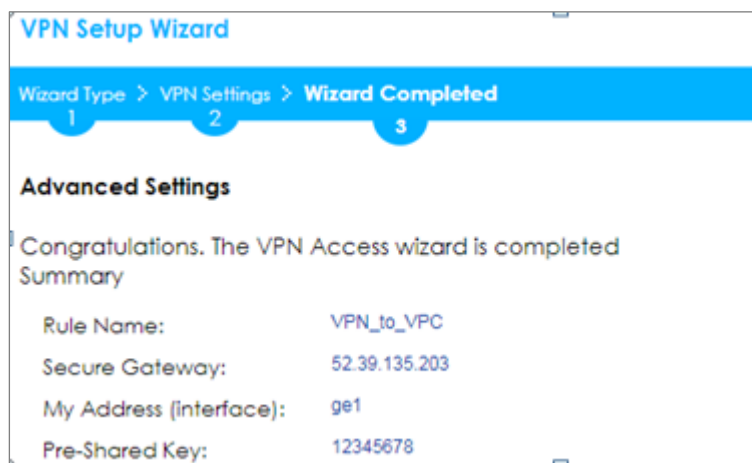
| | |
|---------------------------|--------|
| Negotiation Mode: | main |
| Encryption Algorithm: | aes128 |
| Authentication Algorithm: | sha |
| Key Group: | DH2 |

Phase 2

| | |
|---------------------------|--------|
| Active Protocol: | esp |
| Encapsulation: | tunnel |
| Encryption Algorithm: | aes128 |
| Authentication Algorithm: | sha |

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed



Test the IPSec VPN Tunnel

Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

| Add Edit Remove Activate Inactivate Connect Disconnect Object References | | | | | |
|--|--------|--------------|--------------|--------------------|--|
| # | Status | Name | VPN Gateway | Gateway IP Version | Policy |
| 1 | | VPN_to_Azure | VPN_to_Azure | IPv4 | VPN_to_VPC_LOCAL / VPN_to_VPC_REMOTE |

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic.

MONITOR > VPN Monitor > IPSec

| Disconnect Connection Check | | | | | | | | |
|---|-------------|-------------------------------|----------------|-----------------------|---------|---------|--------------|-------------|
| # | Name | Policy | My Address | Secure Gateway | Up Time | Timeout | Inbound(B... | Outbound... |
| 1 | WIZ_VPN_VPC | 192.168.1.0/24<>172.18.0.0/24 | 61.230.249.133 | P: 52.39.135.203:4500 | 28 | 76292 | 0(0 bytes) | 0(0 bytes) |

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

To test whether or not a tunnel is working, ping from a Local LAN to AWS VPC private Subnet for verification. Ensure that both computers have Internet access.

Ping from Local LAN to AWS VPC private Subnet for verification:

```
C:\Documents and Settings\ZyXEL>ping 172.18.0.15

Pinging 172.18.0.15 with 32 bytes of data:

Reply from 172.18.0.15 : bytes=32 time=27ms TTL=43
Reply from 172.18.0.15 : bytes=32 time=32ms TTL=43
Reply from 172.18.0.15 : bytes=32 time=26ms TTL=43
Reply from 172.18.0.15 : bytes=32 time=27ms TTL=43

Ping statistics for 172.18.0.15 :
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 32ms, Average = 28ms
```

What Could Go Wrong?

If you see below [info] or [error] log message, please check ZyWALL/USG Phase 1 Settings. Make sure your ZyWALL/USG Phase 1 Settings are supported in the Amazon VPC IKE Phase 1 setup list.

MONITOR > Log

| Priority | Category | Message | Note |
|----------|----------|--|---------|
| info | IKE | Recv:[NOTIFY:INVALID_COOKIE] | IKE_LOG |
| info | IKE | Send:[ID][HASH][NOTIFY:INITIAL_CONTACT] | IKE_LOG |
| Priority | Category | Message | Note |
| error | IPSec | SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet | IPSec |
| error | IPSec | SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet | IPSec |
| info | IKE | [COOKIE] Invalid cookie, no sa found | IKE_LOG |
| Priority | Category | Message | Note |
| info | IKE | Recv:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN] | IKE_LOG |

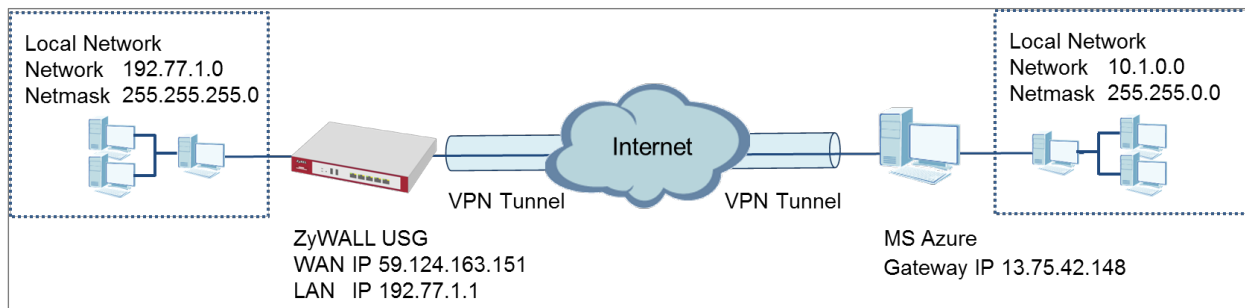
If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG Phase 2 Settings. Make sure your ZyWALL/USG Phase 2 Settings are supported in the Amazon VPC IKE Phase 2 setup list.

MONITOR > Log

| | | | | | |
|-----|--------------------|------|-----|--------------------------------|---------|
| 123 | 2017-09-11 10:1... | info | IKE | Recv:[HASH][SA][NONCE][ID][ID] | IKE_LOG |
| 127 | 2017-09-11 10:1... | info | IKE | Phase 1 IKE SA process done | IKE_LOG |

How to Configure Site-to-site IPSec VPN with Microsoft (MS) Azure

This example shows how to use the VPN Setup Wizard to create a site-to-site VPN between a ZyWALL/USG and a Microsoft (MS) Azure platform. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



ZyWALL Site-to-site IPSec VPN with Microsoft (MS) Azure

Note:

1. All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG40 (Firmware Version: ZLD 4.25) and MS Azure (April, 2016).

Set Up the IPSec VPN Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the MS Azure. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

Choose **Advanced** to create a VPN rule with the customize phase 1, phase 2 settings and authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
1 2 3

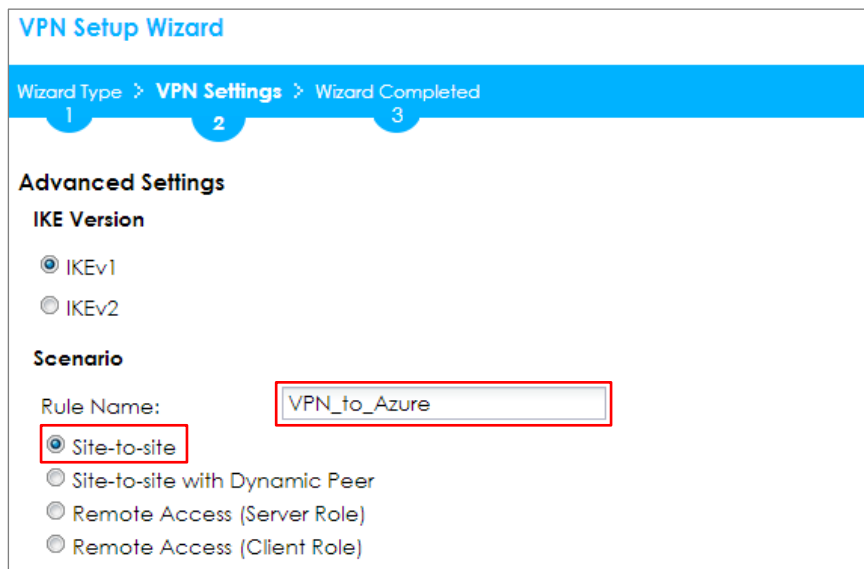
Please select the type of VPN policy you wish to setup.

Type of VPN policy

- ☐ Express
- ☒ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway).
You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Advanced Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name:

☒ **Site-to-site**

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

Then, configure the **Secure Gateway** IP as the peer MS Azure's Gateway IP address (in the example, 13.75.42.148); select **My Address** to be the interface connected to the Internet.

Set the **Negotiation**, **Encryption**, **Authentication**, **Key Group** and **SA Life Time** which MS Azure supports. Please make sure you disable **Dead Peer Detection (DPD)** which is not supported in the MS Azure IKEv1 Policy-based. Type a secure **Pre-Shared Key**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Phase 1 Setting)

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Advanced Settings

Phase 1 Setting

Secure Gateway: 13.75.42.148 (IP or FQDN)

My Address (interface): ge1

Negotiation Mode: Main

Encryption Algorithm: AES256

Authentication Algorithm: SHA1

Key Group: DH2

SA Life Time: 86400 (180 - 3000000 seconds)


☒ NAT Traversal

☐ Dead Peer Detection (DPD)

Authentication Method

☒ Pre-Shared Key 12345678

☐ Certificate default

 Note: For more information about the IPsec Parameters supported in MS Azure, see the Microsoft Azure Documentation [About VPN devices](#) for Site-to-Site VPN Gateway connections.

Continue to Phase 2 Settings to select the **Encapsulation**, **Encryption**, **Authentication**, and **SA Life Time** settings which MS Azure supports.

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the MS Azure. Click **OK**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Phase 2 Setting)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Advanced Settings

Phase 2 Setting

Active Protocol:

ESP

Encapsulation:

Tunnel

Encryption Algorithm:

AES128

Authentication Algorithm:

SHA1

SA Life Time:

86400

(180 - 3000000 seconds)

Perfect Forward Secrecy (PFS):

None

Policy Setting

Local Policy (IP/Mask):

192.77.1.0

255.255.255.0


Remote Policy (IP/Mask):

10.1.0.0

255.255.0.0

Property

☒ Nailed-Up

 **Note:** For more information about the IPsec Parameters supported in MS Azure, see the Microsoft Azure Documentation [About VPN devices](#) for Site-to-Site VPN Gateway connections.

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

**Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings
(Summary)**

Wizard Type > **VPN Settings** > Wizard Completed
 1 2 3

Advanced Settings

Summary

| | |
|--------------------------|----------------------------|
| Rule Name: | VPN_to_Azure |
| Secure Gateway: | 13.75.42.148 |
| Pre-Shared Key: | 12345678 |
| Local Policy (IP/Mask): | 192.77.1.0 / 255.255.255.0 |
| Remote Policy (IP/Mask): | 10.1.0.0 / 255.255.0.0 |

Phase 1

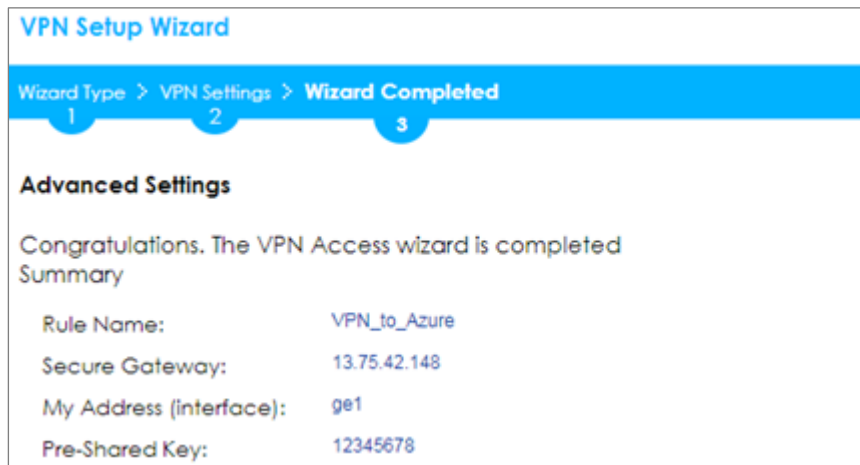
| | |
|---------------------------|--------|
| Negotiation Mode: | main |
| Encryption Algorithm: | aes128 |
| Authentication Algorithm: | sha |
| Key Group: | DH2 |

Phase 2

| | |
|-----------------------|--------|
| Active Protocol: | esp |
| Encapsulation: | tunnel |
| Encryption Algorithm: | aes128 |

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

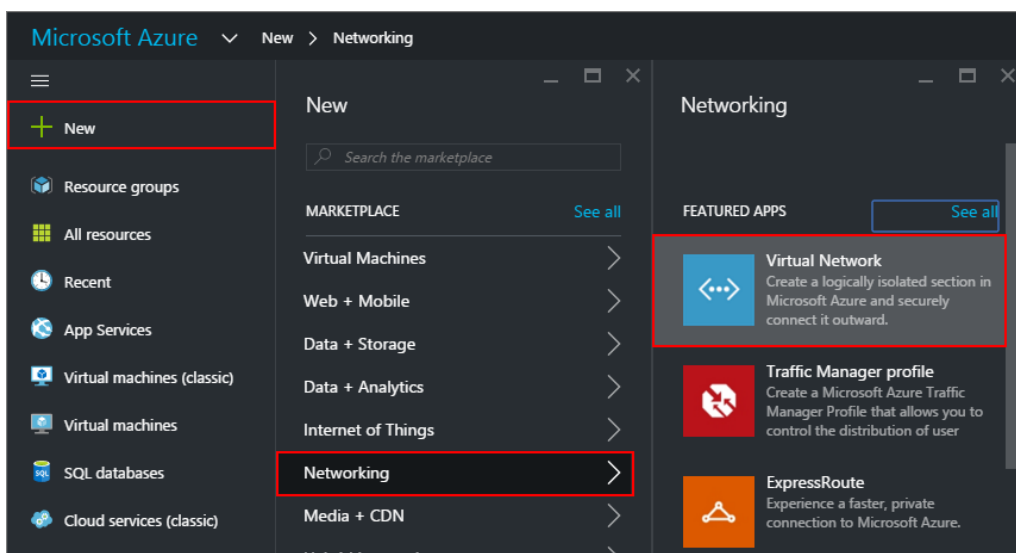
Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed



Set Up the IPSec VPN Tunnel on the MS Azure

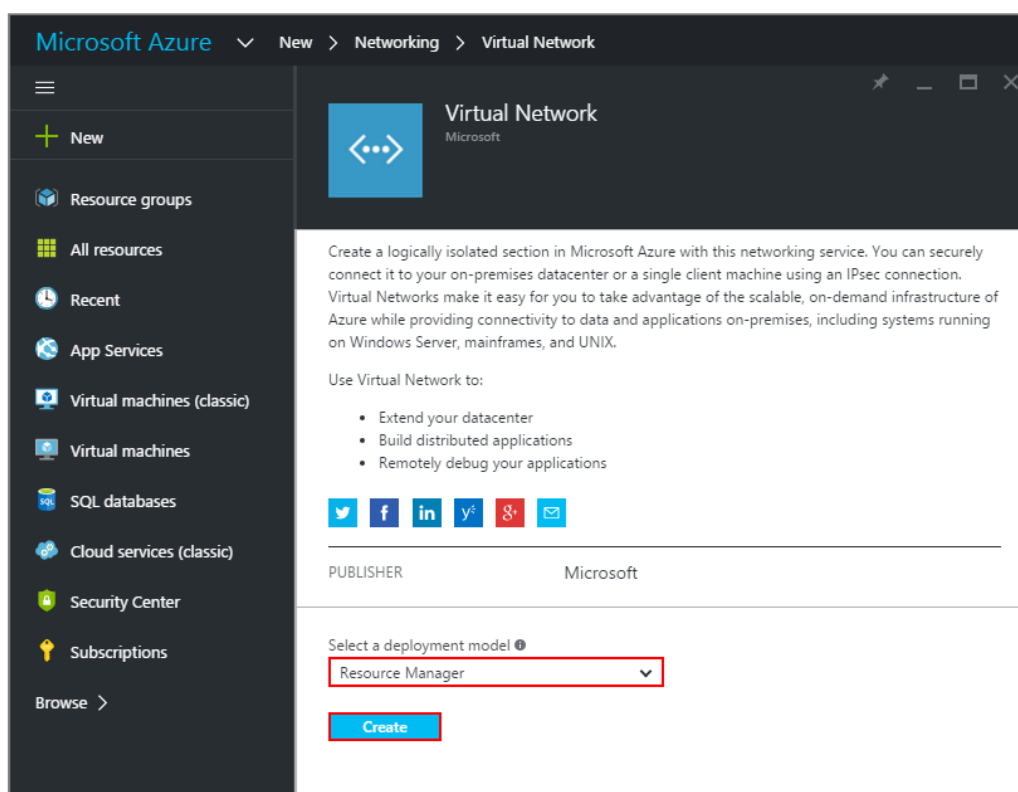
Sign into the **Windows Azure Management Portal**. In the upper left-hand corner of the screen, click **+New > Networking > Virtual Network**.

Azure portal > New > Networking > Virtual Network



Near the bottom of the **Virtual Network** blade, from the **Select a deployment model** list, select **Resource Manager**, and then click **Create**.

New > Networking > Virtual Network > Select a deployment model



On the **Create virtual network** page, enter the **NAME** for the VPN network. For example, **VPN_Vnet_to_USG**. Add your **Address Space**, **Subnet name** and a single **Subnet address range**.

Click **Resource group** and either select an existing resource group, or create a new one by typing a name for your new resource group. For example, **RG_USG**.

LOCATION is directly related to the physical location (region) where the virtual machines (VMs) reside. The region associated with the virtual network cannot be changed after it has been created.

Then, click the **Create** button. After clicking Create, you will see a tile on your dashboard that will reflect the progress of your VNet. The tile will change as the VNet is being created.

New > Networking > Virtual Network > Create virtual network

Microsoft Azure New > Networking > Virtual Network > Create virtual network

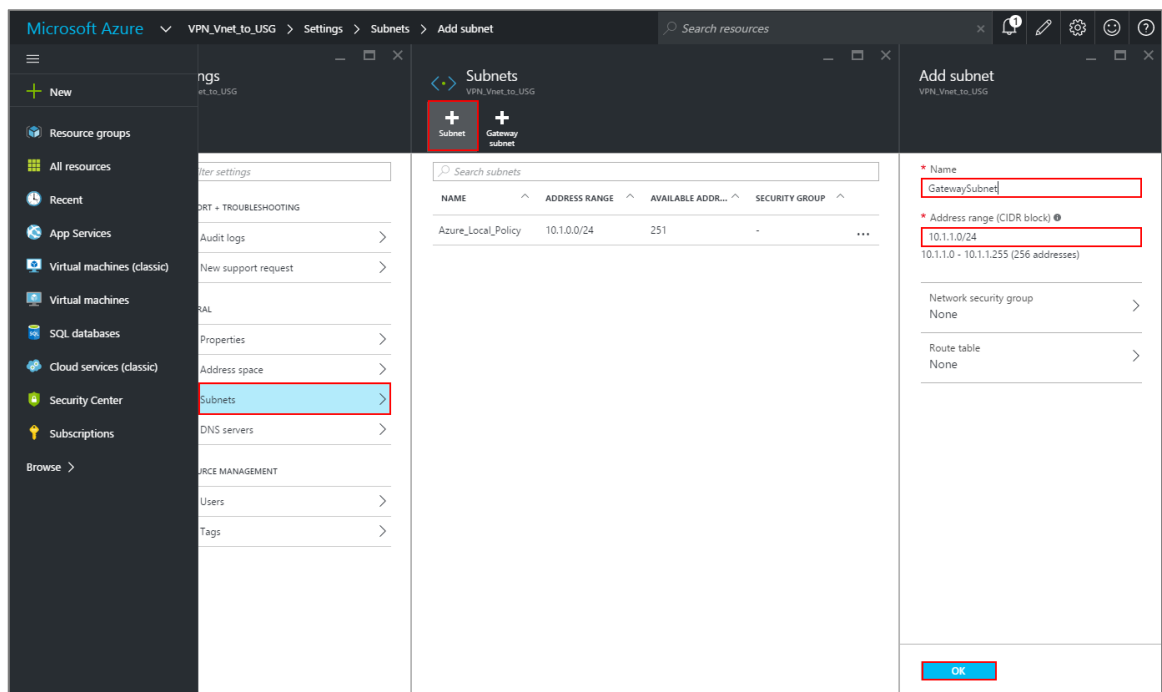
Create virtual network

- * Name: VPN_Vnet_to_USG ✓
- * Address space ⓘ: 10.1.0.0/16 ✓
10.1.0.0 - 10.1.255.255 (65536 addresses)
- * Subnet name: Azure_Local_Policy ✓
- * Subnet address range ⓘ: 10.1.0.0/24 ✓
10.1.0.0 - 10.1.0.255 (256 addresses)
- Subscription: Free Trial ▼
- * Resource group: + New ▼
- New resource group name: RG_USG ✓
- Location: East Asia ▼
- ☒ Pin to dashboard
- Create**

In the portal, navigate to the virtual network to which you just created. On the blade for your virtual network, click the **Settings** icon at the top of the blade to expand the Setting blade to **Subnets > Add > Add Subnet**. **Name** your subnet

GatewaySubnet. You should not name it anything else, or the gateway will not work. Add the IP **Address range** for your gateway. Click **OK** at the bottom of the blade to create the subnet.

VPN Vnet_to_USG > Settings > Subnet > Add subnet



In the portal, go to **New**, then Networking. Select **Virtual network gateway** from the list. On the **Create virtual network gateway** blade **Name** field, name your gateway. Next, choose the **Virtual network** that you want to deploy this gateway to.

Click the arrow (>) to open the **Choose public IP address** blade. Then click **Create New** to open the **Create public IP address** blade. Input a **Name** for your public IP address. Note that this is not asking for an IP address. The IP address will be assigned dynamically. Rather, this is the name of the IP address object that the address will be assigned to. Click **OK** to save your changes.

For **Gateway type**, select **VPN**. For **VPN type**, select **Policy-based**. For **Resource Group**, the resource group is determined by the Virtual Network that you select. For **Location**, make sure it's showing the location that both your Resource Group and VNet exist in.

New > Networking > Create virtual network gateway > Choose public IP address > Create public IP address

The screenshot displays the Microsoft Azure portal interface for creating a virtual network gateway. It consists of three main panels:

- Create virtual network gateway:** This panel contains several configuration fields:
 - Name:** VPN_GW_to_USG
 - Virtual network:** VPN_Vnet_to_USG
 - Public IP address:** Choose a public IP address
 - Gateway type:** VPN (selected), ExpressRoute
 - VPN type:** Route-based, Policy-based (selected)
 - Subscription:** Free Trial
 - Resource group:** RG_USG
 - Location:** East Asia
 - Buttons:** Pin to dashboard, Create
 - Warning:** Provisioning a virtual network gateway may take up to 45 minutes.
- Choose public IP address:** This panel shows a 'Create new' button and a message 'No results'.
- Create public IP address:** This panel shows a 'Name' field with the value 'VPN_GW_to_USG_Public_IP' and an 'OK' button.

In the Azure Portal, navigate to **New > Networking > Local network gateway**. The local network gateway refers to your ZyWALL/USG public IP and local subnet settings.

On the **Create local network gateway** blade, specify a **Name** for your ZyWALL/USG gateway object.

Specify public IP address of your ZyWALL/USG. It cannot be behind NAT and has to be reachable by Azure. **Address space** refers to the address ranges on your ZyWALL/USG local network. For **Resource Group**, select the resource group that you created before. For **Location**, if you are creating a new local network

gateway, you can use the same location as the virtual network gateway. But, this is not required. The local network gateway can be in a different location.

Click **Create** to create the local network gateway.

New > Networking > Local network gateway

The screenshot shows the Microsoft Azure portal interface for creating a local network gateway. The breadcrumb navigation at the top reads "New > Networking > Create local network gateway". The left sidebar contains a navigation menu with options like "New", "Resource groups", "All resources", "Recent", "App Services", "Virtual machines (classic)", "Virtual machines", "SQL databases", "Cloud services (classic)", "Security Center", and "Subscriptions". The main content area is titled "Create local network gateway" and contains the following form fields:

- Name:** VPN_Connection_to_USG (with a green checkmark icon)
- IP address:** 59.124.163.151 (with a green checkmark icon)
- Address space:** 192.77.1.0/24 (with a blue highlight and a dropdown arrow)
- Subscription:** Free Trial (with a dropdown arrow)
- Resource group:** RG_USG (with a dropdown arrow)
- Location:** East Asia (with a dropdown arrow)

At the bottom of the form, there is a checkbox labeled "Pin to dashboard" which is checked, and a blue "Create" button.

Locate your virtual network gateway (VPN_Connection_to_USG in this example) and click **Settings > Connection > Add connection**, **Name** your connection. For **Connection type**, select **Site-to-site (IPSec)**. For **Virtual network gateway**, the value is fixed because you are connecting from this gateway (VPN_GW_to_USG in this example).

For **Local network gateway**, select the local network gateway that you want to use (VPN_Connection_to_USG in this example).

For **Shared Key (PSK)**, the value here must match the value that you are using for your ZyWALL/USG device. For **Resource Group**, select the resource group that you **created before**. Click **OK** to create your connection.

VPN_Connection_to_USG > Settings > Connections > Add connection

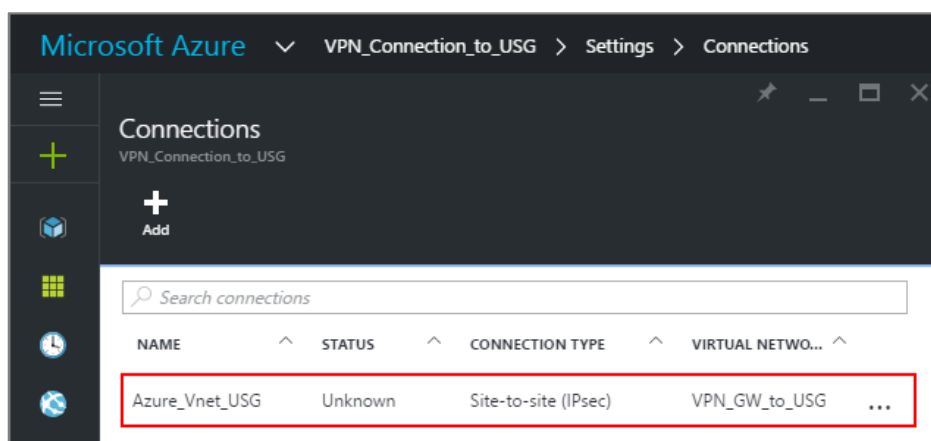
The screenshot shows the 'Add connection' form in the Microsoft Azure portal. The breadcrumb navigation is 'VPN_Connection_to_USG > Settings > Connections > Add connection'. The form is titled 'Add connection' and is for the resource 'VPN_Connection_to_USG'. The form includes the following fields:

- Name:** Azure_Vnet_USG (with a green checkmark)
- Connection type:** Site-to-site (IPsec) (with a dropdown arrow)
- Virtual network gateway:** VPN_GW_to_USG (with a right arrow)
- Local network gateway:** VPN_Connection_to_USG (with a lock icon)
- Shared key (PSK):** zyxel1234 (with a green checkmark)
- Subscription:** Free Trial (with a dropdown arrow)
- Resource group:** RG_USG (with a lock icon)
- Location:** East Asia (with a dropdown arrow)

An 'OK' button is located at the bottom of the form.

When the connection is complete, you'll see it appear in the **Connections** blade for your Gateway.

VPN_Connection_to_USG > Settings > Connections



Test the IPsec VPN Tunnel

Go to ZyWALL/USG **CONFIGURATION > VPN > IPsec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPsec VPN > VPN Connection

| Add Edit Remove Activate Inactivate Connect Disconnect Object References | | | | | |
|--|--------|--------------|--------------|--------------------|--|
| # | Status | Name | VPN Gateway | Gateway IP Version | Policy |
| 1 | | VPN_to_Azure | VPN_to_Azure | IPv4 | VPN_to_Azure_LOCAL/VPN_to_Azure_REMOTE |
| Page 1 of 1 Show 50 Items Displaying 1 - 1 of 1 | | | | | |

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic.

MONITOR > VPN Monitor > IPSec

| Disconnect | | Connection Check | | | | | | |
|-------------|---------------|----------------------------|----------------|-----------------------|---------|---------|--------------|-------------|
| # | Name | Policy | My Address | Secure Gateway | Up Time | Timeout | Inbound(B... | Outbound... |
| 1 | WIZ_VPN_Azure | 192.77.1.0/24<>10.1.0.0/16 | 59.124.163.151 | P: 13.75.42.148:4500 | 14 | 86406 | 0(0 bytes) | 0(0 bytes) |
| Page 1 of 1 | | Show 50 items | | Displaying 1 - 1 of 1 | | | | |

Go to **Azure_Vnet_USG > Settings** to check the tunnel **DATA IN** and **DATA OUT**.

VPN > VPN Settings > Currently Active VPN Tunnels

Microsoft Azure

Azure_Vnet_USG > Settings

+

Settings

Delete

Essentials

Resource group

RG_USG

Status

Connected

Location

East Asia

Subscription name

Free Trial

Subscription ID

23a31ce5-c9fa-4da3-958b-8bb1b6fe8790

Data in

0 B

Data out

576 B

Virtual network

VPN_Vnet_to_USG

Virtual network gateway

VPN_GW_to_USG (13.75.42.148)

Local network gateway

VPN_Connection_to_USG (59.124.163.151)

All settings

45/774

To test whether or not a tunnel is working, ping from a computer at one site to a computer at the other. Ensure that both computers have Internet access.

PC behind ZyWALL/USG > Window 7 > cmd > ping 10.1.0.33

```
C:\Documents and Settings\ZyXEL>ping 10.1.0.33

Pinging 10.1.0.33 with 32 bytes of data:

Reply from 10.1.0.33 : bytes=32 time=18ms TTL=54
Reply from 10.1.0.33 : bytes=32 time=17ms TTL=54
Reply from 10.1.0.33 : bytes=32 time=17ms TTL=54
Reply from 10.1.0.33 : bytes=32 time=16ms TTL=54

Ping statistics for 10.1.0.33 :
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 18ms, Average = 17ms
```

PC behind MS Azure> Window 7 > cmd > ping 192.77.1.33

```
C:\Documents and Settings\ZyXEL>ping 192.77.1.33

Pinging 192.77.1.33 with 32 bytes of data:

Reply from 192.77.1.33 : bytes=32 time=27ms TTL=43
Reply from 192.77.1.33 : bytes=32 time=32ms TTL=43
Reply from 192.77.1.33 : bytes=32 time=26ms TTL=43
Reply from 192.77.1.33 : bytes=32 time=27ms TTL=43

Ping statistics for 192.77.1.33 :
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 32ms, Average = 28ms
```

What Could Go Wrong?

If you see below [info] or [error] log message, please check ZyWALL/USG Phase 1 Settings. Make sure your ZyWALL/USG Phase 1 Settings are supported in the MS Azure IKE Phase 1 setup list.

MONITOR > Log

| Priority | Category | Message | Note |
|----------|----------|--|---------|
| info | IKE | Recv:[NOTIFY:INVALID_COOKIE] | IKE_LOG |
| info | IKE | Send:[ID][HASH][NOTIFY:INITIAL_CONTACT] | IKE_LOG |
| Priority | Category | Message | Note |
| error | IPSec | SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet | IPSec |
| error | IPSec | SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet | IPSec |
| info | IKE | [COOKIE] Invalid cookie, no sa found | IKE_LOG |
| Priority | Category | Message | Note |
| info | IKE | Recv:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN] | IKE_LOG |

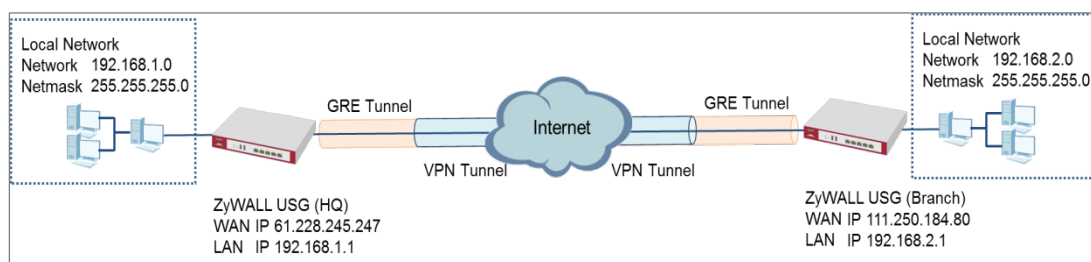
If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG Phase 2 Settings. Make sure your ZyWALL/USG Phase 2 Settings are supported in the MS Azure IKE Phase 2 setup list.

MONITOR > Log

| | | | | | |
|----|----------------|------|-----|--|---------|
| 19 | 2017-09-11 ... | info | IKE | [SA] : No proposal chosen | IKE_LOG |
| 20 | 2017-09-11 ... | info | IKE | [ID] : Tunnel [Server] Phase 2 Local policy mismatch | IKE_LOG |
| 31 | 2017-09-11 ... | info | IKE | Send:[HASH][SA][NONCE][ID][ID] | IKE_LOG |
| 32 | 2017-09-11 ... | info | IKE | Phase 1 IKE SA process done | IKE_LOG |

How to Configure GRE over IPsec VPN Tunnel

This example shows how to use the VPN Setup Wizard to create a GRE over IPsec VPN tunnel between ZyWALL/USG devices. The example instructs how to configure the VPN tunnel between each site. When the GRE over IPsec VPN tunnel is configured, each site can be accessed securely.



ZyWALL/USG GRE over IPsec VPN



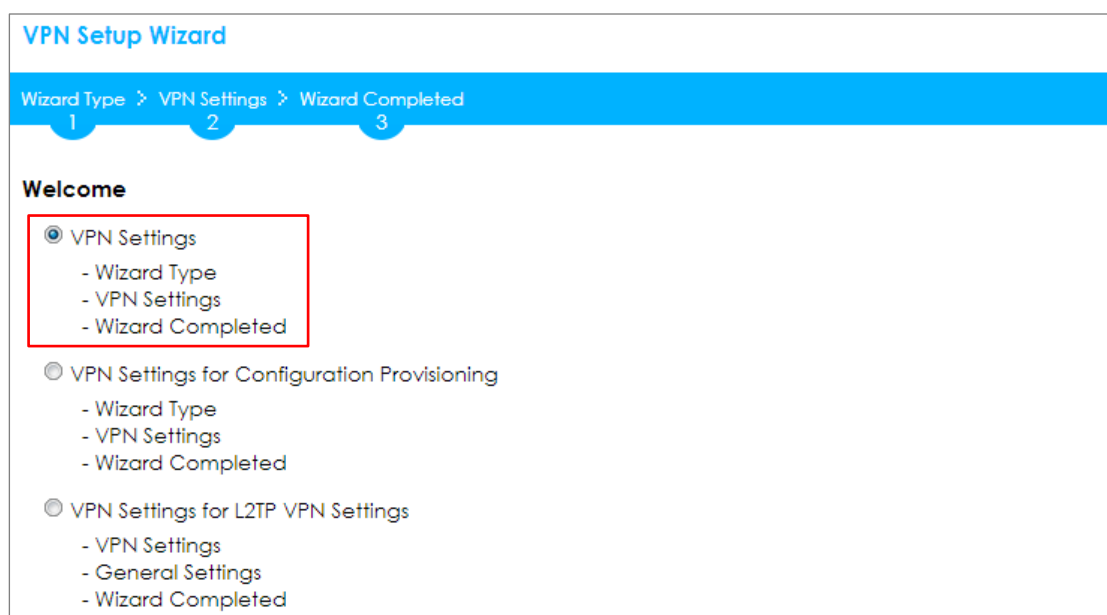
Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG110 (Firmware Version: ZLD 4.25) and ZyWALL 310 (Firmware Version: ZLD 4.25).

Set Up the ZyWALL/USG GRE over IPsec VPN Tunnel of Corporate Network (HQ)

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the FortiGate. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

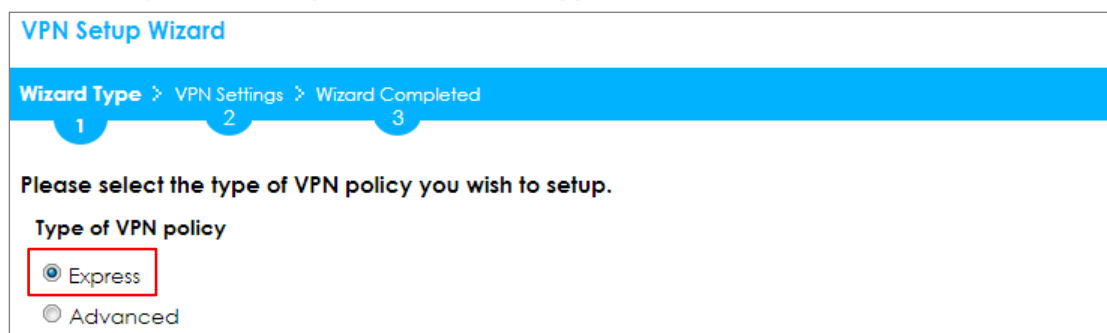
1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Please select the type of VPN policy you wish to setup.

Type of VPN policy

- ☒ Express
- ☐ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name: WIZ_VPN_HQ

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

Configure **Secure Gateway** IP as the Branch's WAN IP address (in the example, 111.250.184.80). Then, type a secure **Pre-Shared Key** (8-32 characters).

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG (HQ) and **Remote Policy** to be the IP address range of the network connected to the ZyWALL/USG (Branch).

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Express Settings

Configuration

Secure Gateway: 111.250.184.80 (IP or FQDN)

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.1.0 255.255.255.0

Remote Policy (IP/Mask): 192.168.2.0 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

**Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings
(Summary)**

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings
Summary
Rule Name: WIZ_VPN_HQ
Secure Gateway: 111.250.184.80
Pre-Shared Key: 12345678
Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask): 192.168.2.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings
Congratulations. The VPN Access wizard is completed
Summary
Rule Name: WIZ_VPN_HQ
Secure Gateway: 111.250.184.80
Pre-Shared Key: 12345678
Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask): 192.168.2.0 / 255.255.255.0

Go to **CONFIGURATION > VPN > IPsec VPN > VPN Gateway > Show Advanced Settings**. Configure **Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPsec router.

CONFIGURATION > VPN > IPsec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type

The screenshot shows the 'Authentication' section of the ZyXEL VPN Gateway configuration. The 'Pre-Shared Key' is selected. The 'Advance' section is expanded, showing 'Local ID Type' as 'IPv4', 'Content' as '0.0.0.0', and 'Peer ID Type' as 'Any' (highlighted with a red box). The 'Content' field for 'Peer ID Type' is empty.


Go to **CONFIGURATION > VPN > IPsec VPN > VPN Connection > Show Advanced Settings > Policy**. Select **Enable GRE over IPsec**.

CONFIGURATION > VPN > IPsec VPN > VPN Connection > Show Advanced Settings > Policy

The screenshot shows the 'Policy' section of the ZyXEL VPN Connection configuration. The 'Local policy' is 'WIZ_VPN_HQ_LOC' and the 'Remote policy' is 'WIZ_VPN_HQ_REM'. The 'Advance' section is expanded, showing 'Enable GRE over IPsec' checked (highlighted with a red box) and 'Policy Enforcement' unchecked.

The GRE tunnel runs between the IPsec public interface on the HQ unit and the Branch unit. Go to **CONFIGURATION > Network > Interface > Tunnel > Add**. Enter the **Interface Name** (The format is *tunnelx*, where x is 0 - 3.). Enter the **IP Address** and **Subnet Mask** for this interface. Specify **My Address** to be the interface or IP address to use as the source address for the packets this interface tunnels to the remote gateway. Enter **Remote Gateway Address** to be the IP address or domain name of the remote gateway to this tunnel traffic.

CONFIGURATION > Network > Interface > Tunnel > Add

| General Settings | | |
|--|---|---|
| <input checked="" type="checkbox"/> Enable | | |
| Interface Properties | | |
| Interface Name: | <input type="text" value="tunnel1"/> | |
| Zone: | <input type="text" value="TUNNEL"/> |  |
| Tunnel Mode: | <input type="text" value="GRE"/> | |
| IP Address Assignment | | |
| IP Address: | <input type="text" value="10.0.0.1"/> | |
| Subnet Mask: | <input type="text" value="255.255.255.0"/> | |
| Metric: | <input type="text" value="0"/> (0-15) | |
| Gateway Settings | | |
| My Address | | |
| <input checked="" type="radio"/> Interface | <input type="text" value="ge1"/> | Static -- 61.226.245.247/255.255.255.255 |
| <input type="radio"/> IP Address | <input type="text" value="0.0.0.0"/> | |
| Remote Gateway Address: | <input type="text" value="111.250.184.80"/> | |

Set Up the ZyWALL/USG GRE over IPsec VPN Tunnel of Corporate Network (Branch)

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the FortiGate. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Please select the type of VPN policy you wish to setup.

Type of VPN policy

- ☒ Express
- ☐ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1

2

3

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name:

WIZ_VPN_Branch

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

Configure **Secure Gateway** IP as the HQ's WAN IP address (in the example, 61.228.245.247). Then, type a secure **Pre-Shared Key** (8-32 characters).

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG (Branch) and **Remote Policy** to be the IP address range of the network connected to the ZyWALL/USG (HQ).

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1

2

3

Express Settings

Configuration

Secure Gateway:

61.228.245.247

(IP or FQDN)

Pre-Shared Key:

12345678

Local Policy (IP/Mask):

192.168.2.0

255.255.255.0

Remote Policy (IP/Mask):

192.168.1.0

255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings
Summary

| | |
|--------------------------|-----------------------------|
| Rule Name: | WIZ_VPN_Branch |
| Secure Gateway: | 61.228.245.247 |
| Pre-Shared Key: | 12345678 |
| Local Policy (IP/Mask): | 192.168.2.0 / 255.255.255.0 |
| Remote Policy (IP/Mask): | 192.168.1.0 / 255.255.255.0 |

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Congratulations. The VPN Access wizard is completed

Summary

| | |
|--------------------------|-----------------------------|
| Rule Name: | WIZ_VPN_Branch |
| Secure Gateway: | 61.228.245.247 |
| Pre-Shared Key: | 12345678 |
| Local Policy (IP/Mask): | 192.168.2.0 / 255.255.255.0 |
| Remote Policy (IP/Mask): | 192.168.1.0 / 255.255.255.0 |

Go to **CONFIGURATION > VPN > IPsec VPN > VPN Gateway > Show Advanced Settings**. Configure **Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPsec router.

CONFIGURATION > VPN > IPsec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type

The screenshot shows the 'Authentication' section of the ZyXEL VPN Gateway configuration. The 'Pre-Shared Key' is selected. Under the 'Advance' section, 'Local ID Type' is set to 'IPv4', 'Content' is '0.0.0.0', and 'Peer ID Type' is set to 'Any' (highlighted with a red box). The 'Content' field for 'Peer ID Type' is empty.

Go to **CONFIGURATION > VPN > IPsec VPN > VPN Connection > Show Advanced Settings > Policy**. Select **Enable GRE over IPsec**.

CONFIGURATION > VPN > IPsec VPN > VPN Connection > Show Advanced Settings > Policy

The screenshot shows the 'Policy' section of the ZyXEL VPN Connection configuration. 'Local policy' is 'WIZ_VPN_Branch_L' and 'Remote policy' is 'WIZ_VPN_Branch_f'. Under the 'Advance' section, 'Enable GRE over IPsec' is checked (highlighted with a red box), and 'Policy Enforcement' is unchecked.

The GRE tunnel runs between the IPsec public interface on the Branch unit and the HQ unit. Go to **CONFIGURATION > Network > Interface > Tunnel > Add**. Enter the **Interface Name** (The format is *tunnelx*, where x is 0 - 3.). Enter the **IP Address** and **Subnet Mask** for this interface. Specify **My Address** to be the interface or IP address to use as the source address for the packets this interface tunnels to the remote gateway. Enter **Remote Gateway Address** to be the IP address or domain name of the remote gateway to this tunnel traffic.

CONFIGURATION > Network > Interface > Tunnel > Add

General Settings

☒ Enable

Interface Properties

Interface Name:

Zone:

Tunnel Mode:

IP Address Assignment

IP Address:

Subnet Mask:

Metric: (0-15)

Gateway Settings

My Address

☒ Interface Static -- 111.250.184.80/255.255.255.255
☐ IP Address
 Remote Gateway Address:

Test the GRE over IPSec VPN Tunnel

Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

| IPv4 Configuration | | | | |
|--|--------|------------|-------------|--------------------------------------|
| Add Edit Remove Activate Inactivate Connect Disconnect Object References | | | | |
| # | Status | Name | VPN Gateway | Gateway IP Version |
| 1 | | WIZ_VPN_HQ | WIZ_VPN_HQ | IPv4 |
| | | | | WIZ_VPN_HQ_LOCAL/... |
| Page 1 of 1 Show 50 items | | | | |
| Displaying 1 - 1 of 1 | | | | |

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and **Inbound (Bytes)/Outbound (Bytes)** Traffic.

MONITOR > VPN Monitor > IPSec

| Disconnect | | Connection Check | | | | | |
|-------------|------------|--------------------------------|----------------|-----------------------|---------|---------------|----------------|
| # | Name | Policy | My Address | Secure Gateway | Timeout | Inbound(Byte) | Outbound(Byte) |
| 1 | WIZ_VPN_HQ | 192.168.1.0/24<>192.168.2.0/24 | 61.225.245.247 | P: 111.250.184.80 | 86360 | 0(0 bytes) | 0(0 bytes) |
| Page 1 of 1 | | Show 50 items | | Displaying 1 - 1 of 1 | | | |

What Could Go Wrong?

If you see below [info] or [error] log message, please check ZyWALL/USG Phase 1 Settings. Make sure your ZyWALL/USG Phase 1 Settings are supported in the Amazon VPC IKE Phase 1 setup list.

MONITOR > Log

| Priority | Category | Message | Note |
|----------|----------|--|---------|
| info | IKE | Recv:[NOTIFY:INVALID_COOKIE] | IKE_LOG |
| info | IKE | Send:[ID][HASH][NOTIFY:INITIAL_CONTACT] | IKE_LOG |
| Priority | Category | Message | Note |
| error | IPSec | SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet | IPSec |
| error | IPSec | SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet | IPSec |
| info | IKE | [COOKIE] Invalid cookie, no sa found | IKE_LOG |
| Priority | Category | Message | Note |
| info | IKE | Recv:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN] | IKE_LOG |

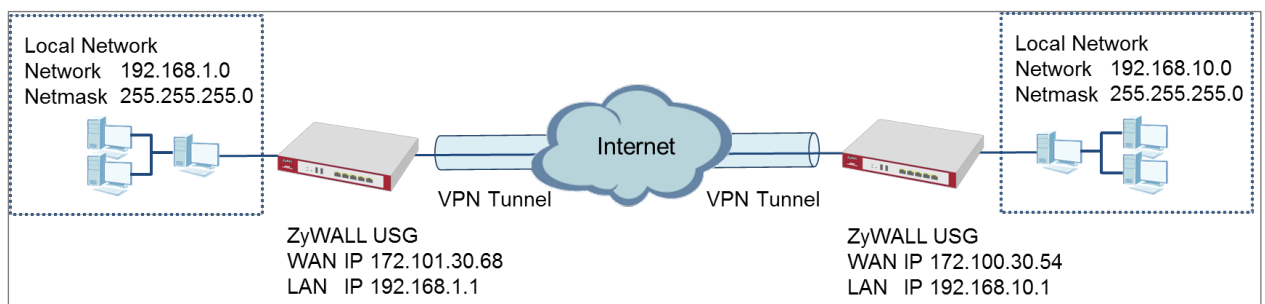
If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG Phase 2 Settings. Make sure your ZyWALL/USG Phase 2 Settings are supported in the Amazon VPC IKE Phase 2 setup list.

MONITOR > Log


| | | | | | |
|----|----------------|------|-----|--|---------|
| 19 | 2017-09-11 ... | info | IKE | [SA] : No proposal chosen | IKE_LOG |
| 20 | 2017-09-11 ... | info | IKE | [ID] : Tunnel [Server] Phase 2 Local policy mismatch | IKE_LOG |
| 31 | 2017-09-11 ... | info | IKE | Send:[HASH][SA][NONCE][ID][ID] | IKE_LOG |
| 32 | 2017-09-11 ... | info | IKE | Phase 1 IKE SA process done | IKE_LOG |

How to Configure Site-to-site IPSec VPN Where the Peer has a Static IP Address

This example shows how to use the VPN Setup Wizard to create a site-to-site VPN with the Peer has a Static IP Address. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



ZyWALL Site-to-site IPSec VPN with a Static IP Address Peer

 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the ZyWALL/USG IPSec VPN Tunnel of Corporate Network (HQ) In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
1 2 3

Welcome

☒ VPN Settings

- Wizard Type
- VPN Settings
- Wizard Completed

☐ VPN Settings for Configuration Provisioning

- Wizard Type
- VPN Settings
- Wizard Completed

☐ VPN Settings for L2TP VPN Settings

- VPN Settings
- General Settings
- Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
1 2 3

Please select the type of VPN policy you wish to setup.

Type of VPN policy

☒ Express

☐ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway).
 You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

123

Express Settings

IKE Version

☒ IKEv1
☐ IKEv2

Scenario

Rule Name:

☒ Site-to-site
☐ Site-to-site with Dynamic Peer
☐ Remote Access (Server Role)
☐ Remote Access (Client Role)

Configure **Secure Gateway** IP as the peer ZyWALL/USG's WAN IP address (in the example, 172.100.30.54). Type a secure **Pre-Shared Key** (8-32 characters).

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the peer ZyWALL/USG.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Configuration

Secure Gateway: 172.100.30.54 (IP or FQDN)

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Summary

Rule Name: WIZ_VPN_HQ

Secure Gateway: 172.100.30.54

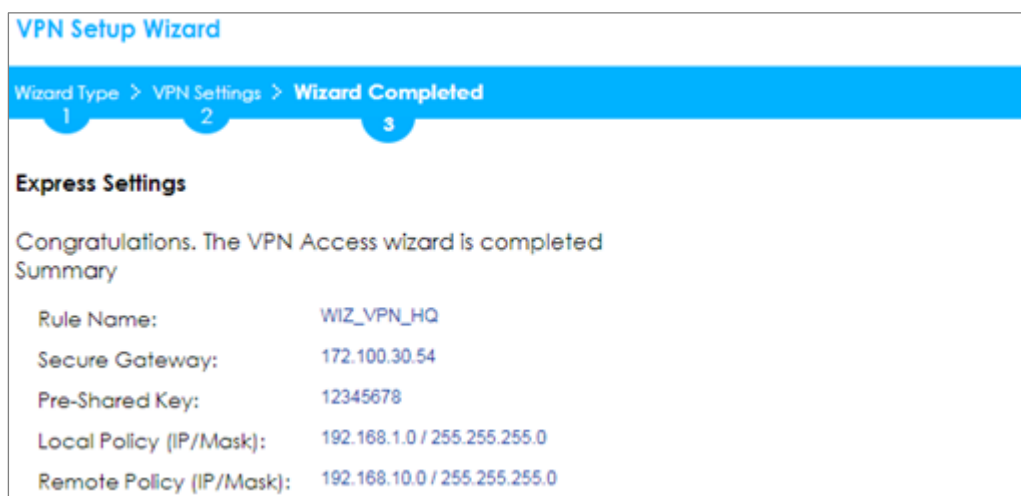
Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed



VPN Setup Wizard

Wizard Type > VPN Settings > **Wizard Completed**

Express Settings

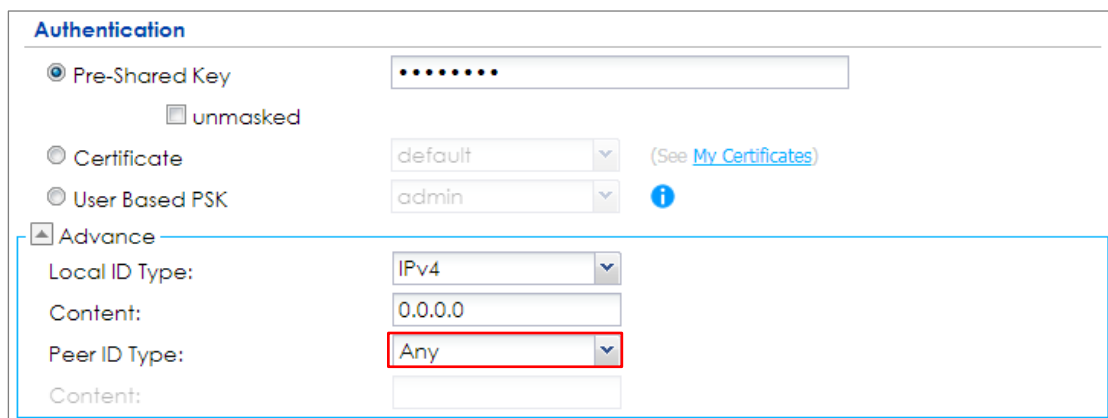
Congratulations. The VPN Access wizard is completed

Summary

| | |
|--------------------------|------------------------------|
| Rule Name: | WIZ_VPN_HQ |
| Secure Gateway: | 172.100.30.54 |
| Pre-Shared Key: | 12345678 |
| Local Policy (IP/Mask): | 192.168.1.0 / 255.255.255.0 |
| Remote Policy (IP/Mask): | 192.168.10.0 / 255.255.255.0 |

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** and click **Show Advanced Settings**. Configure **Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPSec router.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type



Authentication

☒ Pre-Shared Key ☐ unmasked

☐ Certificate (See [My Certificates](#))

☐ User Based PSK [i](#)

☒ **Advance**

Local ID Type:

Content:

Peer ID Type: (highlighted with a red box)

Content:

Set Up the ZyWALL/USG IPSec VPN Tunnel of Corporate Network (Branch)

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
1 2 3

Welcome

☒ VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

☐ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

☐ VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and to use a pre-shared key. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Please select the type of VPN policy you wish to setup.

Type of VPN policy

☒ Express

☐ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name: WIZ_VPN_Branch

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

Configure **Secure Gateway** IP as the peer ZyWALL/USG's WAN IP address (in the example, 172.101.30.68). Type a secure **Pre-Shared Key** (8-32 characters).

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the peer ZYWALL/USG.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Configuration

Secure Gateway: 172.101.30.68 (IP or FQDN)

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Summary

Rule Name: WIZ_VPN_Branch

Secure Gateway: 172.101.30.68

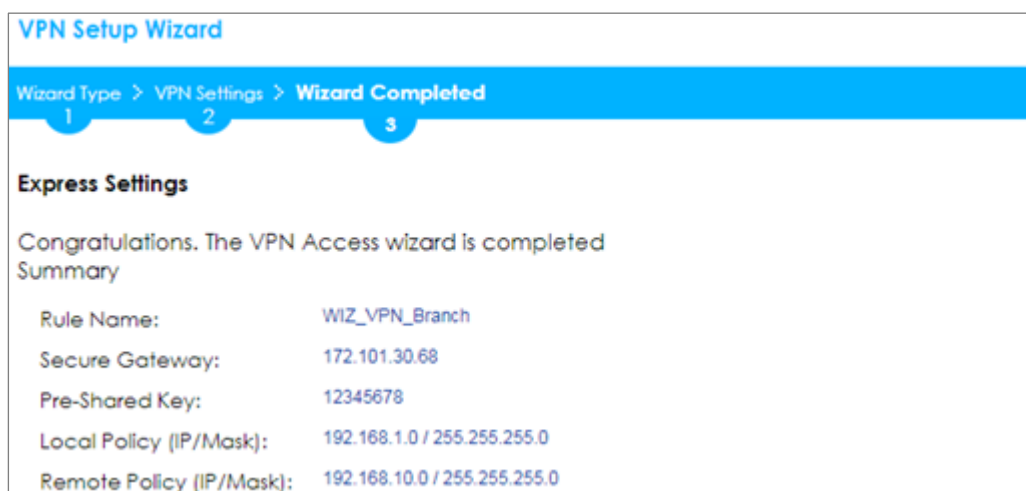
Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Express Settings

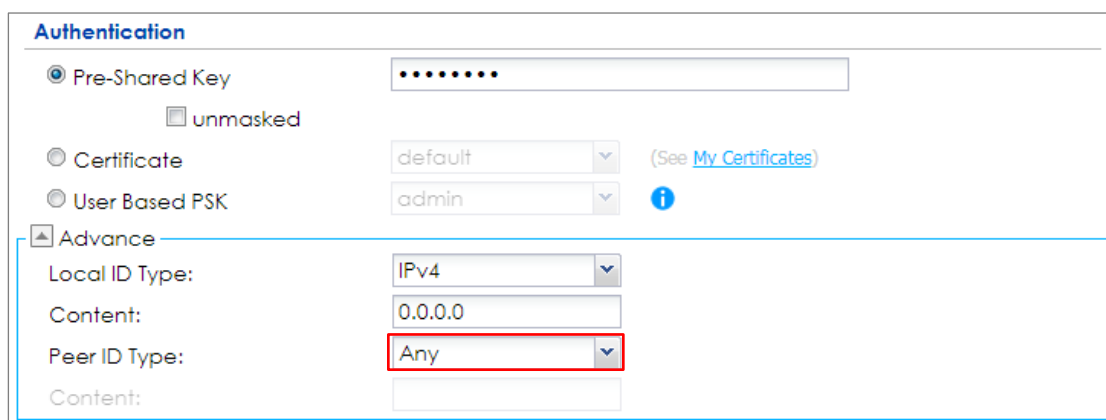
Congratulations. The VPN Access wizard is completed

Summary

| | |
|--------------------------|------------------------------|
| Rule Name: | WIZ_VPN_Branch |
| Secure Gateway: | 172.101.30.68 |
| Pre-Shared Key: | 12345678 |
| Local Policy (IP/Mask): | 192.168.1.0 / 255.255.255.0 |
| Remote Policy (IP/Mask): | 192.168.10.0 / 255.255.255.0 |

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** and click **Show Advanced Settings**. Configure **Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPSec router.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type



Authentication

☒ Pre-Shared Key ☐ unmasked

☐ Certificate (See [My Certificates](#))

☐ User Based PSK [i](#)

☒ Advance

Local ID Type:

Content:

Peer ID Type: [i](#)

Content:

Test the IPSec VPN Tunnel

Go to ZYWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

| Add Edit Remove Activate Inactivate Connect Disconnect Object References | | | | | |
|--|--------|--------------|--------------|--------------------|--|
| # | Status | Name | VPN Gateway | Gateway IP Version | Policy |
| 1 | | VPN_to_Azure | VPN_to_Azure | IPv4 | WIZ_VPN_HQ_LOCAL / WIZ_VPN_HQ_REMOTE |
| << Page 1 of 1 >> Show 50 items | | | | | |
| Displaying 1 - 1 of 1 | | | | | |

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and **Inbound(Bytes)/Outbound(Bytes)** Traffic.

MONITOR > VPN Monitor > IPSec

| Disconnect | | Connection Check | | | | | | |
|---------------------------------|--------------------|----------------------------------|---------------|------------------|---------|---------|------------|------------|
| # | Name | Policy | My Address | Secure Gateway | Up Time | Timeout | Inbound... | Outbou... |
| 1 | Hub_HQ-to-Branch_A | 192.168.1.0/24<>192.168.10.0/24 | 172.101.30.68 | P: 172.100.30.54 | 101 | 86319 | 0(0 bytes) | 0(0 bytes) |
| << Page 1 of 1 >> Show 50 items | | | | | | | | |
| Displaying 1 - 1 of 1 | | | | | | | | |

To test whether or not a tunnel is working, ping from a computer at one site to a computer at the other. Ensure that both computers have Internet access (via the IPSec devices).

PC at HQ Office > Window 7 > cmd > ping 192.168.10.33

```
C:\Documents and Settings\ZYXEL>ping 192.168.10.33

Pinging 192.168.10.33 with 32 bytes of data:

Reply from 192.168.10.33: bytes=32 time=18ms TTL=54
Reply from 192.168.10.33: bytes=32 time=17ms TTL=54
Reply from 192.168.10.33: bytes=32 time=17ms TTL=54
Reply from 192.168.10.33: bytes=32 time=16ms TTL=54

Ping statistics for 192.168.10.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 18ms, Average = 17ms
```

PC at Branch Office > Window 7 > cmd > ping 192.168.1.33

```
C:\Documents and Settings\ZYXEL>ping 192.168.1.33

Pinging 192.168.1.33 with 32 bytes of data:

Reply from 192.168.1.33: bytes=32 time=27ms TTL=43
Reply from 192.168.1.33: bytes=32 time=32ms TTL=43
Reply from 192.168.1.33: bytes=32 time=26ms TTL=43
Reply from 192.168.1.33: bytes=32 time=27ms TTL=43

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 32ms, Average = 28ms
```

What Could Go Wrong?

If you see below [info] or [error] log message, please check ZyWALL/USG Phase 1 Settings. Both ZyWALL/USG at the HQ and Branch sites must use the same Pre-Shared Key, Encryption, Authentication method, DH key group and ID Type to establish the IKE SA.

MONITOR > Log

| Priority | Category | Message | Note |
|----------|----------|--|---------|
| info | IKE | Recv:[NOTIFY:INVALID_COOKIE] | IKE_LOG |
| info | IKE | Send:[ID][HASH][NOTIFY:INITIAL_CONTACT] | IKE_LOG |
| Priority | Category | Message | Note |
| error | IPSec | SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet | IPSec |
| error | IPSec | SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet | IPSec |
| info | IKE | [COOKIE] Invalid cookie, no sa found | IKE_LOG |
| Priority | Category | Message | Note |
| info | IKE | Recv:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN] | IKE_LOG |

If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG Phase 2 Settings. Both ZyWALL/USG at the HQ and Branch sites must use the same Protocol, Encapsulation, Encryption, Authentication method and PFS to establish the IKE SA.

MONITOR > Log

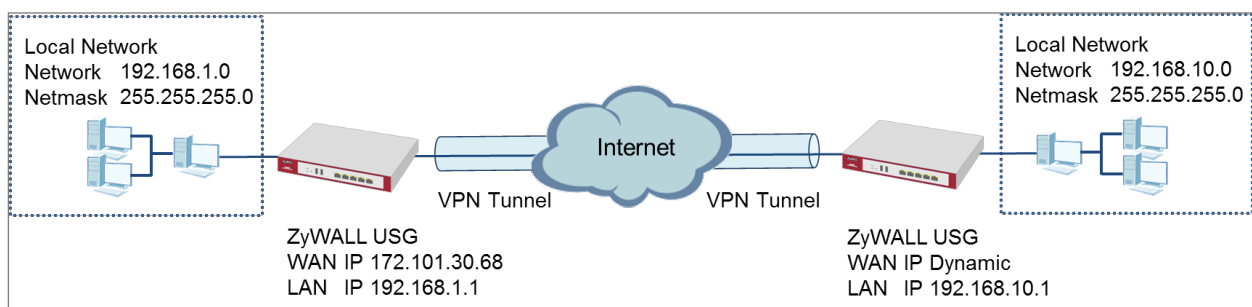
| | | | | | |
|----|----------------|------|-----|--|---------|
| 19 | 2017-09-11 ... | info | IKE | [SA] : No proposal chosen | IKE_LOG |
| 20 | 2017-09-11 ... | info | IKE | [ID] : Tunnel [Server] Phase 2 Local policy mismatch | IKE_LOG |
| 31 | 2017-09-11 ... | info | IKE | Send:[HASH][SA][NONCE][ID][ID] | IKE_LOG |
| 32 | 2017-09-11 ... | info | IKE | Phase 1 IKE SA process done | IKE_LOG |

Make sure the both ZyWALL/USG at the HQ and Branch sites security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.


Default NAT traversal is enable on ZyWALL/USG, please make sure the remote IPSec device must also have NAT traversal enabled.

How to Configure Site-to-site IPSec VPN Where the Peer has a Dynamic IP Address

This example shows how to use the VPN Setup Wizard to create a site-to-site VPN with the Peer has a Dynamic IP Address. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



ZyWALL Site-to-site IPSec VPN with a Dynamic IP Address Peer

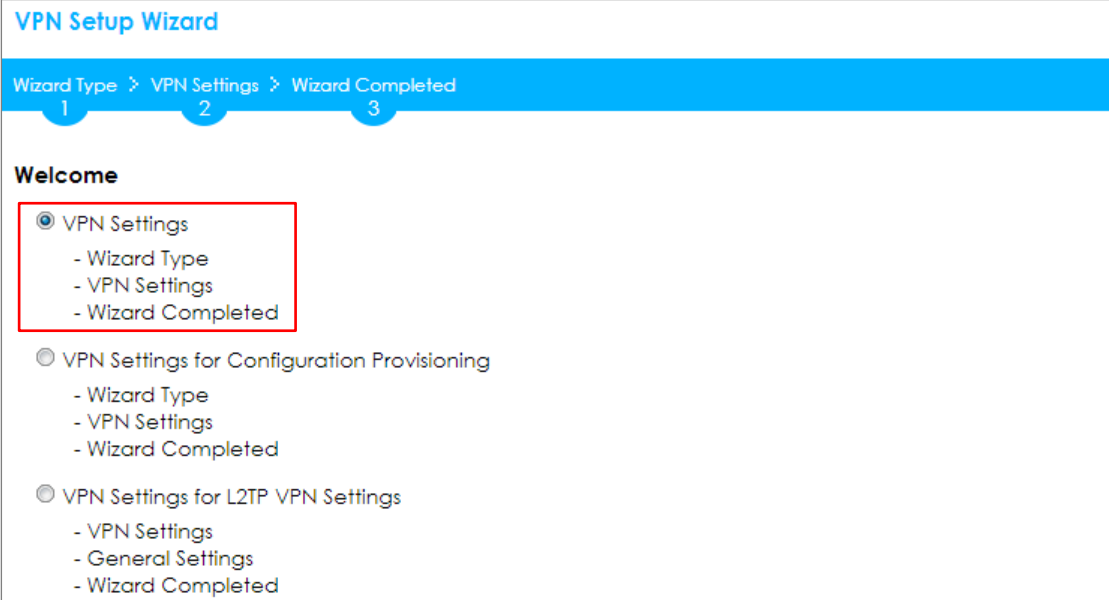
 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the ZyWALL/USG IPSec VPN Tunnel of Corporate Network

(HQ)

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Please select the type of VPN policy you wish to setup.

Type of VPN policy

☒ Express

☐ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway).
 You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site with Dynamic Peer**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name:

☐ Site-to-site

☒ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

Type a secure **Pre-Shared Key** (8-32 characters). Then, set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the peer ZYWALL/USG.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Configuration

Secure Gateway: Any

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Summary)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Summary

Rule Name: WIZ_VPN_HQ

Secure Gateway: Any

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings > Wizard completed

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Congratulations. The VPN Access wizard is completed

Summary

| | |
|--------------------------|------------------------------|
| Rule Name: | WIZ_VPN_HQ |
| Secure Gateway: | Any |
| Pre-Shared Key: | 12345678 |
| Local Policy (IP/Mask): | 192.168.1.0 / 255.255.255.0 |
| Remote Policy (IP/Mask): | 192.168.10.0 / 255.255.255.0 |

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** and click **Show Advanced Settings**. Configure **Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPSec router.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type

Authentication

☒ Pre-Shared Key

.....

☐ unmasked

☐ Certificate

default

(See [My Certificates](#))

☐ User Based PSK

admin

i

☐ Advance

Local ID Type:

IPv4

Content:

0.0.0.0

Peer ID Type:

Any

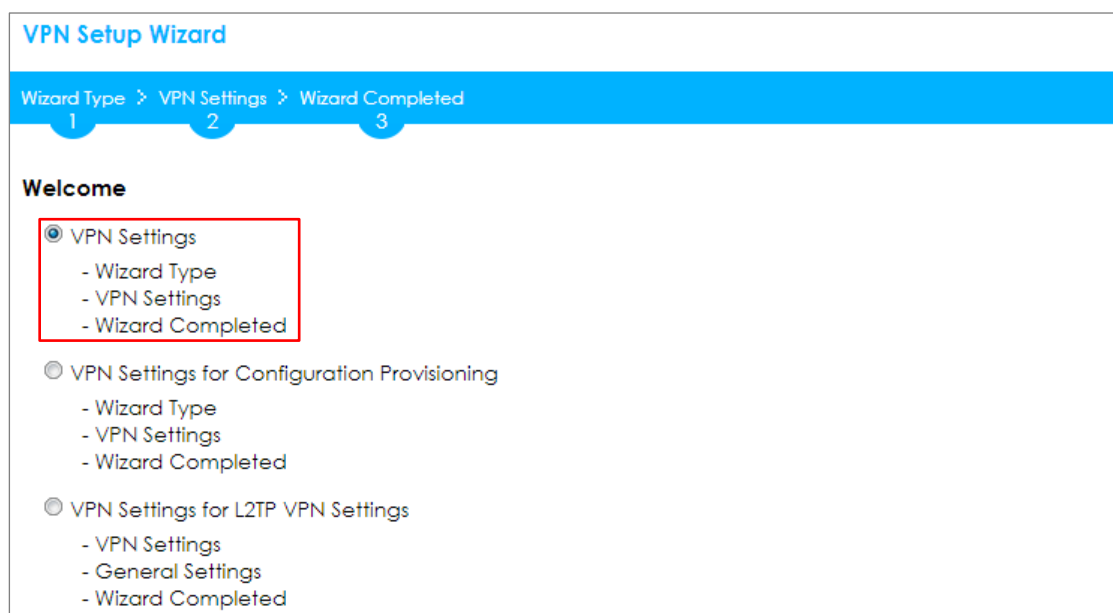
Content:

Set Up the ZyWALL/USG IPSec VPN Tunnel of Corporate Network

(Branch has a Dynamic IP Address)

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** to create a **Site-to-site VPN** Rule Name.

Quick Setup > VPN Setup Wizard > Welcome
Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
 1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and to use a pre-shared key. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Please select the type of VPN policy you wish to setup.

Type of VPN policy

☒ Express

☐ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name: WIZ_VPN_Branch_Dynamic

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

Configure **Secure Gateway** IP as the peer ZyWALL/USG's WAN IP address (in the example, 172.101.30.68). Type a secure **Pre-Shared Key** (8-32 characters).

Set **Local Policy** to be the ZyWALL/USG local IP address that can use the VPN tunnel and set **Remote Policy** to the peer ZyWALL/USG local IP address that can use the VPN tunnel. Click **OK**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Configuration

Secure Gateway: 172.101.30.68 (IP or FQDN)

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Summary

Rule Name: WIZ_VPN_Branch_Dynamic

Secure Gateway: 172.101.30.68

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Congratulations. The VPN Access wizard is completed

Summary

| | |
|--------------------------|-------------------------|
| Rule Name: | WIZ_VPN_Branch_Dynamic |
| Secure Gateway: | 172.101.30.68 |
| Pre-Shared Key: | 12345678 |
| Local Policy (IP/Mask): | 0.0.0.0 / 255.255.255.0 |
| Remote Policy (IP/Mask): | Any |

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** and click **Show Advanced Settings**. Configure **Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPSec router.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type

Authentication

☒ Pre-Shared Key

.....

☐ unmasked

☐ Certificate

default

(See [My Certificates](#))

☐ User Based PSK

admin

i

☒ Advance

Local ID Type:

IPv4

Content:

0.0.0.0

Peer ID Type:

Any

Content:

Test the IPSec VPN Tunnel

The Site-to-site VPN with Dynamic Peer can only initiate the VPN tunnel from the peer has a dynamic IP Address. Go to **CONFIGURATION > VPN > IPSec VPN > VPN**

Connection, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

| Add Edit Remove Activate Inactivate Connect Disconnect Object References | | | | | |
|--|--------|----------------|------------------|--------------------|---|
| # | Status | Name | VPN Gateway | Gateway IP Version | Policy |
| 1 | | WIZ_VPN_Bra... | WIZ_VPN_Branc... | IPv4 | WIZ_VPN_Branch_Dynamic_LOCAL / WIZ_VPN_Branch_Dyna... |
| Page 1 of 1 Show 50 items | | | | | Displaying 1 - 1 of 1 |

Go to **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and **Inbound(Bytes)/Outbound(Bytes)** Traffic.

MONITOR > VPN Monitor > IPSec

| Disconnect Connection Check | | | | | | | | |
|---|------------------------|---------------------|---------------|------------------|-----------------------|---------|---------------|--------------|
| # | Name | Policy | My Address | Secure Gateway | Up Time | Timeout | Inbound(By... | Outbound(... |
| 1 | WIZ_VPN_Branch_Dynamic | 192.168.1.0/24<>... | 172.101.30.68 | D: 172.100.30.54 | 18 | 86402 | 0(0 bytes) | 0(0 bytes) |
| Page 1 of 1 Show 50 items | | | | | Displaying 1 - 1 of 1 | | | |

To test whether or not a tunnel is working, ping from a computer at one site to a computer at the other. Ensure that both computers have Internet access (via the IPSec devices).

PC at HQ Office > Window 7 > cmd > ping 192.168.10.33

```
C:\Documents and Settings\ZyXEL>ping 192.168.1.33

Pinging 192.168.1.33 with 32 bytes of data:

Reply from 192.168.1.33: bytes=32 time=27ms TTL=43
Reply from 192.168.1.33: bytes=32 time=32ms TTL=43
Reply from 192.168.1.33: bytes=32 time=26ms TTL=43
Reply from 192.168.1.33: bytes=32 time=27ms TTL=43

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 32ms, Average = 28ms
```

PC at Branch Office > Window 7 > cmd > ping 192.168.1.33


```
C:\Documents and Settings\ZyXEL>ping 192.168.10.33

Pinging 192.168.10.33 with 32 bytes of data:

Reply from 192.168.10.33: bytes=32 time=18ms TTL=54
Reply from 192.168.10.33: bytes=32 time=17ms TTL=54
Reply from 192.168.10.33: bytes=32 time=17ms TTL=54
Reply from 192.168.10.33: bytes=32 time=16ms TTL=54

Ping statistics for 192.168.10.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 18ms, Average = 17ms
```

What Could Go Wrong?

If you see below [info] or [error] log message, please check ZyWALL/USG Phase 1 Settings. Both ZyWALL/USG at the HQ and Branch sites must use the same Pre-Shared Key, Encryption, Authentication method, DH key group and ID Type to establish the IKE SA.

MONITOR > Log

| Priority | Category | Message | Note |
|----------|----------|--|---------|
| info | IKE | Recv:[NOTIFY:INVALID_COOKIE] | IKE_LOG |
| info | IKE | Send:[ID][HASH][NOTIFY:INITIAL_CONTACT] | IKE_LOG |
| Priority | Category | Message | Note |
| error | IPSec | SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet | IPSec |
| error | IPSec | SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet | IPSec |
| info | IKE | [COOKIE] Invalid cookie, no sa found | IKE_LOG |
| Priority | Category | Message | Note |
| info | IKE | Recv:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN] | IKE_LOG |

If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG Phase 2 Settings. Both ZyWALL/USG at the HQ and Branch sites must use the same Protocol, Encapsulation, Encryption, Authentication method and PFS to establish the IKE SA.

MONITOR > Log

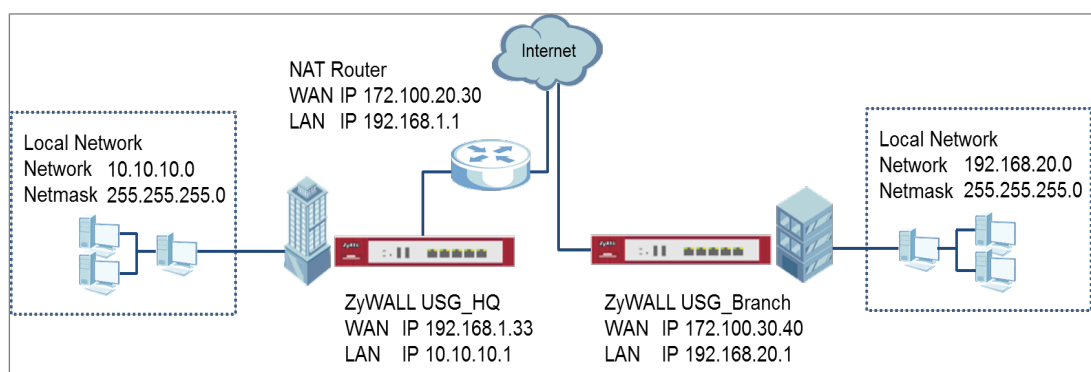
| | | | | | |
|----|----------------|------|-----|--|---------|
| 19 | 2017-09-11 ... | info | IKE | [SA] : No proposal chosen | IKE_LOG |
| 20 | 2017-09-11 ... | info | IKE | [ID] : Tunnel [Server] Phase 2 Local policy mismatch | IKE_LOG |
| 31 | 2017-09-11 ... | info | IKE | Send:[HASH][SA][NONCE][ID][ID] | IKE_LOG |
| 32 | 2017-09-11 ... | info | IKE | Phase 1 IKE SA process done | IKE_LOG |

Make sure the both ZyWALL/USG at the HQ and Branch sites security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

Default NAT traversal is enable on ZyWALL/USG, please make sure the remote IPSec device must also have NAT traversal enabled.

How to Configure IPsec Site to Site VPN while one Site is behind a NAT router

This example shows how to use the VPN Setup Wizard to create a IPsec Site to Site VPN tunnel between ZyWALL/USG devices. The example instructs how to configure the VPN tunnel between each site while one Site is behind a NAT router. When the IPsec Site to Site VPN tunnel is configured, each site can be accessed securely.



ZyWALL/USG Site to Site VPN while one Site is behind a NAT router

Note:

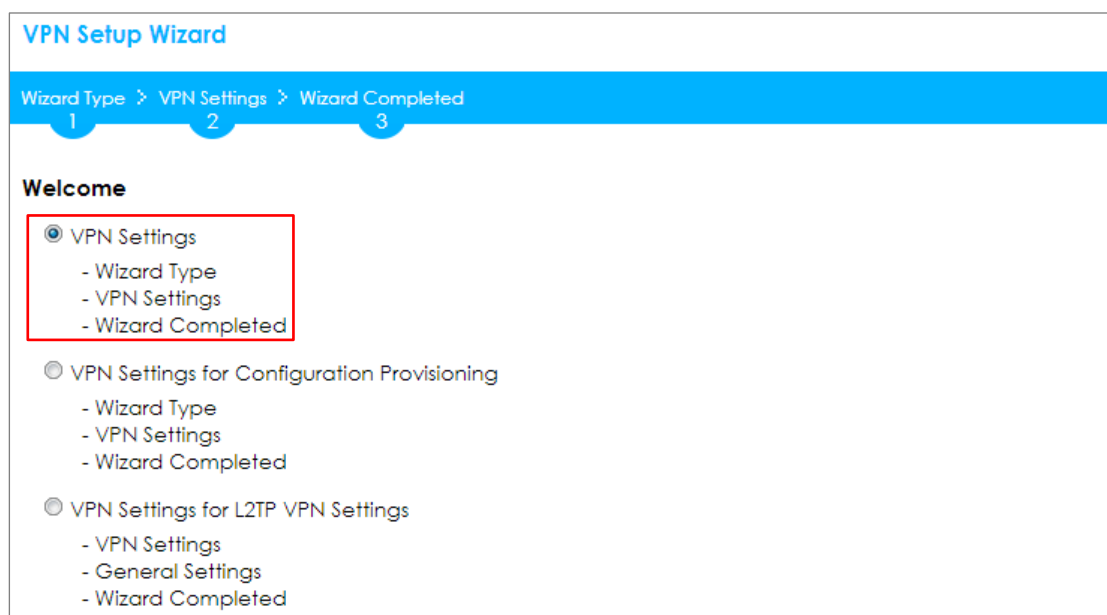
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG110 (Firmware Version: ZLD 4.25) and ZyWALL 310 (Firmware Version: ZLD 4.25).

Set Up the ZyWALL/USG IPsec VPN Tunnel of Corporate

Network (HQ)

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the FortiGate. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

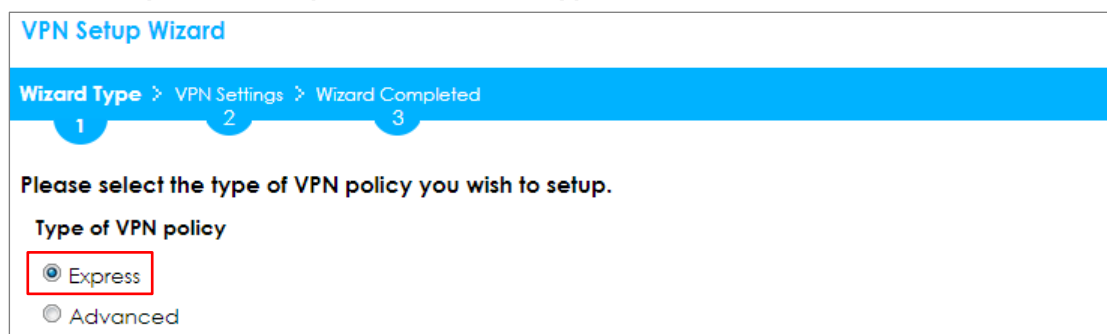
1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Please select the type of VPN policy you wish to setup.

Type of VPN policy

- ☒ Express
- ☐ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name: WIZ_VPN_HQ

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

Configure **Secure Gateway** IP as the Branch's WAN IP address (in the example, 172.100.30.40). Then, type a secure **Pre-Shared Key** (8-32 characters).

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG (HQ) and **Remote Policy** to be the IP address range of the network connected to the ZyWALL/USG (Branch).

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

Configuration

Secure Gateway: 172.101.30.40 (IP or FQDN)

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 10.10.10.0 255.255.255.0

Remote Policy (IP/Mask): 192.168.20.0 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Summary

| | |
|--------------------------|------------------------------|
| Rule Name: | WIZ_VPN_HQ |
| Secure Gateway: | 172.100.30.40 |
| Pre-Shared Key: | 12345678 |
| Local Policy (IP/Mask): | 10.10.10.0 / 255.255.255.0 |
| Remote Policy (IP/Mask): | 192.168.20.0 / 255.255.255.0 |

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Congratulations. The VPN Access wizard is completed

Summary

| | |
|--------------------------|------------------------------|
| Rule Name: | WIZ_VPN_HQ |
| Secure Gateway: | 172.100.30.40 |
| Pre-Shared Key: | 12345678 |
| Local Policy (IP/Mask): | 10.10.10.0 / 255.255.255.0 |
| Remote Policy (IP/Mask): | 192.168.20.0 / 255.255.255.0 |

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings**. Configure **Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPSec router.

**CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced
Settings > Authentication > Peer ID Type**

Authentication

☒ Pre-Shared Key

.....

☐ unmasked

☐ Certificate

default

(See [My Certificates](#))

☐ User Based PSK

admin

☒ Advance

Local ID Type:

IPv4

Content:

0.0.0.0

Peer ID Type:

Any

Content:

Set Up the ZyWALL/USG IPSec VPN Tunnel of Corporate Network (Branch)

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the FortiGate. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Welcome

☒ VPN Settings

- Wizard Type
- VPN Settings
- Wizard Completed

☐ VPN Settings for Configuration Provisioning

- Wizard Type
- VPN Settings
- Wizard Completed

☐ VPN Settings for L2TP VPN Settings

- VPN Settings
- General Settings
- Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Please select the type of VPN policy you wish to setup.

Type of VPN policy

☒ Express

☐ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name: WIZ_VPN_Branch

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

Configure **Secure Gateway** IP as the Branch's WAN IP address (in the example, 172.100.20.30). Then, type a secure **Pre-Shared Key** (8-32 characters).

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG (HQ) and **Remote Policy** to be the IP address range of the network connected to the ZyWALL/USG (Branch).

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Configuration

Secure Gateway: 172.100.20.30 (IP or FQDN)

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.20.0 255.255.255.0

Remote Policy (IP/Mask): 10.10.10.0 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Summary

| | |
|--------------------------|------------------------------|
| Rule Name: | WIZ_VPN_Branch |
| Secure Gateway: | 172.100.20.30 |
| Pre-Shared Key: | 12345678 |
| Local Policy (IP/Mask): | 192.168.20.0 / 255.255.255.0 |
| Remote Policy (IP/Mask): | 10.10.10.0 / 255.255.255.0 |

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPsec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPsec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Congratulations. The VPN Access wizard is completed

Summary

| | |
|--------------------------|------------------------------|
| Rule Name: | WIZ_VPN_Branch |
| Secure Gateway: | 172.100.20.30 |
| Pre-Shared Key: | 12345678 |
| Local Policy (IP/Mask): | 192.168.20.0 / 255.255.255.0 |
| Remote Policy (IP/Mask): | 10.10.10.0 / 255.255.255.0 |

Go to **CONFIGURATION > VPN > IPsec VPN > VPN Gateway > Show Advanced Settings**. Configure **Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPsec router.

**CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced
Settings > Authentication > Peer ID Type**

Authentication

☒ Pre-Shared Key

☐ unmasked

☐ Certificate
 (See [My Certificates](#))

☐ User Based PSK
 ⓘ

☒ Advance

Local ID Type:

 Content:

 Peer ID Type:

 Content:

Set Up the NAT Router (Using ZyWALL USG device in this example)

Go to **CONFIGURATION > Network > NAT > Add**. Select the **Incoming Interface** on which packets for the NAT rule must be received. Specified the **User-**

Defined **Original IP** field and Type the translated destination IP address that this NAT rule supports.

CONFIGURATION > Network > NAT > Add

| General Settings | |
|---|--|
| <input checked="" type="checkbox"/> Enable Rule | |
| Rule Name: | VPN_NAT |
| Port Mapping Type | |
| Classification: | <input type="radio"/> Virtual Server <input checked="" type="radio"/> 1:1 NAT <input type="radio"/> Many 1:1 NAT |
| Mapping Rule | |
| Incoming Interface: | ge1 |
| Original IP: | User Defined |
| User-Defined Original IP: | 172.100.20.30 (IP Address) |
| Mapped IP: | User Defined |
| User-Defined Mapped IP: | 192.168.1.33 (IP Address) |
| Port Mapping Type: | any |

Go to **CONFIGURATION > Security Policy > Policy Control**. IP forwarding must be enabled at the firewall for the following IP protocols and UDP ports:

IP protocol = 50 → Used by data path (ESP)

IP protocol = 51 → Used by data path (AH)

UDP Port Number = 500 → Used by IKE (IPSec control path)

UDP Port Number = 4500 → Used by NAT-T (IPsec NAT traversal)

CONFIGURATION > Security Policy > Policy Control

General Settings

☒ Enable Policy Control

IPv4 Configuration

☐ Allow Asymmetrical Route

[Add](#)
[Edit](#)
[Remove](#)
[Activate](#)
[Inactivate](#)
[Move](#)
[Clone](#)

| Pri... | St... | Name | From | To | IPv4 Sou... | IPv4 Des... | Service | User | Schedule |
|--------|-------|-----------------|--------------------------|---------------------|-------------|-------------|---|------|----------|
| 1 | | LAN_Outgoing | LAN | any (Exc... | any | any | any | any | none |
| 2 | | DMZ_to_WAN | DMZ | WAN | any | any | any | any | none |
| 3 | | IPSec_VPN_Ou... | IPSec... | any (Exc... | any | any | any | any | none |
| 4 | | SSL_VPN_Outg... | SSL_VPN | any (Exc... | any | any | any | any | none |
| 5 | | TUNNEL_Outg... | TUNNEL | any (Exc... | any | any | any | any | none |
| 6 | | LAN_to_Device | LAN | ZyWALL | any | any | any | any | none |
| 7 | | DMZ_to_Device | DMZ | ZyWALL | any | any | Default_Allow_DMZ_To_ZyWALL | any | none |
| 8 | | WAN_to_Device | WAN | ZyWALL | any | any | Default_Allow_WAN_To_ZyWALL | any | none |
| 9 | | IPSec_VPN_to... | IPSec... | ZyWALL | any | any | any | any | none |
| 10 | | SSL_VPN_to_D... | SSL_VPN | ZyWALL | any | any | any | any | none |
| 11 | | TUNNEL_to_De... | TUNNEL | ZyWALL | any | any | any | any | none |
| D... | | | any | any | any | any | any | any | none |

[Page 1](#) of 1 | Show 50 items

Default_Allow_WAN_To_ZyWALL

Description:
System Default Allow From WAN To ZyWALL

Members:

- AH
- ESP
- IKE
- NATT
- GRE
- VRRP

[Apply](#)
[Reset](#)

Test the IPSec VPN Tunnel

Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

[Add](#)
[Edit](#)
[Remove](#)
[Activate](#)
[Inactivate](#)
[Connect](#)
[Disconnect](#)
[Object References](#)

| # | Status | Name | VPN Gateway | Gateway IP Version | Policy |
|---|--------|------------|-------------|--------------------|--|
| 1 | | WIZ_VPN_HQ | WIZ_VPN_HQ | IPv4 | WIZ_VPN_HQ_LOCAL / WIZ_VPN_HQ_REMOTE |

[Page 1](#) of 1 | Show 50 items

Displaying 1 - 1 of 1

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and **Inbound (Bytes)/Outbound (Bytes)** Traffic.

MONITOR > VPN Monitor > IPSec

| Disconnect | | Connection Check | | | | | | | |
|-----------------------|------------|--------------------------------|--------------|-----------------------|-----------|---------|---------------|--------------|--|
| # | Name | Policy | My Address | Secure Gateway | Up Time ^ | Timeout | Inbound(By... | Outbound(... | |
| 1 | WIZ_VPN_HQ | 10.10.10.0/24<>192.168.20.0/24 | 192.168.1.33 | P: 172.100.30.40:4500 | 14 | 86406 | 0(0 bytes) | 0(0 bytes) | |
| Page 1 | | of 1 | | Show 50 | | items | | | |
| Displaying 1 - 1 of 1 | | | | | | | | | |

To test whether or not a tunnel is working, ping from a computer at one site to a computer at the other. Ensure that both computers have Internet access (via the IPSec devices).

PC behind ZyWALL/USG (HQ) > Window 7 > cmd > ping 192.168.20.33

```
C:\Documents and Settings\ZYXEL>ping 192.168.20.33

Pinging 192.168.20.33 with 32 bytes of data:

Reply from 192.168.20.33: bytes=32 time=27ms TTL=43
Reply from 192.168.20.33: bytes=32 time=32ms TTL=43
Reply from 192.168.20.33: bytes=32 time=26ms TTL=43
Reply from 192.168.20.33: bytes=32 time=27ms TTL=43

Ping statistics for 192.168.20.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 32ms, Average = 28ms
```

PC behind ZyWALL/USG (Branch) > Window 7 > cmd > ping 10.10.10.33

```
C:\Documents and Settings\ZYXEL>ping 10.10.10.33

Pinging 10.10.10.33 with 32 bytes of data:

Reply from 10.10.10.33: bytes=32 time=18ms TTL=54
Reply from 10.10.10.33: bytes=32 time=17ms TTL=54
Reply from 10.10.10.33: bytes=32 time=17ms TTL=54
Reply from 10.10.10.33: bytes=32 time=16ms TTL=54

Ping statistics for 10.10.10.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 18ms, Average = 17ms
```

What Could Go Wrong?

If you see below [info] or [error] log message, please check ZyWALL/USG Phase 1 Settings. Both ZyWALL/USG at the HQ and Branch sites must use the same Pre-Shared Key, Encryption, Authentication method, DH key group and ID Type to establish the IKE SA.

MONITOR > Log

| Priority | Category | Message | Note |
|----------|----------|--|---------|
| info | IKE | Recv:[NOTIFY:INVALID_COOKIE] | IKE_LOG |
| info | IKE | Send:[ID][HASH][NOTIFY:INITIAL_CONTACT] | IKE_LOG |
| Priority | Category | Message | Note |
| error | IPSec | SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet | IPSec |
| error | IPSec | SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet | IPSec |
| info | IKE | [COOKIE] Invalid cookie, no sa found | IKE_LOG |
| Priority | Category | Message | Note |
| info | IKE | Recv:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN] | IKE_LOG |

If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG Phase 2 Settings. Both ZyWALL/USG at the HQ and Branch sites must use the same Protocol, Encapsulation, Encryption, Authentication method and PFS to establish the IKE SA.

MONITOR > Log

| | | | | | |
|----|----------------|------|-----|--|---------|
| 19 | 2017-09-11 ... | info | IKE | [SA] : No proposal chosen | IKE_LOG |
| 20 | 2017-09-11 ... | info | IKE | [ID] : Tunnel [Server] Phase 2 Local policy mismatch | IKE_LOG |
| 31 | 2017-09-11 ... | info | IKE | Send:[HASH][SA][NONCE][ID][ID] | IKE_LOG |
| 32 | 2017-09-11 ... | info | IKE | Phase 1 IKE SA process done | IKE_LOG |

Make sure the both ZyWALL/USG at the HQ and Branch sites security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

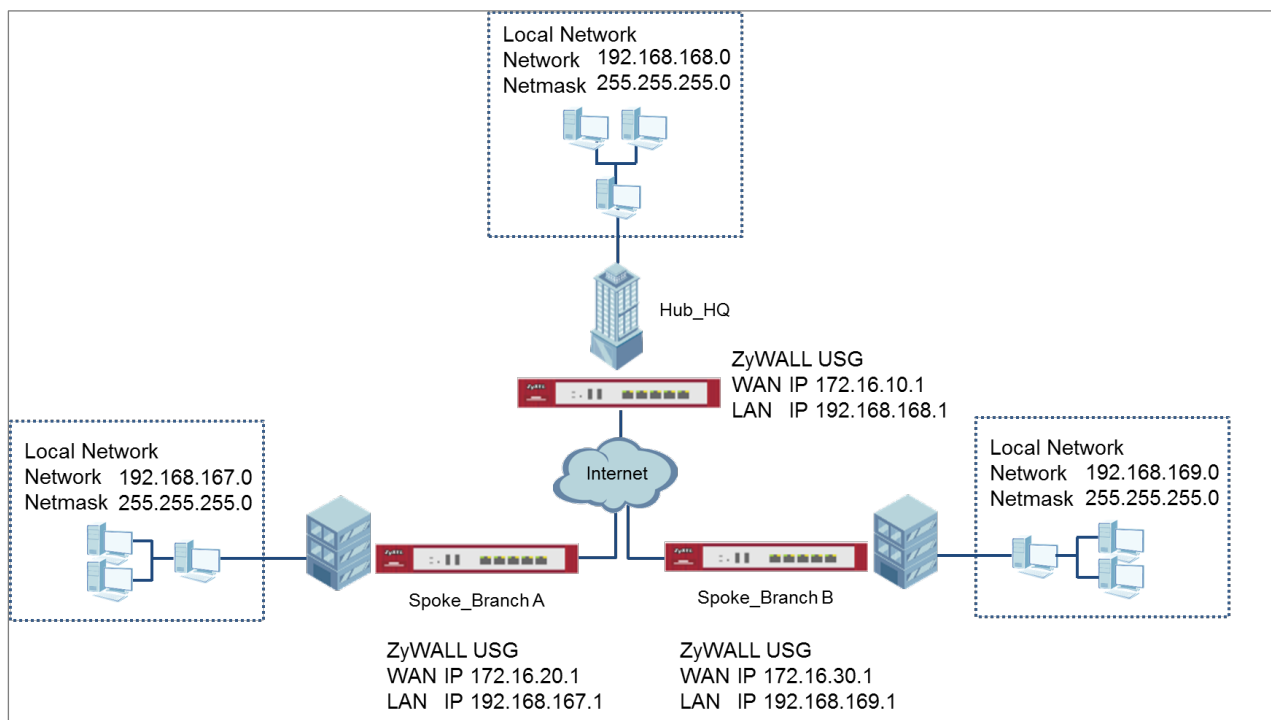
Default NAT traversal is enable on ZyWALL/USG, please make sure the remote IPSec device must also have NAT traversal enabled.


How to Configure Hub-and-Spoke IPSec VPN

This is an example of a hub-and-spoke VPN with the HQ ZyWALL/USG as the hub and spoke VPNs to Branches A and B. When the VPN tunnel is configured, traffic passes between branches via the hub (HQ). Traffic can also pass between spoke-and-spoke through the hub. Here are two methods to set up hub-and-spoke VPN connections: 1. With VPN Concentrator 2. Without VPN Concentrator.

With just two branch offices, you could just manually set up VPN tunnels between HQ and the branches. With many branches it's best to use the VPN Concentrator to set up branch-HQ tunnels automatically.

ZyWALL/USG Hub-and-Spoke VPN Example



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the IPSec VPN Tunnel on the ZyWALL/USG by Using VPN Concentrator Hub_HQ-to-Branch_A

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Please select the type of VPN policy you wish to setup.

Type of VPN policy

- ☒ Express
- ☐ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

123

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name:

Hub_HQ-to-Branch_A

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

Then, configure the **Secure Gateway** IP as the **Branch A**'s Gateway IP address (in the example, 172.16.20.1). Type a secure **Pre-Shared Key** (8-32 characters) which must match your **Branch A**'s Pre-Shared Key.

Set **Local Policy** to be the IP address range of the network connected to the **Hub_HQ** and **Remote Policy** to be the IP address range of the network connected to the **Branch A**. Click **OK**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

Configuration

Secure Gateway: 172.16.20.1 (IP or FQDN)

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.168.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.167.0 / 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Summary)

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

Summary

Rule Name: Hub_HQ-to-Branch_A

Secure Gateway: 172.16.20.1

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.168.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.167.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings > Wizard Completed

VPN Setup Wizard

Wizard Type

>

VPN Settings

>

Wizard Completed

1

2

3

Express Settings

Congratulations. The VPN Access wizard is completed

Summary

| | |
|--------------------------|-------------------------------|
| Rule Name: | Hub_HQ-to-Branch_A |
| Secure Gateway: | 172.16.20.1 |
| Pre-Shared Key: | 12345678 |
| Local Policy (IP/Mask): | 192.168.168.0 / 255.255.255.0 |
| Remote Policy (IP/Mask): | 192.168.167.0 / 255.255.255.0 |

Hub_HQ-to-Branch_B

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
1 2 3

Please select the type of VPN policy you wish to setup.

Type of VPN policy

- ☒ Express
- ☐ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name:

Hub_HQ-to-Branch_B

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

Then, configure the **Secure Gateway** IP as the **Branch B**'s Gateway IP address (in the example, 172.16.30.1). Type a secure **Pre-Shared Key** (8-32 characters) which must match your **Branch B**'s Pre-Shared Key.

Set **Local Policy** to be the IP address range of the network connected to the **Hub_HQ** and **Remote Policy** to be the IP address range of the network connected to the **Branch B**. Click **OK**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

123

Express Settings

Configuration

Secure Gateway: 172.16.30.1 (IP or FQDN)

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.168.0 255.255.255.0

Remote Policy (IP/Mask): 192.168.169.0 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Summary)

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

123

Express Settings

Summary

Rule Name: Hub_HQ-to-Branch_B

Secure Gateway: 172.16.30.1

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.168.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.169.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings > Wizard Completed

VPN Setup Wizard

Wizard Type >

VPN Settings >

Wizard Completed

1

2

3

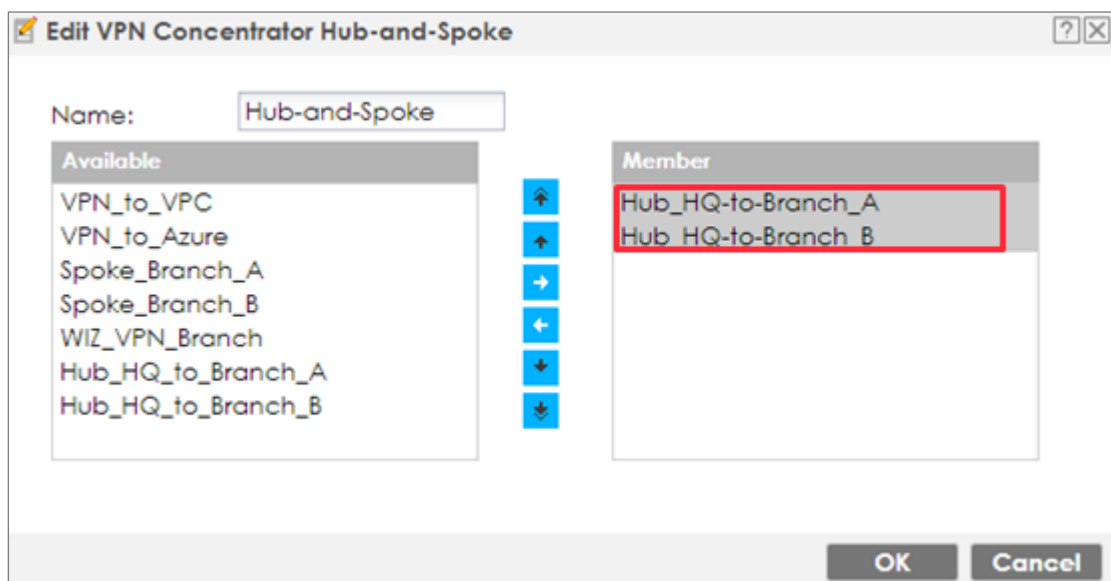
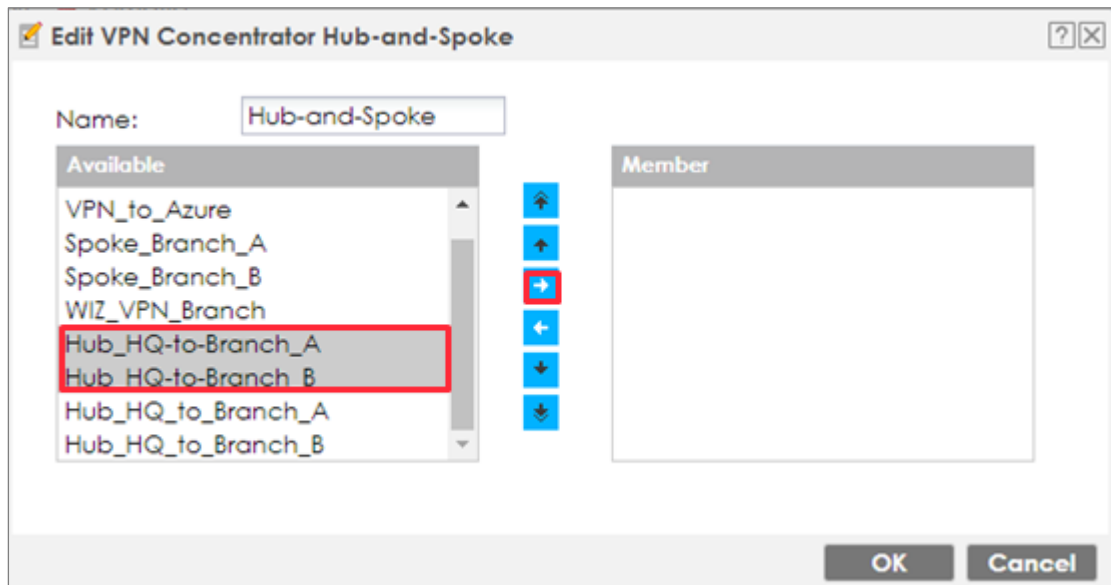
Express Settings

Congratulations. The VPN Access wizard is completed
 Summary

| | |
|--------------------------|-------------------------------|
| Rule Name: | Hub_HQ-to-Branch_B |
| Secure Gateway: | 172.16.30.1 |
| Pre-Shared Key: | 12345678 |
| Local Policy (IP/Mask): | 192.168.168.0 / 255.255.255.0 |
| Remote Policy (IP/Mask): | 192.168.169.0 / 255.255.255.0 |

Hub_HQ Concentrator

In the ZyWALL/USG, go to **CONFIGURATION > VPN > IPSec VPN > Concentrator**, add a VPN Concentrator rule. Select VPN tunnels to be in the same member group and click **Save**.



Spoke_Branch_A

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
1 2 3

Please select the type of VPN policy you wish to setup.

Type of VPN policy

- ☒ Express
- ☐ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

123

Express Settings

IKE Version

☒ IKEv1
☐ IKEv2

Scenario

Rule Name:

☒ Site-to-site
☐ Site-to-site with Dynamic Peer
☐ Remote Access (Server Role)
☐ Remote Access (Client Role)

Then, configure the **Secure Gateway** IP as the **Hub_HQ**'s Gateway IP address (in the example, 172.16.10.1). Type a secure **Pre-Shared Key** (8-32 characters) which must match your **Hub_HQ**'s Pre-Shared Key.

Set **Local Policy** to be the IP address range of the network connected to the **Spoke_Branch_A** and **Remote Policy** to be the IP address range of the network connected to the **Hub_HQ**. Click **OK**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

123

Express Settings

Configuration

Secure Gateway: 172.16.10.1 (IP or FQDN)

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.167.0 255.255.255.0

Remote Policy (IP/Mask): 192.168.168.0 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Summary)

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

123

Express Settings

Summary

Rule Name: Spoke_Branch_A

Secure Gateway: 172.16.10.1

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.167.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.168.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings > Wizard Completed

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Congratulations. The VPN Access wizard is completed

Summary

| | |
|--------------------------|-------------------------------|
| Rule Name: | Spoke_Branch_A |
| Secure Gateway: | 172.16.10.1 |
| Pre-Shared Key: | 12345678 |
| Local Policy (IP/Mask): | 192.168.167.0 / 255.255.255.0 |
| Remote Policy (IP/Mask): | 192.168.168.0 / 255.255.255.0 |

Go to **Network > Routing > Policy Route** to add a **Policy Route** to allow traffic from **Spoke_Branch_A** to **Spoke_Branch_B**.

Click **Create new Object** and set **Address** to be the local network behind the **Spoke_Branch_B**. Select **Source Address** to be the local network behind the

Spoke_Branch_A. Then, scroll down the **Destination Address** list to choose the newly created **Spoke_Branch_B_LOCAL** address. Click **OK**.

Network > Routing > Policy Route

+

Add Policy Route

Show Advanced Settings

Create new Object ▼

Criteria

| | |
|----------------------|----------------------|
| User: | any ▼ |
| Incoming: | any (Excluding ZyV ▼ |
| Source Address: | Spock_Branch_A_L ▼ |
| Destination Address: | Spock_Branch_B_L ▼ |
| DSCP Code: | any ▼ |
| Schedule: | none ▼ |
| Service: | any ▼ |

Next-Hop

| | |
|-------------|------------------|
| Type: | VPN Tunnel ▼ |
| VPN Tunnel: | Spoke_Branch_A ▼ |

Spoke_Branch_B

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Please select the type of VPN policy you wish to setup.

Type of VPN policy

- ☒ Express
- ☐ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

123

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name:

Spoke_Branch_B

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

Then, configure the **Secure Gateway** IP as the **Hub_HQ**'s Gateway IP address (in the example, 172.16.10.1). Type a secure **Pre-Shared Key** (8-32 characters) which must match your **Hub_HQ**'s Pre-Shared Key.

Set **Local Policy** to be the IP address range of the network connected to the **Spoke_Branch_B** and **Remote Policy** to be the IP address range of the network connected to the **Hub_HQ**. Click **OK**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Configuration

Secure Gateway: 172.168.10.1 (IP or FQDN)

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.169.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.168.0 / 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Summary)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Summary

Rule Name: Spoke_Branch_B

Secure Gateway: 172.16.10.1

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.169.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.168.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings > Wizard Completed

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Congratulations. The VPN Access wizard is completed

Summary

| | |
|--------------------------|-------------------------------|
| Rule Name: | Spoke_Branch_B |
| Secure Gateway: | 172.16.10.1 |
| Pre-Shared Key: | 12345678 |
| Local Policy (IP/Mask): | 192.168.169.0 / 255.255.255.0 |
| Remote Policy (IP/Mask): | 192.168.168.0 / 255.255.255.0 |

Go to **Network > Routing > Policy Route** to add a Policy Route to allow traffic from **Spoke_Branch_B** to **Spoke_Branch_A**.

Click **Create new Object** and set **Address** to be the local network behind the **Spoke_Branch_A**. Select **Source Address** to be the local network behind the

Spoke_Branch_B. Then, scroll down the **Destination Address** list to choose the newly created **Spoke_Branch_A_LOCAL** address. Click **OK**.

Network > Routing > Policy Route

+

Add Policy Route

Show Advanced Settings

Create new Object ▼

Criteria

User:

any ▼

Incoming:

any (Excluding ZyV ▼

Source Address:

Spock_Branch_B_L ▼

Destination Address:

Spock_Branch_A_L ▼

DSCP Code:

any ▼

Schedule:

none ▼

Service:

any ▼

Next-Hop

Type:

VPN Tunnel ▼

VPN Tunnel:

Spoke_Branch_B ▼

Test the IPSec VPN Tunnel

Go to ZyWALL/USG **CONFIGURATION > VPN > IPsec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

Hub_HQ > CONFIGURATION > VPN > IPsec VPN > VPN Connection

| IPv4 Configuration | | | | |
|--|--------|--------------------|--------------------|--|
| Add Edit Remove Activate Inactivate Connect Disconnect Object References | | | | |
| # | Status | Name | VPN Gateway | Policy |
| 1 | | Hub_HQ-to-Branch_A | Hub_HQ-to-Branch_A | Hub_HQ-to-Branch_A_LOCAL/Hub_HQ-to-Branch_A_REMOTE |
| 2 | | Hub_HQ-to-Branch_B | Hub_HQ-to-Branch_B | Hub_HQ-to-Branch_B_LOCAL/Hub_HQ-to-Branch_B_REMOTE |
| Page 1 of 1 Show 50 items Displaying 1 - 2 of 2 | | | | |

Spoke_Branch_A > CONFIGURATION > VPN > IPsec VPN > VPN Connection

| IPv4 Configuration | | | | |
|--|--------|----------------|----------------|--|
| Add Edit Remove Activate Inactivate Connect Disconnect Object References | | | | |
| # | Status | Name | VPN Gateway | Policy |
| 1 | | Spoke-Branch_A | Spoke-Branch_A | Spoke-Branch_A_LOCAL/Spoke-Branch_A_REMOTE |
| Page 1 of 1 Show 50 items Displaying 1 - 1 of 1 | | | | |

Spoke_Branch_B > CONFIGURATION > VPN > IPsec VPN > VPN Connection

| IPv4 Configuration | | | | |
|--|--------|----------------|----------------|--|
| Add Edit Remove Activate Inactivate Connect Disconnect Object References | | | | |
| # | Status | Name | VPN Gateway | Policy |
| 1 | | Spoke-Branch_B | Spoke-Branch_B | Spoke-Branch_B_LOCAL/Spoke-Branch_B_REMOTE |
| Page 1 of 1 Show 50 items Displaying 1 - 1 of 1 | | | | |

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPsec** and verify the tunnel **Up Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic. Click **Connectivity Check** to verify the result of ICMP Connectivity.

Hub_HQ > MONITOR > VPN Monitor > IPsec > Hub_HQ-to-Branch_A

| Disconnect | | Connection Check | | | | | | |
|------------|--------------------|------------------------------------|-------------|-----------------|---------|---------|-------------|------------|
| # | Name | Policy | My Address | Secure Gatew... | Up Time | Timeout | Inbound(... | Outboun... |
| 1 | Hub_HQ-to-Branch_A | 192.168.168.0/24<>192.168.167.0/24 | 172.16.10.1 | P: 172.16.20.1 | 253 | 86167 | 0(0 bytes) | 0(0 bytes) |
| 2 | Hub_HQ-to-Branch_B | 192.168.168.0/24<>192.168.169.0/24 | 172.16.10.1 | P: 172.16.30.1 | 68 | 86352 | 1(78 bytes) | 0(0 bytes) |

Page 1 of 1 Show 50 items Displaying 1 - 2 of 2


Connectivity Check

Connectivity Check

IP Address:

OK Cancel

Result

 ICMP Connectivity Check PASS on Hub_HQ-to-Branch_A

OK

Hub_HQ > MONITOR > VPN Monitor > IPSec > Hub_HQ-to-Branch_B

| # | Name | Policy | My Address | Secure Gatew... | Up Time | Timeout | Inbound(... | Outbound... |
|---|--------------------|------------------------------------|-------------|-----------------|---------|---------|-------------|-------------|
| 1 | Hub_HQ-to-Branch_A | 192.168.168.0/24<>192.168.167.0/24 | 172.16.10.1 | P: 172.16.20.1 | 253 | 86167 | 0(0 bytes) | 0(0 bytes) |
| 2 | Hub_HQ-to-Branch_B | 192.168.168.0/24<>192.168.169.0/24 | 172.16.10.1 | P: 172.16.30.1 | 68 | 86352 | 1(78 bytes) | 0(0 bytes) |

Page 1 of 1 Show 50 items Displaying 1 - 2 of 2


Connectivity Check

Connectivity Check

IP Address:

OK Cancel

Result

 ICMP Connectivity Check PASS on Hub_HQ-to-Branch_B

OK

Spoke_Branch_A > MONITOR > VPN Monitor > IPsec

| # | Name | Policy | My Address | Secure Gat... | Up Time | Timeout | Inbound(B... | Outbound(... |
|---|----------------|------------------------------------|-------------|----------------|---------|---------|--------------|--------------|
| 1 | Spoke_Branch_A | 192.168.167.0/24<>192.168.168.0/24 | 172.16.20.1 | P: 172.16.10.1 | 66 | 86354 | 0(0 bytes) | 0(0 bytes) |

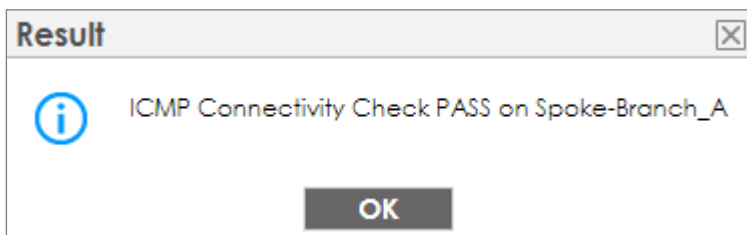
Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

Connectivity Check

Connectivity Check

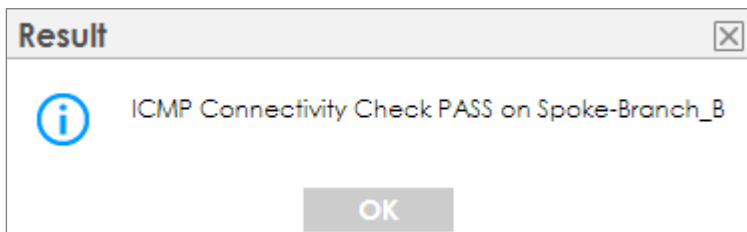
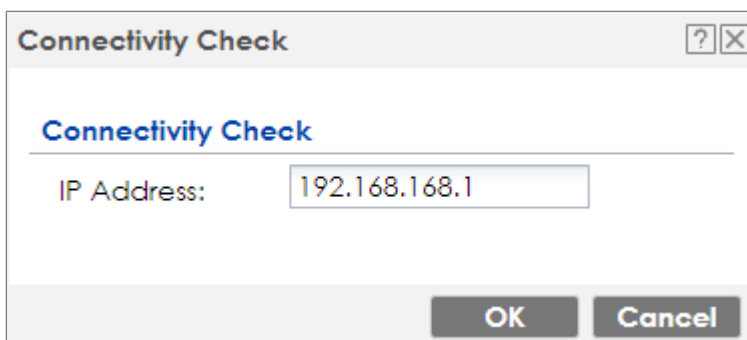
IP Address:

OK Cancel



Spoke_Branch_B > MONITOR > VPN Monitor > IPSec

| Disconnect | | Connection Check | | | | | | |
|---|----------------|------------------------------------|-------------|----------------|---------|---------|---------------|--------------|
| # | Name | Policy | My Address | Secure Gat... | Up Time | Timeout | Inbound[By... | Outbound[... |
| 1 | Spoke_Branch_B | 192.168.169.0/24<>192.168.168.0/24 | 172.16.30.1 | P: 172.16.10.1 | 8 | 86412 | 0(0 bytes) | 0(0 bytes) |
| Page 1 of 1 Show 50 items Displaying 1 - 1 of 1 | | | | | | | | |



What Could Go Wrong?

If you see [info] or [error] log message such as below, please check ZyWALL/USG Phase 1 Settings. All ZyWALL/USG units must use the same Pre-Shared Key, Encryption, Authentication method, DH key group and ID Type to establish the IKE SA.

| Priority | Category | Message | Note |
|----------|----------|--|---------|
| info | IKE | Recv:[NOTIFY:INVALID_COOKIE] | IKE_LOG |
| info | IKE | Send:[ID][HASH][NOTIFY:INITIAL_CONTACT] | IKE_LOG |
| Priority | Category | Message | Note |
| error | IPSec | SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet | IPSec |
| error | IPSec | SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet | IPSec |
| info | IKE | [COOKIE] Invalid cookie, no sa found | IKE_LOG |
| Priority | Category | Message | Note |
| info | IKE | Recv:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN] | IKE_LOG |

If you see that Phase 1 IKE SA process done but still get [info] log message as below, please check ZyWALL/USG and SonicWALL Phase 2 Settings. All ZyWALL/USG units must use the same Protocol, Encapsulation, Encryption, Authentication method and PFS to establish the IKE SA.

| | | | | | |
|----|----------------|------|-----|--|---------|
| 19 | 2017-09-11 ... | info | IKE | [SA] : No proposal chosen | IKE_LOG |
| 20 | 2017-09-11 ... | info | IKE | [ID] : Tunnel [Server] Phase 2 Local policy mismatch | IKE_LOG |
| 31 | 2017-09-11 ... | info | IKE | Send:[HASH][SA][NONCE][ID][ID] | IKE_LOG |
| 32 | 2017-09-11 ... | info | IKE | Phase 1 IKE SA process done | IKE_LOG |

Make sure the all ZyWALL/USG units' security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

By default, NAT traversal is enabled on ZyWALL/USG, so please make sure the remote IPSec device also has NAT traversal enabled.

Set Up the IPSec VPN Tunnel of ZyWALL/USG without Using VPN Concentrator Hub_HQ-to-Branch_A

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** and select **Enable**. Type the **VPN Gateway Name** used to identify this VPN gateway.

Then, configure the **Secure Gateway** IP as the **Branch A's** Gateway IP address (in the example, 172.16.20.1). Type a secure **Pre-Shared Key** (8-32 characters) which must match your **Branch A's** Pre-Shared Key and click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway

General Settings

☒ Enable

VPN Gateway Name:

Hub_HQ-to-Branch_A

IKE Version

☒ IKEv1
 ☐ IKEv2

Gateway Settings

My Address

☒ Interface

ge2

DHCP client -- 172.16.10.1/255.255.255.

☐ Domain Name / IPv4

Peer Gateway Address

☒ Static Address

Primary

172.16.20.1

Secondary

0.0.0.0

☐ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval:

300

(60-86400 seconds)

☐ Dynamic Address

Authentication

☒ Pre-Shared Key

.....

unmasked

☐ Certificate

default

(See [My Certificates](#))

☐ User Based PSK

admin

☐ Advance

Phase 1 Settings

SA Life Time:

86400

(180 - 3000000 Seconds)

Negotiation Mode:

Main

☐ Advance

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** and select **Enable**. Type the **Connection Name** used to identify this VPN connection. Select scenario as **Site-to-site** and VPN Gateway which is configured in Step 1.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > General Settings and VPN Gateway

General Settings

☒ Enable

Connection Name:

Hub_HQ-to-Branch_A

☐ Advance

VPN Gateway

Application Scenario

☒ Site-to-site

☐ Site-to-site with Dynamic Peer
 ☐ Remote Access (Server Role)
 ☐ Remote Access (Client Role)
 ☐ Vpn Tunnel Interface

VPN Gateway:

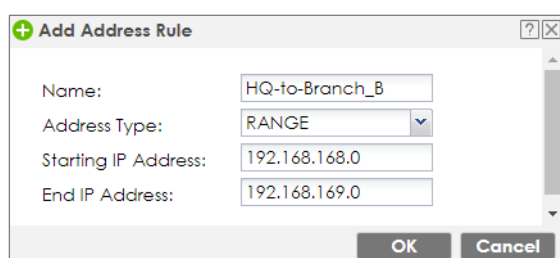
Hub_HQ-to-Branch

ge2 172.16.20.1, 0.0.0.0

Click **Create new Object** on the upper bar to add the address range of the local network behind **Hub_HQ** to **Branch_B** and an address of local network behind **Branch A**.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Create new Object

Local Policy

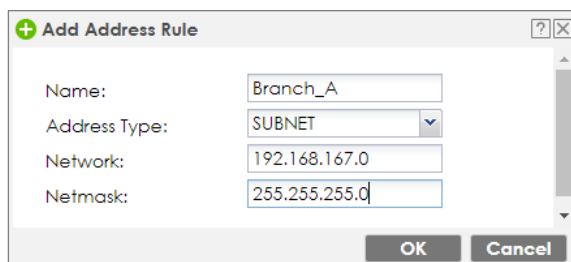


The 'Add Address Rule' dialog box is shown with the following fields:

- Name: HQ-to-Branch_B
- Address Type: RANGE
- Starting IP Address: 192.168.168.0
- End IP Address: 192.168.169.0

Buttons: OK, Cancel

Remote Policy



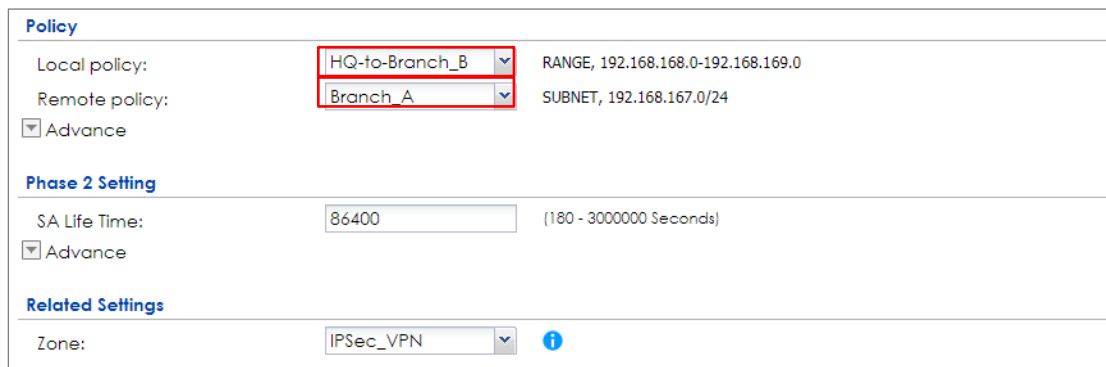
The 'Add Address Rule' dialog box is shown with the following fields:

- Name: Branch_A
- Address Type: SUBNET
- Network: 192.168.167.0
- Netmask: 255.255.255.0

Buttons: OK, Cancel

Set **Local Policy** to be **HQ-to-Branch_B** and **Remote Policy** to **Branch_A** which are newly created. Click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Policy



The 'Policy' configuration page is shown with the following settings:

- Local policy: HQ-to-Branch_B (selected)
- Remote policy: Branch_A (selected)
- Phase 2 Setting: SA Life Time: 86400 (180 - 3000000 Seconds)
- Related Settings: Zone: IPSec_VPN

Hub_HQ-to-Branch_B

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway**, select **Enable**. Type the **VPN Gateway Name** used to identify this VPN gateway.

Then, configure the **Secure Gateway** IP as the **Branch B's** Gateway IP address (in the example, 172.16.30.1). Type a secure **Pre-Shared Key** (8-32 characters) which must match your **Branch B's** Pre-Shared Key and click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway

General Settings

☒ Enable

VPN Gateway Name: Hub_HQ-to-Branch_B

IKE Version

☒ IKEv1
 ☐ IKEv2

Gateway Settings

My Address

☒ Interface ge2 DHCP client -- 172.16.10.1/255.255.255.
 ☐ Domain Name / IPv4

Peer Gateway Address

☒ Static Address

Primary 172.16.30.1
 Secondary 0.0.0.0

☐ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: 300 (60-86400 seconds)

☐ Dynamic Address

Authentication

☒ Pre-Shared Key

☐ unmasked

☐ Certificate default (See [My Certificates](#))

☐ User Based PSK admin

☒ Advance

Go to **CONFIGURATION > VPN > IPsec VPN > VPN Connection** and select **Enable**.

Type the **Connection Name** used to identify this VPN connection. Select scenario as **Site-to-site** and VPN Gateway which is configured in Step 1.

CONFIGURATION > VPN > IPsec VPN > VPN Connection > General Settings and VPN Gateway

General Settings

☒ Enable

Connection Name:

Hub_HQ-to-Branch_B

☐ Advance

VPN Gateway

Application Scenario

☒ Site-to-site
 ☐ Site-to-site with Dynamic Peer
 ☐ Remote Access (Server Role)
 ☐ Remote Access (Client Role)
 ☐ Vpn Tunnel Interface

VPN Gateway:

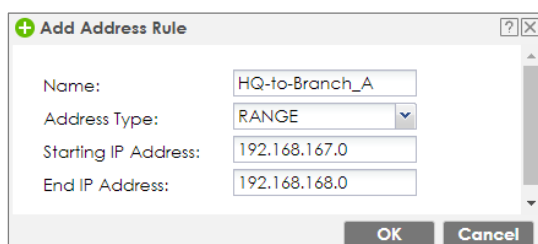
Hub_HQ-to-Branch

ge2 172.16.30.1, 0.0.0.0

Click **Create new Object** on the upper bar to add the address range of the local network behind **Hub_HQ** to **Branch_A** and an address of local network behind **Branch B**.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Create new Object

Local Policy

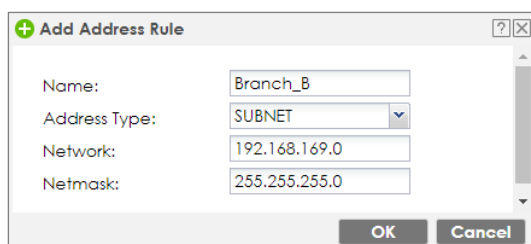


The 'Add Address Rule' dialog box for the Local Policy configuration. It contains the following fields:

- Name: HQ-to-Branch_A
- Address Type: RANGE
- Starting IP Address: 192.168.167.0
- End IP Address: 192.168.168.0

Buttons: OK, Cancel

Remote Policy



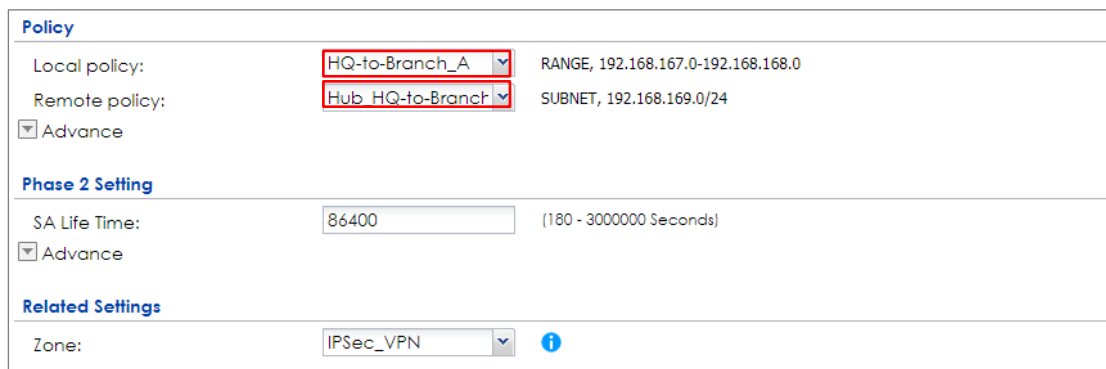
The 'Add Address Rule' dialog box for the Remote Policy configuration. It contains the following fields:

- Name: Branch_B
- Address Type: SUBNET
- Network: 192.168.169.0
- Netmask: 255.255.255.0

Buttons: OK, Cancel

Set **Local Policy** to be **HQ-to-Branch_B** and **Remote Policy** to **Branch_B** which are newly created. Click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Policy



The 'Policy' configuration page for the IPSec VPN connection. It contains the following sections and fields:

- Policy**
 - Local policy: HQ-to-Branch_A (selected from dropdown)
 - Remote policy: Hub_HQ-to-Branch (selected from dropdown)
 - Advanced: [checked]
- Phase 2 Setting**
 - SA Life Time: 86400 (180 - 3000000 Seconds)
 - Advanced: [checked]
- Related Settings**
 - Zone: IPSec_VPN (selected from dropdown)

Spoke_Branch_A

Go to **CONFIGURATION > VPN > IPsec VPN > VPN Gateway**, select **Enable**. Type the **VPN Gateway Name** used to identify this VPN gateway.

Then, configure the **Secure Gateway** IP as the **Hub_HQ**'s Gateway IP address (in the example, 172.16.10.1). Type a secure **Pre-Shared Key** (8-32 characters) which must match your **Hub_HQ**'s Pre-Shared Key and click **OK**.

CONFIGURATION > VPN > IPsec VPN > VPN Gateway

General Settings

☒ Enable

VPN Gateway Name:

IKE Version

☒ IKEv1

☐ IKEv2

Gateway Settings

My Address

☒ Interface DHCP client -- 172.16.20.1/255.255.255.

☐ Domain Name / IPv4

Peer Gateway Address

☒ Static Address

Primary

Secondary

☐ Fall back to Primary Peer Gateway when possible

Fail Back Check Interval: (60-86400 seconds)

☐ Dynamic Address

Authentication

☒ Pre-Shared Key

.....

unmasked

☐ Certificate

default

(See [My Certificates](#))

☐ User Based PSK

Remote_Client

☐ Advance

Phase 1 Settings

SA Life Time:

86400

(180 - 3000000 Seconds)

Negotiation Mode:

Main

☐ Advance

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** and select **Enable**. Type the **Connection Name** used to identify this VPN connection. Select scenario as **Site-to-site** and VPN Gateway which is configured in Step 1.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > General Settings and VPN Gateway

General Settings

☒ Enable

Connection Name:

Spoke_Branch_A

☐ Advance

VPN Gateway

Application Scenario

☒ Site-to-site

☐ Site-to-site with Dynamic Peer
 ☐ Remote Access (Server Role)
 ☐ Remote Access (Client Role)
 ☐ Vpn Tunnel Interface

VPN Gateway:

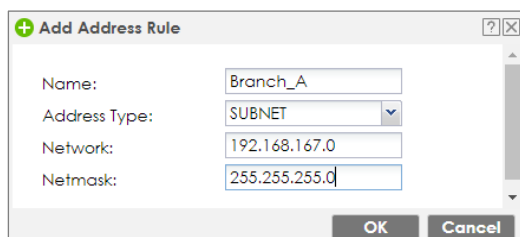
Spoke_Branch_A

ge2 172.16.10.1, 0.0.0.0

Click **Create new Object** on the upper bar to add the address of the local network behind **Branch A** and the address range of the local network behind **Hub_HQ** to **Branch_B**.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Create new Object

Local Policy



Add Address Rule

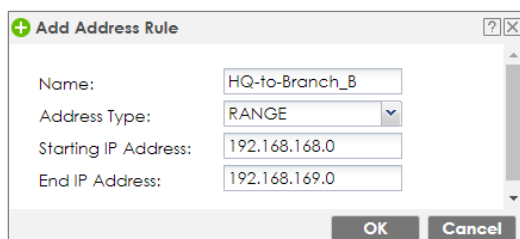
Name:

Address Type:

Network:

Netmask:

Remote Policy



Add Address Rule

Name:

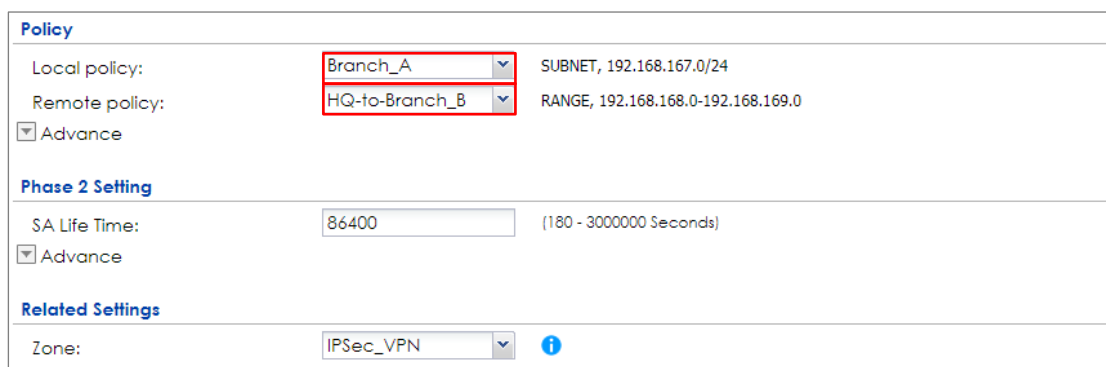
Address Type:

Starting IP Address:

End IP Address:

Set **Local Policy** to be **Branch_A** and **Remote Policy** to **HQ-to-Branch_B** which are newly created. Click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Policy



Policy

Local policy: SUBNET, 192.168.167.0/24

Remote policy: RANGE, 192.168.168.0-192.168.169.0

☐ Advance

Phase 2 Setting

SA Life Time: (180 - 3000000 Seconds)

☐ Advance

Related Settings

Zone:

Spoke_Branch_B

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway**, select **Enable**. Type the **VPN Gateway Name** used to identify this VPN gateway.

Then, configure the **Secure Gateway** IP as the **Hub_HQ's** Gateway IP address (in the example, 172.16.10.1). Type a secure **Pre-Shared Key** (8-32 characters) which must match your **Hub_HQ's** Pre-Shared Key and click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway

General Settings

☒ Enable

VPN Gateway Name:

IKE Version

☒ IKEv1

☐ IKEv2

Gateway Settings

My Address

☒ Interface DHCP client -- 172.16.30.1/255.255.255.

☐ Domain Name / IPv4

Peer Gateway Address

☒ Static Address

Primary

Secondary

☐ Fall back to Primary Peer Gateway when possible

Fail Back Check Interval: (60-86400 seconds)

☐ Dynamic Address

Authentication

☒ Pre-Shared Key

.....

unmasked

☐ Certificate

default

(See [My Certificates](#))

☐ User Based PSK

Remote_Client

☐ Advance

Phase 1 Settings

SA Life Time:

86400

(180 - 3000000 Seconds)

Negotiation Mode:

Main

☐ Advance

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** and select **Enable**. Type the **Connection Name** used to identify this VPN connection. Select scenario as **Site-to-site** and VPN Gateway which is configured in Step 1.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > General Settings and VPN Gateway

General Settings

☒ Enable

Connection Name:

Spoke_Branch_B

☐ Advance

VPN Gateway

Application Scenario

☒ Site-to-site

☐ Site-to-site with Dynamic Peer
 ☐ Remote Access (Server Role)
 ☐ Remote Access (Client Role)
 ☐ Vpn Tunnel Interface

VPN Gateway:

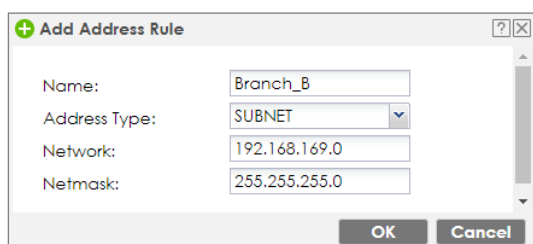
Spoke_Branch_B

ge2 172.16.10.1, 0.0.0.0

Click **Create new Object** on the upper bar to add the address of local network behind **Branch B** and address range of local network behind **Hub_HQ** to **Branch_A**.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Create new Object

Local Policy

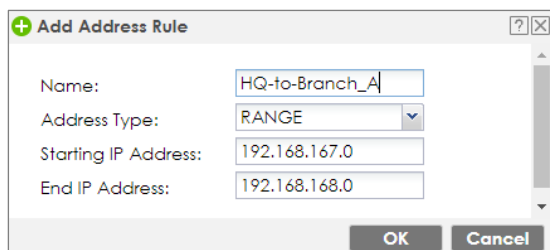


The 'Add Address Rule' dialog box is shown with the following fields:

- Name: Branch_B
- Address Type: SUBNET
- Network: 192.168.169.0
- Netmask: 255.255.255.0

Buttons: OK, Cancel

Remote Policy



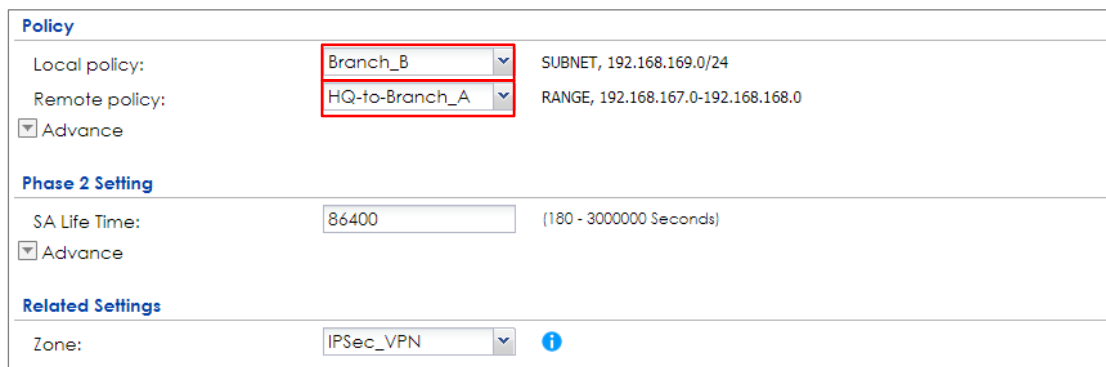
The 'Add Address Rule' dialog box is shown with the following fields:

- Name: HQ-to-Branch_A
- Address Type: RANGE
- Starting IP Address: 192.168.167.0
- End IP Address: 192.168.168.0

Buttons: OK, Cancel

Set **Local Policy** to be **Branch_B** and **Remote Policy** to **HQ-to-Branch_A** which are newly created. Click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Policy



The 'Policy' configuration page is shown with the following settings:

- Local policy:** Branch_B (SUBNET, 192.168.169.0/24)
- Remote policy:** HQ-to-Branch_A (RANGE, 192.168.167.0-192.168.168.0)
- Phase 2 Setting:** SA Life Time: 86400 (180 - 3000000 Seconds)
- Related Settings:** Zone: IPSec_VPN

Test the IPsec VPN Tunnel

Go to ZyWALL/USG **CONFIGURATION > VPN > IPsec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

Hub_HQ > CONFIGURATION > VPN > IPsec VPN > VPN Connection

| IPv4 Configuration | | | | |
|--|--------|--------------------|--------------------|--|
| Add Edit Remove Activate Inactivate Connect Disconnect Object References | | | | |
| # | Status | Name | VPN Gateway | Policy |
| 1 | | Hub_HQ-to-Branch_A | Hub_HQ-to-Branch_A | HQ-to-Branch_B/ Branch_A |
| 2 | | Hub_HQ-to-Branch_B | Hub_HQ-to-Branch_B | HQ-to-Branch_A/ Branch_B |
| << Page 1 of 1 >> Show 50 items | | | | Displaying 1 - 2 of 2 |

Spoke_Branch_A > CONFIGURATION > VPN > IPsec VPN > VPN Connection

| IPv4 Configuration | | | | |
|--|--------|----------------|----------------|--|
| Add Edit Remove Activate Inactivate Connect Disconnect Object References | | | | |
| # | Status | Name | VPN Gateway | Policy |
| 1 | | Spoke_Branch_A | Spoke_Branch_A | Branch_A/ HQ-to-Branch_B |
| << Page 1 of 1 >> Show 50 items | | | | Displaying 1 - 1 of 1 |

Spoke_Branch_B > CONFIGURATION > VPN > IPsec VPN > VPN Connection

| IPv4 Configuration | | | | |
|--|--------|----------------|----------------|--|
| Add Edit Remove Activate Inactivate Connect Disconnect Object References | | | | |
| # | Status | Name | VPN Gateway | Policy |
| 1 | | Spoke_Branch_B | Spoke_Branch_B | Branch_B/ HQ-to-Branch_A |
| << Page 1 of 1 >> Show 50 items | | | | Displaying 1 - 1 of 1 |

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic. Click **Connectivity Check** to verify the result of ICMP Connectivity.

Hub_HQ > MONITOR > VPN Monitor > IPSec > Hub_HQ-to-Branch_A

| Disconnect Connection Check | | | | | | | | | |
|---|--------------------|---|-------------|----------------|---------|---------|-----------|-----------|--|
| # | Name | Policy | My Address | Secure Gat... | Up Time | Timeout | Inbou... | Outb... | |
| 1 | Hub_HQ-to-Branch_A | 192.168.168.0-192.168.169.0<>192.168.167.0/24 | 172.16.10.1 | P: 172.16.20.1 | 584 | 85836 | 0(0 by... | 0(0 by... | |
| 2 | Hub_HQ-to-Branch_B | 192.168.167.0-192.168.168.0<>192.168.169.0/24 | 172.16.10.1 | P: 172.16.30.1 | 23 | 86397 | 0(0 by... | 0(0 by... | |
| <div> Page 1 of 1 Show 50 items Displaying 1 - 2 of 2 </div> | | | | | | | | | |

?

×

Connectivity Check

Connectivity Check

IP Address:

OK

Cancel

×

Result

i

ICMP Connectivity Check PASS on Hub_HQ-to-Branch_A

OK

Hub_HQ > MONITOR > VPN Monitor > IPSec > Hub_HQ-to-Branch_B

| Disconnect Connection Check | | | | | | | | | |
|---|--------------------|---|-------------|----------------|---------|---------|-----------|-----------|--|
| # | Name | Policy | My Address | Secure Gat... | Up Time | Timeout | Inbou... | Outb... | |
| 1 | Hub_HQ-to-Branch_A | 192.168.168.0-192.168.169.0<>192.168.167.0/24 | 172.16.10.1 | P: 172.16.20.1 | 584 | 85836 | 0(0 by... | 0(0 by... | |
| 2 | Hub_HQ-to-Branch_B | 192.168.167.0-192.168.168.0<>192.168.169.0/24 | 172.16.10.1 | P: 172.16.30.1 | 23 | 86397 | 0(0 by... | 0(0 by... | |
| <div> Page 1 of 1 Show 50 items Displaying 1 - 2 of 2 </div> | | | | | | | | | |

?

×

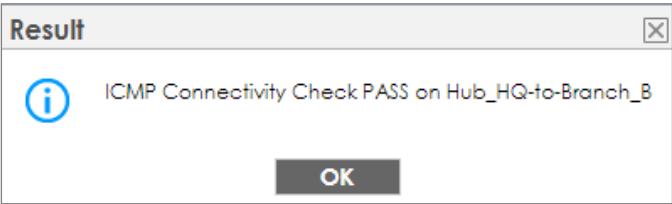
Connectivity Check

Connectivity Check

IP Address:

OK

Cancel



Spoke_Branch_A > MONITOR > VPN Monitor > IPSec

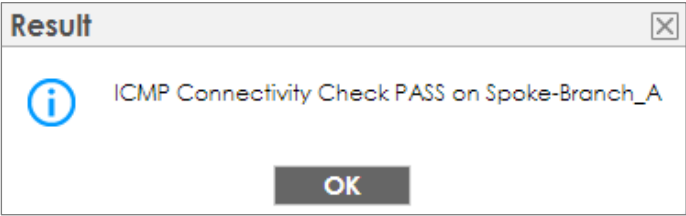
| Disconnect | | Connection Check | | | | | | | |
|---|----------------|---|-------------|----------------|---------|---------|-----------|-----------|--|
| # | Name | Policy | My Address | Secure Gateway | Up Time | Timeout | Inbou... | Outb... | |
| 1 | Spoke_Branch_A | 192.168.167.0/24<>192.168.168.0-192.168.169.0 | 172.16.20.1 | P: 172.16.10.1 | 30 | 73410 | 0(0 by... | 0(0 by... | |
| Page 1 of 1 Show 50 items Displaying 1 - 1 of 1 | | | | | | | | | |

Connectivity Check

Connectivity Check

IP Address: 192.168.168.1

OKCancel



Spoke_Branch_B > MONITOR > VPN Monitor > IPSec

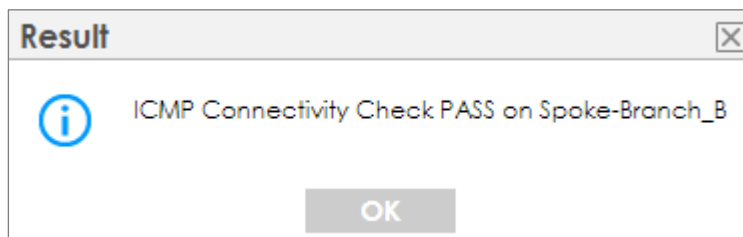
| Disconnect | | Connection Check | | | | | | | |
|---|----------------|---|-------------|----------------|----------|---------|----------|----------|--|
| # | Name | Policy | My Address | Secure Gateway | Up Ti... | Time... | Inbo... | Outb... | |
| 1 | Spoke_Branch_B | 192.168.169.0/24<>192.168.167.0-192.168.168.0 | 172.16.30.1 | P: 172.16.10.1 | 115 | 86305 | 0(0 b... | 0(0 b... | |
| Page 1 of 1 Show 50 items Displaying 1 - 1 of 1 | | | | | | | | | |

Connectivity Check

Connectivity Check

IP Address: 192.168.168.1

OKCancel



What Could Go Wrong?

If you see [info] or [error] log message such as below, please check ZyWALL/USG Phase 1 Settings. All ZyWALL/USG units must use the same Pre-Shared Key, Encryption, Authentication method, DH key group and ID Type to establish the IKE SA.

| Priority | Category | Message | Note |
|----------|----------|--|---------|
| info | IKE | Recv:[NOTIFY:INVALID_COOKIE] | IKE_LOG |
| info | IKE | Send:[ID][HASH][NOTIFY:INITIAL_CONTACT] | IKE_LOG |
| Priority | Category | Message | Note |
| error | IPSec | SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet | IPSec |
| error | IPSec | SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet | IPSec |
| info | IKE | [COOKIE] Invalid cookie, no sa found | IKE_LOG |
| Priority | Category | Message | Note |
| info | IKE | Recv:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN] | IKE_LOG |

If you see that Phase 1 IKE SA process done but still get [info] log message as below, please check ZyWALL/USG and SonicWALL Phase 2 Settings. All ZyWALL/USG units must use the same Protocol, Encapsulation, Encryption, Authentication method and PFS to establish the IKE SA.

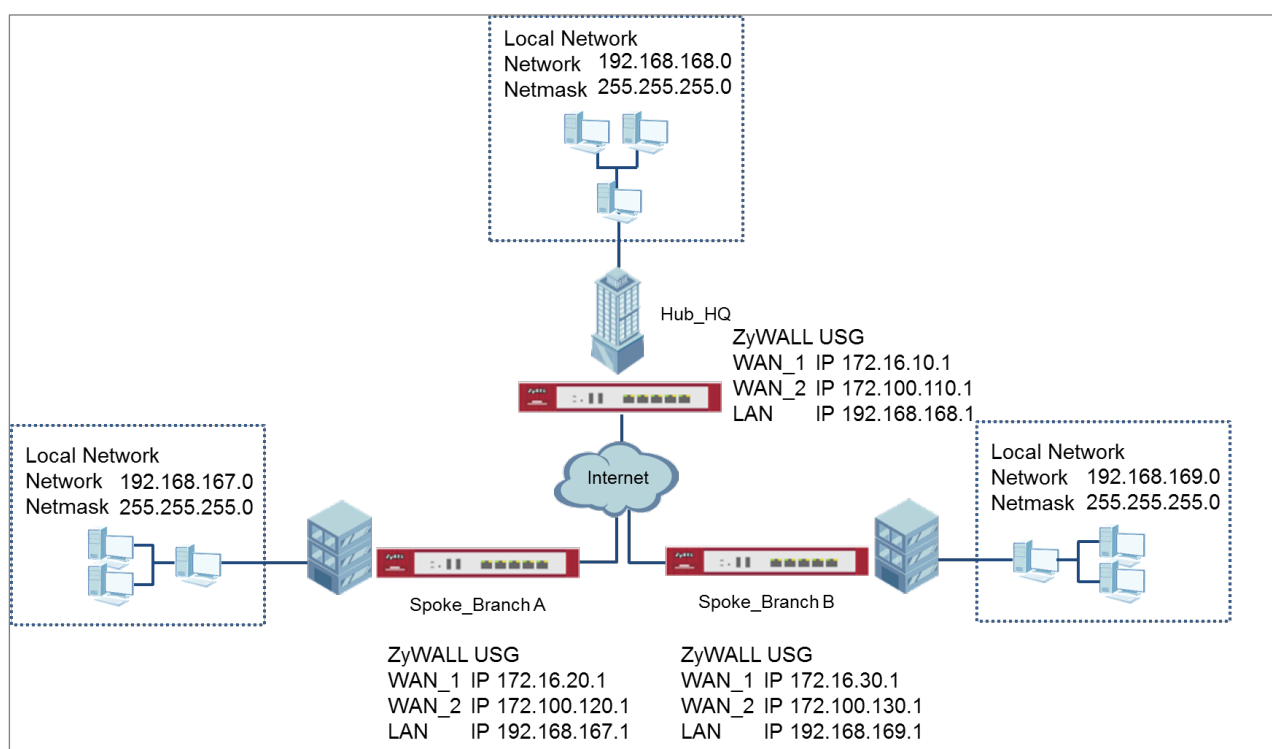
| | | | | | |
|----|----------------|------|-----|--|---------|
| 19 | 2017-09-11 ... | info | IKE | [SA] : No proposal chosen | IKE_LOG |
| 20 | 2017-09-11 ... | info | IKE | [ID] : Tunnel [Server] Phase 2 Local policy mismatch | IKE_LOG |
| 31 | 2017-09-11 ... | info | IKE | Send:[HASH][SA][NONCE][ID][ID] | IKE_LOG |
| 32 | 2017-09-11 ... | info | IKE | Phase 1 IKE SA process done | IKE_LOG |

Make sure the all ZyWALL/USG units' security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

By default, NAT traversal is enabled on ZyWALL/USG, so please make sure the remote IPSec device also has NAT traversal enabled.

How to Use Dual-WAN to Perform Fail-Over on VPN Using the VPN Concentrator

This is an example of using Dual-WAN to perform fail-over on a hub-and-spoke VPN with the HQ ZyWALL/USG as the hub and spoke VPNs to Branches A and B. When the VPN tunnel is configured, traffic passes between branches via the hub (HQ). Traffic can also pass between spoke-and-spoke through the hub. If the primary WAN interface is unavailable, the backup WAN interface will be used. When the primary WAN interface is available again, traffic will use that interface again.



Hub & Spoken VPN Using the VPN Concentrator with Backup

Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the IPSec VPN Tunnel on the ZyWALL/USG Hub_HQ-to-Branch_A

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway**, select **Enable**. Type the **VPN Gateway Name** used to identify this VPN gateway.

Then, configure the **Primary** Gateway IP as the **Branch A's wan1** IP address (in the example, 172.16.20.1) and **Secondary** Gateway IP as the **Branch A's wan2** IP address (in the example, 172.100.120.1). Select **Fall back to Primary Peer Gateway when possible** and set desired **Fall Back Check Interval** time.

Type a secure **Pre-Shared Key** (8-32 characters) which must match your **Branch A's** Pre-Shared Key and click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway

General Settings

☒ Enable

VPN Gateway Name: Hub_HQ-to-Branch_A

IKE Version

☒ IKEv1

☐ IKEv2

Gateway Settings

My Address

☒ Interface ge2 DHCP client -- 172.16.10.1/255.255.255.

☐ Domain Name / IPv4

Peer Gateway Address

☒ Static Address

Primary 172.16.20.1

Secondary 172.100.120.1

☒ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: 300 (60-86400 seconds)

☐ Dynamic Address

Authentication

☒ Pre-Shared Key

.....

unmasked

☐ Certificate

default

(See [My Certificates](#))

☐ User Based PSK

admin

☐ Advance

Phase 1 Settings

SA Life Time:

86400

(180 - 3000000 Seconds)

Negotiation Mode:

Main

☐ Advance

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** and select **Enable**. Type the **Connection Name** used to identify this VPN connection. Select scenario as **Site-to-site** and VPN Gateway which is configured in Step 1.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > General Settings and VPN Gateway

General Settings

☒ Enable

Connection Name:

Hub_HQ-to-Branch_A

☐ Advance

VPN Gateway

Application Scenario

☒ Site-to-site
 ☐ Site-to-site with Dynamic Peer
 ☐ Remote Access (Server Role)
 ☐ Remote Access (Client Role)
 ☐ Vpn Tunnel Interface

VPN Gateway:

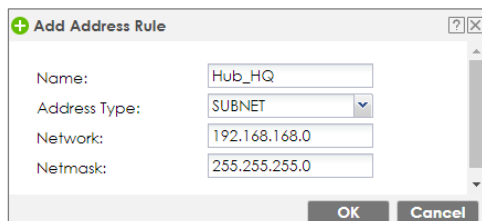
Hub_HQ-to-Branch_A

ge2 172.16.20.1, 172.100.120.1

Click **Create new Object** to add the address of local network behind **Hub_HQ** and an address of local network behind **Branch A**.

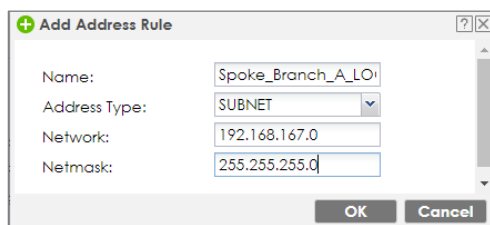
CONFIGURATION > VPN > IPSec VPN > VPN Connection > Create new Object

Local Policy



Dialog box titled "Add Address Rule" with fields for Name, Address Type, Network, and Netmask. The Name field is set to "Hub_HQ", Address Type is "SUBNET", Network is "192.168.168.0", and Netmask is "255.255.255.0". There are OK and Cancel buttons at the bottom.

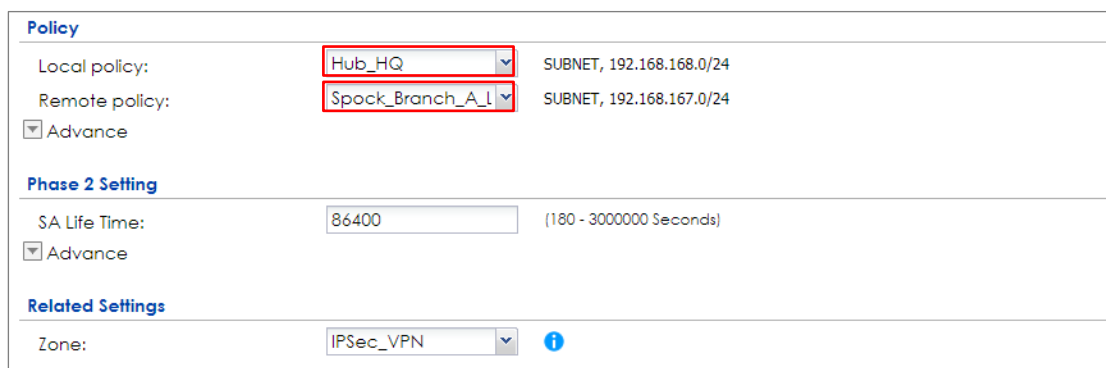
Remote Policy




Dialog box titled "Add Address Rule" with fields for Name, Address Type, Network, and Netmask. The Name field is set to "Spoke_Branch_A_L...", Address Type is "SUBNET", Network is "192.168.167.0", and Netmask is "255.255.255.0". There are OK and Cancel buttons at the bottom.

Set **Local Policy** to be **Hub_HQ** and **Remote Policy** to **Branch_A** which are newly created. Click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Policy



Policy configuration page with sections: Policy, Phase 2 Setting, and Related Settings. The Local policy is set to "Hub_HQ" and the Remote policy is set to "Spock_Branch_A_L". The SA Life Time is set to 86400 seconds. The Zone is set to "IPSec_VPN".

| Policy | | |
|---|------------------|---|
| Local policy: | Hub_HQ | SUBNET, 192.168.168.0/24 |
| Remote policy: | Spock_Branch_A_L | SUBNET, 192.168.167.0/24 |
| <input checked="" type="checkbox"/> Advance | | |
| Phase 2 Setting | | |
| SA Life Time: | 86400 | (180 - 3000000 Seconds) |
| <input checked="" type="checkbox"/> Advance | | |
| Related Settings | | |
| Zone: | IPSec_VPN |  |

Hub_HQ-to-Branch_B

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway**, select **Enable**. Type the **VPN Gateway Name** used to identify this VPN gateway.

Then, configure the **Primary** Gateway IP as the **Branch B's wan1** IP address (in the example, 172.16.30.1) and **Secondary** Gateway IP as the **Branch B's wan2** IP address (in the example, 172.100.130.1). Select **Fall back to Primary Peer Gateway when possible** and set desired **Fall Back Check Interval** time.

Type a secure **Pre-Shared Key** (8-32 characters) which must match your **Branch A's** Pre-Shared Key and click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway

General Settings

☒ Enable

VPN Gateway Name:

Hub_HQ-to-Branch_B

IKE Version

☒ IKEv1
 ☐ IKEv2

Gateway Settings

My Address

☒ Interface

ge2

 DHCP client -- 172.16.10.1/255.255.255.

☐ Domain Name / IPv4

Peer Gateway Address

☒ Static

Primary

172.16.30.1

Secondary

172.100.130.1

☒ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval:

300

(60-86400 seconds)

| Authentication | |
|---|--|
| <input checked="" type="radio"/> Pre-Shared Key | |
| <input type="checkbox"/> unmasked | |
| <input type="radio"/> Certificate | default (See My Certificates) |
| <input type="radio"/> User Based PSK | admin |
| <input type="checkbox"/> Advance | |
| Phase 1 Settings | |
| SA Life Time: | 86400 (180 - 3000000 Seconds) |
| Negotiation Mode: | Main |
| <input type="checkbox"/> Advance | |

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** to enable VPN Connection. Select scenario as **Site-to-site** and VPN Gateway which is configured in Step 1.

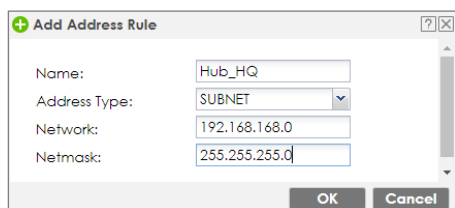
CONFIGURATION > VPN > IPSec VPN > VPN Connection > General Settings and VPN Gateway

| General Settings | |
|--|---|
| <input checked="" type="checkbox"/> Enable | |
| Connection Name: | Hub_HQ-to-Branch_B |
| <input type="checkbox"/> Advance | |
| VPN Gateway | |
| Application Scenario | |
| <input checked="" type="radio"/> Site-to-site | |
| <input type="radio"/> Site-to-site with Dynamic Peer | |
| <input type="radio"/> Remote Access (Server Role) | |
| <input type="radio"/> Remote Access (Client Role) | |
| <input type="radio"/> Vpn Tunnel Interface | |
| VPN Gateway: | Hub_HQ-to-Branch ge2 172.16.30.1, 172.100.130.1 |

Click **Create new Object** to add an address of local network behind **Hub_HQ** and an address of local network behind **Branch B**.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Create new Object

Local Policy

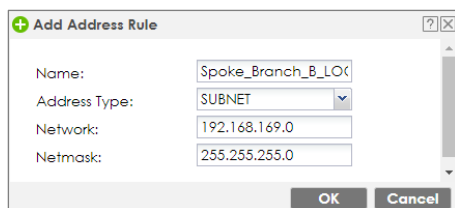


The 'Add Address Rule' dialog box is shown with the following fields:

- Name: Hub_HQ
- Address Type: SUBNET
- Network: 192.168.168.0
- Netmask: 255.255.255.0

Buttons: OK, Cancel

Remote Policy



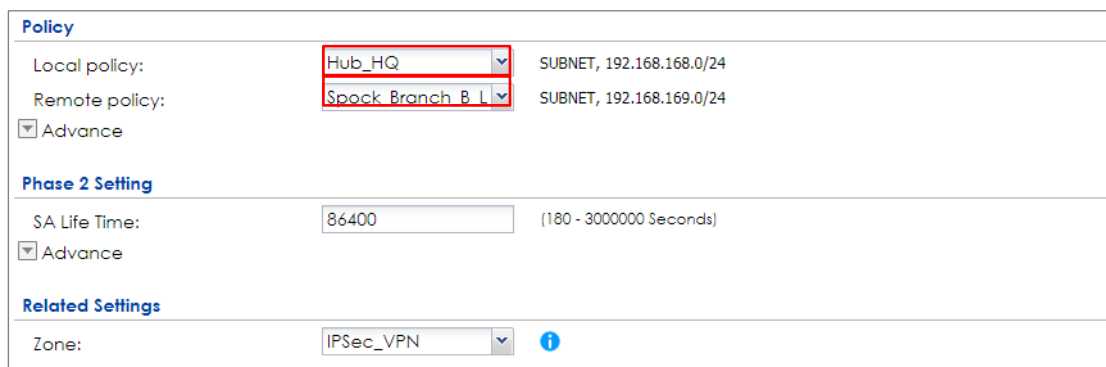
The 'Add Address Rule' dialog box is shown with the following fields:

- Name: Spoke_Branch_B_LO
- Address Type: SUBNET
- Network: 192.168.169.0
- Netmask: 255.255.255.0

Buttons: OK, Cancel

Set **Local Policy** to be **Hub_HQ** and **Remote Policy** to **Branch_B** which are newly created. Click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Policy



The 'Policy' configuration page is shown with the following settings:

- Local policy:** Hub_HQ (selected from dropdown)
- Remote policy:** Spoke_Branch_B_L (selected from dropdown)
- Advance:** (checkbox checked)
- Phase 2 Setting:**
 - SA Life Time:** 86400 (180 - 3000000 Seconds)
 - Advance:** (checkbox checked)
- Related Settings:**
 - Zone:** IPSec_VPN (selected from dropdown)

Hub_HQ Concentrator

In the ZyWALL/USG, go to **CONFIGURATION > VPN > IPsec VPN > Concentrator**, add a VPN Concentrator rule. Select VPN tunnels to the same member group and click **Save**.

+ Add VPN Concentrator

Name: Hub-and-Spoke

Available

VPN_to_VPC
VPN_to_Azure
WIZ_VPN_HQ
WIZ_VPN_Branch
Hub_HQ_to_Branch_A
Hub_HQ_to_Branch_B

Member

+ Add VPN Concentrator

Name:

Hub-and-Spoke

Available

VPN_to_VPC
VPN_to_Azure
Hub_HQ_to_Branch_B
WIZ_VPN_Branch
Spoke_Branch_A
Spoke_Branch_B
Hub_HQ_to_Branch_A

↑

↑

→

←

↓

⌵

Member

Hub_HQ-to-Branch_A
Hub HQ-to-Branch B

Spoke_Branch_A

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway**, select **Enable**. Type the **VPN Gateway Name** used to identify this VPN gateway.

Then, configure the **Primary** Gateway IP as the **Hub_HQ's wan1** IP address (in the example, 172.16.10.1) and **Secondary** Gateway IP as the **Hub_HQ's wan2** IP address (in the example, 172.100.110.1). Select **Fall back to Primary Peer Gateway when possible** and set desired **Fall Back Check Interval** time.

Type a secure **Pre-Shared Key** (8-32 characters) which must match your **Hub_HQ's** Pre-Shared Key and click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway

General Settings

☒ Enable

VPN Gateway Name:

IKE Version

☒ IKEv1
 ☐ IKEv2

Gateway Settings

My Address

☒ Interface DHCP client -- 172.16.20.1/255.255.255.
 ☐ Domain Name / IPv4

Peer Gateway Address

☒ Static Address

Primary
Secondary

☒ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: (60-86400 seconds)

☐ Dynamic Address

Authentication

☒ Pre-Shared Key

.....

unmasked

☐ Certificate

default

(See [My Certificates](#))

☐ User Based PSK

Remote_Client

☐ Advance

Phase 1 Settings

SA Life Time:

86400

(180 - 3000000 Seconds)

Negotiation Mode:

Main

☐ Advance

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** and select **Enable**. Type the **Connection Name** used to identify this VPN connection. Select scenario as **Site-to-site** and VPN Gateway which is configured in Step 1.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > General Settings and VPN Gateway

General Settings

☒ Enable

Connection Name:

Spoke_Branch_A

☐ Advance

VPN Gateway

Application Scenario

☒ Site-to-site

☐ Site-to-site with Dynamic Peer
 ☐ Remote Access (Server Role)
 ☐ Remote Access (Client Role)
 ☐ Vpn Tunnel Interface

VPN Gateway:

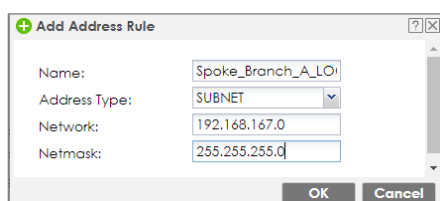
Spoke_Branch_A

ge2 172.16.10.1, 172.100.110.1

Click **Create new Object** to add the address of local network behind **Branch A** and an address of local network behind **Hub_HQ**

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Create new Object

Local Policy

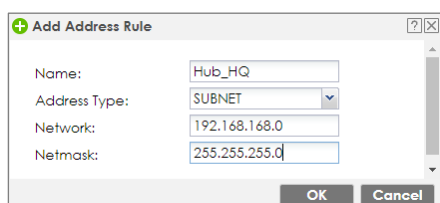


The 'Add Address Rule' dialog box is shown with the following fields:

- Name: Spoke_Branch_A_LO
- Address Type: SUBNET
- Network: 192.168.167.0
- Netmask: 255.255.255.0

Buttons: OK, Cancel

Remote Policy



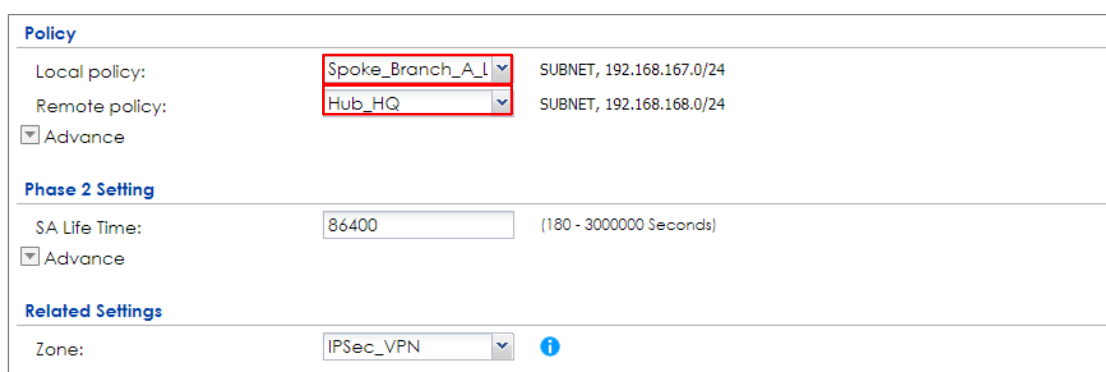
The 'Add Address Rule' dialog box is shown with the following fields:

- Name: Hub_HQ
- Address Type: SUBNET
- Network: 192.168.168.0
- Netmask: 255.255.255.0

Buttons: OK, Cancel

Set **Local Policy** to be **Spoke_Branch_A_LOCAL** and **Remote Policy** to **Hub_HQ** which are newly created. Click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Policy



The 'Policy' configuration page is shown with the following settings:

- Local policy:** Spoke_Branch_A_L (highlighted with a red box)
- Remote policy:** Hub_HQ (highlighted with a red box)
- Advance:** ☒ Advance
- Phase 2 Setting:**
 - SA Life Time: 86400 (180 - 3000000 Seconds)
 - Advance:** ☒ Advance
- Related Settings:**
 - Zone: IPSec_VPN

Go to **Network > Routing > Policy Route** to add a **Policy Route** to allow traffic from **Spoke_Branch_A** to **Spoke_Branch_B**.

Click **Create new Object** and set the address to be the local network behind the **Spoke_Branch_B**. Select **Source Address** to be the local network behind the **Spoke_Branch_A**. Then, scroll down the **Destination Address** list to choose the newly created **Spoke_Branch_B_LOCAL** address. Click **OK**.

Network > Routing > Policy Route

| Criteria | |
|----------------------|---------------------|
| User: | any |
| Incoming: | any (Excluding ZyV) |
| Source Address: | Spoke_Branch_A_L |
| Destination Address: | Spoke_Branch_B_L |
| DSCP Code: | any |
| Schedule: | none |
| Service: | any |
| Next-Hop | |
| Type: | VPN Tunnel |
| VPN Tunnel: | Spoke_Branch_A |

Spoke_Branch_B

Go to **CONFIGURATION > VPN > IPsec VPN > VPN Gateway**, select **Enable**. Type the **VPN Gateway Name** used to identify this VPN gateway.

Then, configure the **Primary** Gateway IP as the **Hub_HQ**'s **wan1** IP address (in the example, 172.16.10.1) and **Secondary** Gateway IP as the **Hub_HQ**'s **wan2** IP

address (in the example, 172.100.110.1). Select **Fall back to Primary Peer Gateway when possible** and set desired **Fall Back Check Interval** time.

Type a secure **Pre-Shared Key** (8-32 characters) which must match your **Hub_HQ**'s Pre-Shared Key and click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway

General Settings

☒ Enable

VPN Gateway Name:

IKE Version
☒ IKEv1
☐ IKEv2

Gateway Settings

My Address
☒ Interface DHCP client -- 172.16.30.1/255.255.255.
☐ Domain Name / IPv4

Peer Gateway Address
☒ Static Address ?

Primary
Secondary

☒ Fall back to Primary Peer Gateway when possible
Fall Back Check Interval: (60-86400 seconds)
☐ Dynamic Address ?

Authentication

☒ Pre-Shared Key
☐ unmasked

☐ Certificate (See [My Certificates](#))
☐ User Based PSK ?

☒ Advance

Phase 1 Settings

SA Life Time: (180 - 3000000 Seconds)
Negotiation Mode:
☒ Advance

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** and select **Enable**.

Type the **Connection Name** used to identify this VPN connection. Select scenario as **Site-to-site** and VPN Gateway which is configured in Step 1.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > General Settings and VPN Gateway

General Settings

☒ Enable

Connection Name:

☒ Advance

VPN Gateway

Application Scenario

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

☐ Vpn Tunnel Interface

VPN Gateway: ge2 172.16.10.1, 172.100.110.1

Click **Create new Object** to add the address of local network behind **Branch B** and an address of local network behind **Hub_HQ**.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Create new Object

Local Policy

Add Address Rule

Name:

Address Type:

Network:

Netmask:

Remote Policy

Add Address Rule

Name:


Address Type:

Network:

Netmask:

Set **Local Policy** to be **Spoke_Branch_B_LOCAL** and **Remote Policy** to **Hub_HQ** which are newly created. Click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Policy

| Policy | | |
|---|-------------------------------|---|
| Local policy: | Spoke_Branch_B_L | SUBNET, 192.168.169.0/24 |
| Remote policy: | Hub_HQ | SUBNET, 192.168.168.0/24 |
| <input checked="" type="checkbox"/> Advance | | |
| Phase 2 Setting | | |
| SA Life Time: | 86400 | (180 - 3000000 Seconds) |
| <input checked="" type="checkbox"/> Advance | | |
| Related Settings | | |
| Zone: | IPSec_VPN |  |

Go to **Network > Routing > Policy Route** to add a Policy Route to allow traffic from **Spoke_Branch_B** to **Spoke_Branch_A**.

Click **Create new Object** and set the address to be the local network behind the **Spoke_Branch_A**. Select **Source Address** to be the local network behind the **Spoke_Branch_B**. Then, scroll down the **Destination Address** list to choose the newly created **Spoke_Branch_A_LOCAL** address. Click **OK**.

Network > Routing > Policy Route

| Criteria | |
|----------------------|----------------------------------|
| User: | any |
| Incoming: | any (Excluding ZyV) |
| Source Address: | Spoke_Branch_B_L |
| Destination Address: | Spoke_Branch_A_L |
| DSCP Code: | any |
| Schedule: | none |
| Service: | any |
| Next-Hop | |
| Type: | VPN Tunnel |
| VPN Tunnel: | Spoke_Branch_B |

Test the IPsec VPN Tunnel

Go to ZyWALL/USG **CONFIGURATION > VPN > IPsec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

Hub_HQ > CONFIGURATION > VPN > IPsec VPN > VPN Connection

| IPv4 Configuration | | | | |
|--|--------|--------------------|--------------------|---|
| Add Edit Remove Activate Inactivate Connect Disconnect Object References | | | | |
| # | Status | Name | VPN Gateway | Policy |
| 1 | | Hub_HQ-to-Branch_A | Hub_HQ-to-Branch_A | Hub_HQ/Spoke_Branch_A_LOCAL |
| 2 | | Hub_HQ-to-Branch_B | Hub_HQ-to-Branch_B | Hub_HQ/Spoke_Branch_B_LOCAL |
| Page 1 of 1 Show 50 Items Displaying 1 - 2 of 2 | | | | |

Spoke_Branch_A > CONFIGURATION > VPN > IPsec VPN > VPN Connection

| IPv4 Configuration | | | | |
|--|--------|----------------|----------------|---|
| Add Edit Remove Activate Inactivate Connect Disconnect Object References | | | | |
| # | Status | Name | VPN Gateway | Policy |
| 1 | | Spoke-Branch_A | Spoke-Branch_A | Spoke-Branch_A_LOCAL/Hub_HQ |
| Page 1 of 1 Show 50 Items Displaying 1 - 1 of 1 | | | | |

Spoke_Branch_B > CONFIGURATION > VPN > IPsec VPN > VPN Connection

| IPv4 Configuration | | | | |
|--|--------|----------------|----------------|---|
| Add Edit Remove Activate Inactivate Connect Disconnect Object References | | | | |
| # | Status | Name | VPN Gateway | Policy |
| 1 | | Spoke-Branch_B | Spoke-Branch_B | Spoke-Branch_B_LOCAL/Hub_HQ |
| Page 1 of 1 Show 50 Items Displaying 1 - 1 of 1 | | | | |

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic. Click **Connectivity Check** to verify the result of ICMP Connectivity.

Hub_HQ > MONITOR > VPN Monitor > IPSec > Hub_HQ-to-Branch_A

| | | Disconnect | | Connection Check | | | | |
|---------------------------|--------------------|------------------------------------|-------------|------------------|---------|---------|-----------------------|-------------|
| # | Name | Policy | My Addr... | Secure Gatew... | Up Time | Timeout | Inbound(...) | Outbound... |
| 1 | Hub_HQ-to-Branch_A | 192.168.168.0/24<>192.168.167.0/24 | 172.16.10.1 | P: 172.16.20.1 | 690 | 85730 | 1(46 bytes) | 1(60 bytes) |
| 2 | Hub_HQ-to-Branch_B | 192.168.168.0/24<>192.168.169.0/24 | 172.16.10.1 | P: 172.16.30.1 | 505 | 85915 | 1(78 bytes) | 0(0 bytes) |
| Page 1 of 1 Show 50 items | | | | | | | Displaying 1 - 2 of 2 | |

Connectivity Check

Connectivity Check

IP Address: 192.168.167.1

OK Cancel

Result

ICMP Connectivity Check PASS on Hub_HQ-to-Branch_A

OK

Hub_HQ > MONITOR > VPN Monitor > IPSec > Hub_HQ-to-Branch_B

| | | Disconnect | | Connection Check | | | | |
|---|--------------------|------------------------------------|-------------|------------------|---------|---------|--------------|-------------|
| # | Name | Policy | My Addr... | Secure Gatew... | Up Time | Timeout | Inbound(...) | Outbound... |
| 1 | Hub_HQ-to-Branch_A | 192.168.168.0/24<>192.168.167.0/24 | 172.16.10.1 | P: 172.16.20.1 | 690 | 85730 | 1(46 bytes) | 1(60 bytes) |
| 2 | Hub_HQ-to-Branch_B | 192.168.168.0/24<>192.168.169.0/24 | 172.16.10.1 | P: 172.16.30.1 | 505 | 85915 | 1(78 bytes) | 0(0 bytes) |

◀◀

Page 1

of 1

▶▶

Show

50

items

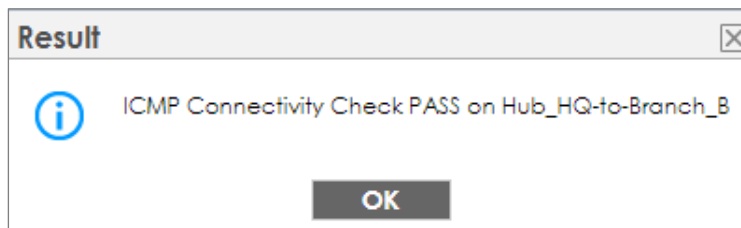
Displaying 1 - 2 of 2

Connectivity Check

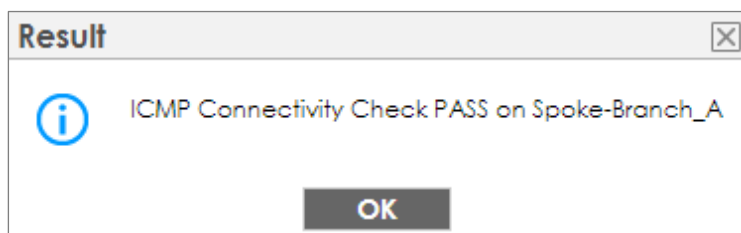
Connectivity Check

IP Address: 192.168.169.1

OK Cancel

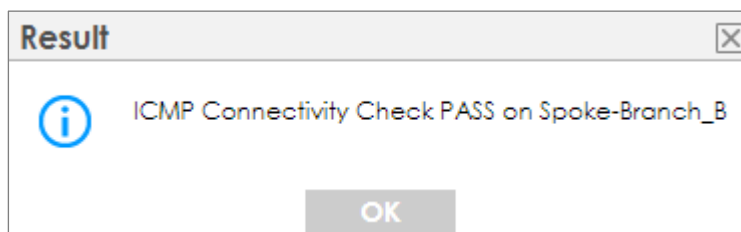
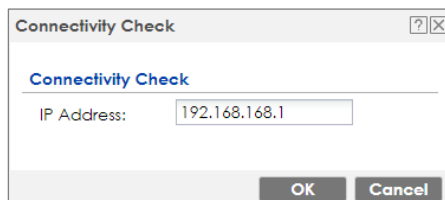


Spoke_Branch_A > MONITOR > VPN Monitor > IPSec



Spoke_Branch_B > MONITOR > VPN Monitor > IPSec

| Disconnect | | Connection Check | | | | | | |
|-----------------------------------|----------------|------------------------------------|-------------|----------------|---------|---------|--------------|-----------------------|
| # | Name | Policy | My Address | Secure Ga... | Up Time | Timeout | Inbound(B... | Outbound(... |
| 1 | Spoke_Branch_B | 192.168.169.0/24<>192.168.168.0/24 | 172.16.30.1 | P: 172.16.10.1 | 4 | 73436 | 0(0 bytes) | 0(0 bytes) |
| < < Page 1 of 1 > > Show 50 Items | | | | | | | | Displaying 1 - 1 of 1 |



What Could Go Wrong?

If you see [info] or [error] log message such as below, please check ZyWALL/USG Phase 1 Settings. All ZyWALL/USG units must use the same Pre-Shared Key, Encryption, Authentication method, DH key group and ID Type to establish the IKE SA.

| Priority | Category | Message | Note |
|----------|----------|--|---------|
| info | IKE | Recv:[NOTIFY:INVALID_COOKIE] | IKE_LOG |
| info | IKE | Send:[ID][HASH][NOTIFY:INITIAL_CONTACT] | IKE_LOG |
| Priority | Category | Message | Note |
| error | IPSec | SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet | IPSec |
| error | IPSec | SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet | IPSec |
| info | IKE | [COOKIE] Invalid cookie, no sa found | IKE_LOG |
| Priority | Category | Message | Note |
| info | IKE | Recv:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN] | IKE_LOG |

If you see that Phase 1 IKE SA process done but still get [info] log message as below, please check ZyWALL/USG Phase 2 Settings. All ZyWALL/USG units must use the same Protocol, Encapsulation, Encryption, Authentication method and PFS to establish the IKE SA.

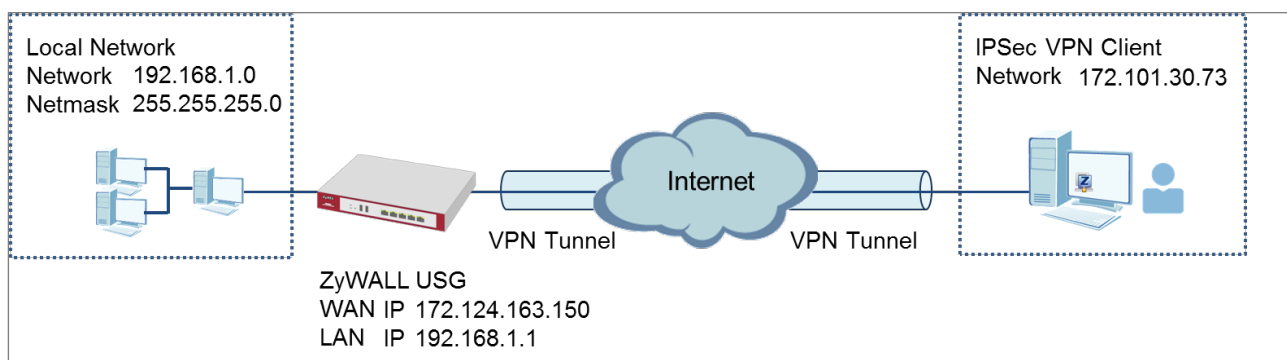
| | | | | | |
|----|----------------|------|-----|--|---------|
| 19 | 2017-09-11 ... | info | IKE | [SA] : No proposal chosen | IKE_LOG |
| 20 | 2017-09-11 ... | info | IKE | [ID] : Tunnel [Server] Phase 2 Local policy mismatch | IKE_LOG |
| 31 | 2017-09-11 ... | info | IKE | Send:[HASH][SA][NONCE][ID][ID] | IKE_LOG |
| 32 | 2017-09-11 ... | info | IKE | Phase 1 IKE SA process done | IKE_LOG |


Make sure the all ZyWALL/USG units' security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

By default, NAT traversal is enabled on ZyWALL/USG, so please make sure the remote IPSec device also has NAT traversal enabled.

How to Configure IPsec VPN with ZyWALL IPsec VPN Client

This example shows how to use the VPN Setup Wizard to create a site-to-site VPN between a ZyWALL/USG and a ZyWALL IPsec VPN Client. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25) and ZyWALL IPsec VPN

ZyWALL IPsec VPN Client with VPN Tunnel Connected

Set Up the ZyWALL/USG IPSec VPN Tunnel

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings for Configuration Provisioning** wizard to create a VPN rule that can be used with the ZyWALL IPSec VPN Client. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Welcome

- ☐ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☒ **VPN Settings for Configuration Provisioning**
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Please select the type of VPN policy you wish to setup.

Type of VPN policy

- ☒ **Express**
- ☐ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway).
You may use 1-31 alphanumeric characters. This value is case-sensitive. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings-1

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name: WIZ_VPN_PROVISIONING

Application Scenario: Remote Access (Server Role)

Type a secure **Pre-Shared Key** (8-32 characters). Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings-2

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Express Settings

Configuration

Secure Gateway: Any

Pre-Shared Key: zyx12345

Local Policy (IP/Mask): 192.168.1.33 / 255.255.255.0

Remote Policy (IP/Mask): Any

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings-3

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Summary

Rule Name: WIZ_VPN_PROVISIONING

Secure Gateway: Any

Pre-Shared Key: zyx12345

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): Any

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Congratulations. The VPN Access wizard is completed

Summary

Rule Name: WIZ_VPN_PROVISIONING

Secure Gateway: Any

Pre-Shared Key: zyx12345

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): Any

Go to **CONFIGURATION > Object > User/Group > Add A User** and create a user account for the ZyWALL IPSec VPN Client user.

CONFIGURATION > Object > User/Group > Add A User

User Configuration

User Name : Remote_Client

User Type: user

Password:

Retype:

Description: Local User

Authentication Timeout Settings

☒ Use Default Settings
☐ Use Manual Settings

Lease Time: 1440 minutes

Reauthentication Time: 1440 minutes

Go to **CONFIGURATION > VPN > IPSec VPN > Configuration Provisioning**. In the **General Settings** section, select the **Enable Configuration Provisioning**. Then, go to the **Configuration** section and click **Add** to bind a configured **VPN Connection** to **Allowed User**. Click **Activate** and **Apply** to save the configuration.

CONFIGURATION > VPN > IPSec VPN > Configuration Provisioning

General Settings

☒ Enable Configuration Provisioning

Authentication

Client Authentication Method: default

Configuration

Add Edit Remove Activate Inactivate Move

| # | Status | Priority | Type | VPN Connection | Allowed User |
|---|--------|----------|------|----------------------|---------------|
| 1 | | 1 | 4in4 | WIZ_VPN_PROVISIONING | Remote_Client |

Page 1 of 1 Show 50 items

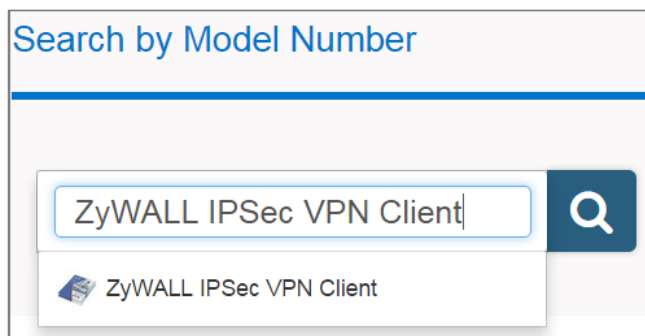
Apply

Reset

Set Up the ZyWALL IPSec VPN Client

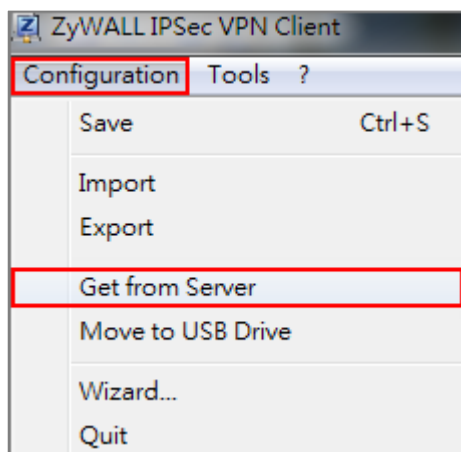
Download **ZyWALL IPSec VPN Client** software from ZyXEL Download Library:

http://www.zyxel.com/support/download_landing.shtml



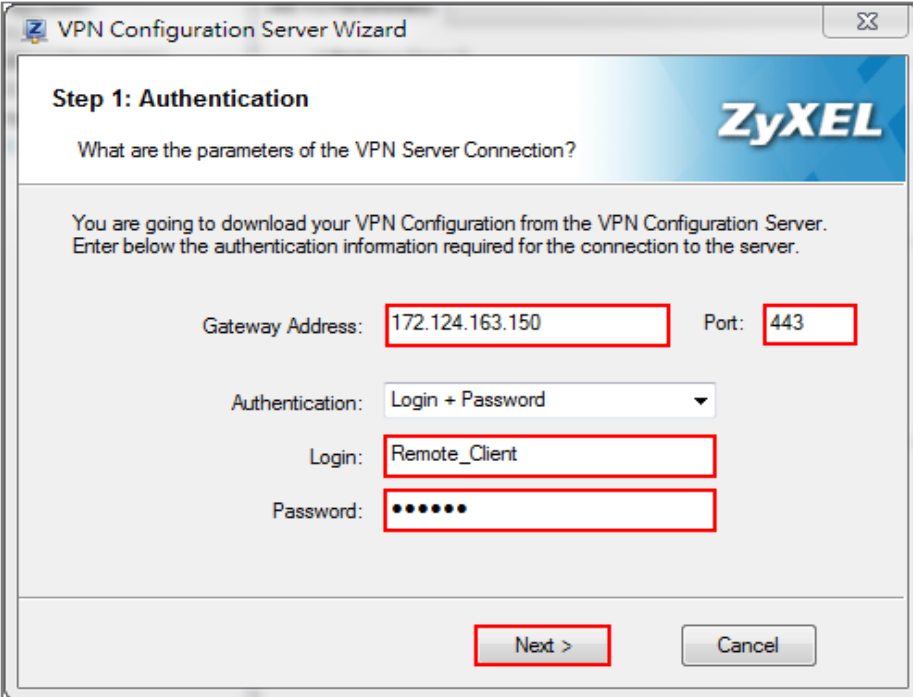
Open ZyWALL IPSec VPN Client, select **CONFIGURATION > Get from Server**.

CONFIGURATION > Get from Server



Enter the WAN IP address or URL for the ZyWALL/USG in the **Gateway Address**. If you changed the default HTTPS **Port** on the ZyWALL/USG, and then enter the new one here. Enter the **Login** user name and **Password** exactly as configured on the ZyWALL or external authentication server. Click **Next**, you will see it's processing VPN configuration from the server.

CONFIGURATION > Get from Server > Step 1: Authentication



VPN Configuration Server Wizard

Step 1: Authentication

What are the parameters of the VPN Server Connection?

You are going to download your VPN Configuration from the VPN Configuration Server.
Enter below the authentication information required for the connection to the server.

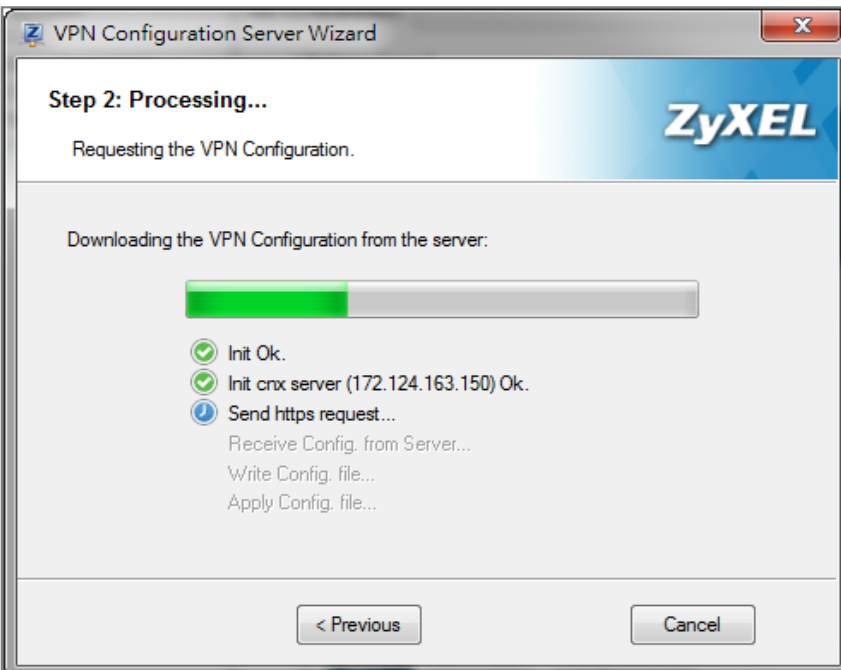
Gateway Address: Port:

Authentication:

Login:

Password:

CONFIGURATION > Get from Server > Step 2: Processing



VPN Configuration Server Wizard

Step 2: Processing...

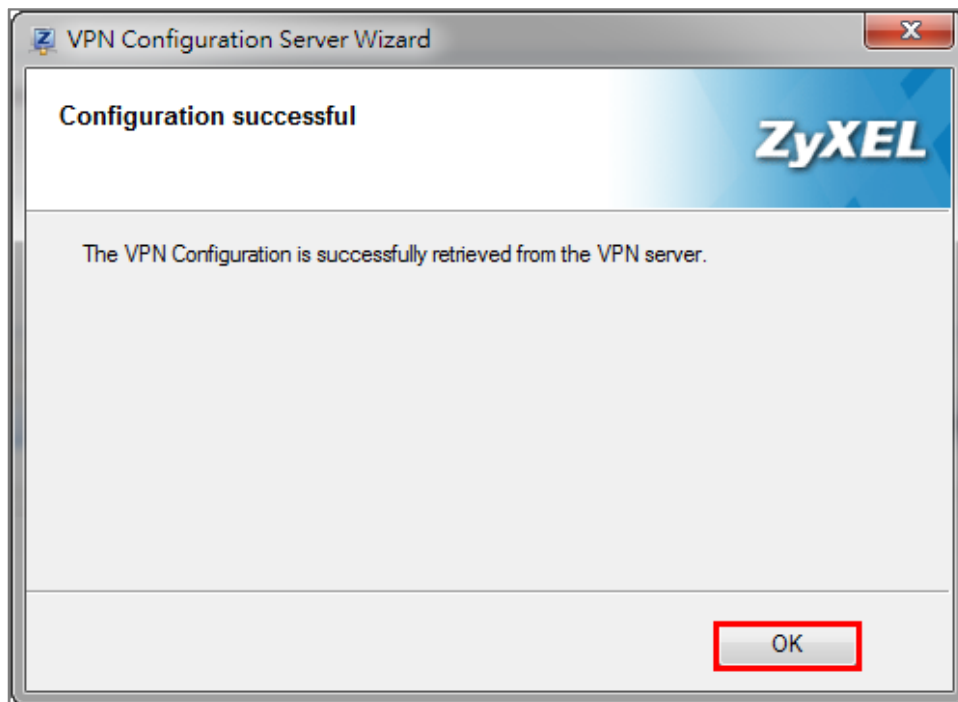
Requesting the VPN Configuration.

Downloading the VPN Configuration from the server:

- ☒ Init Ok.
- ☒ Init crx server (172.124.163.150) Ok.
- ☒ Send https request...
- ☐ Receive Config. from Server...
- ☐ Write Config. file...
- ☐ Apply Config. file...

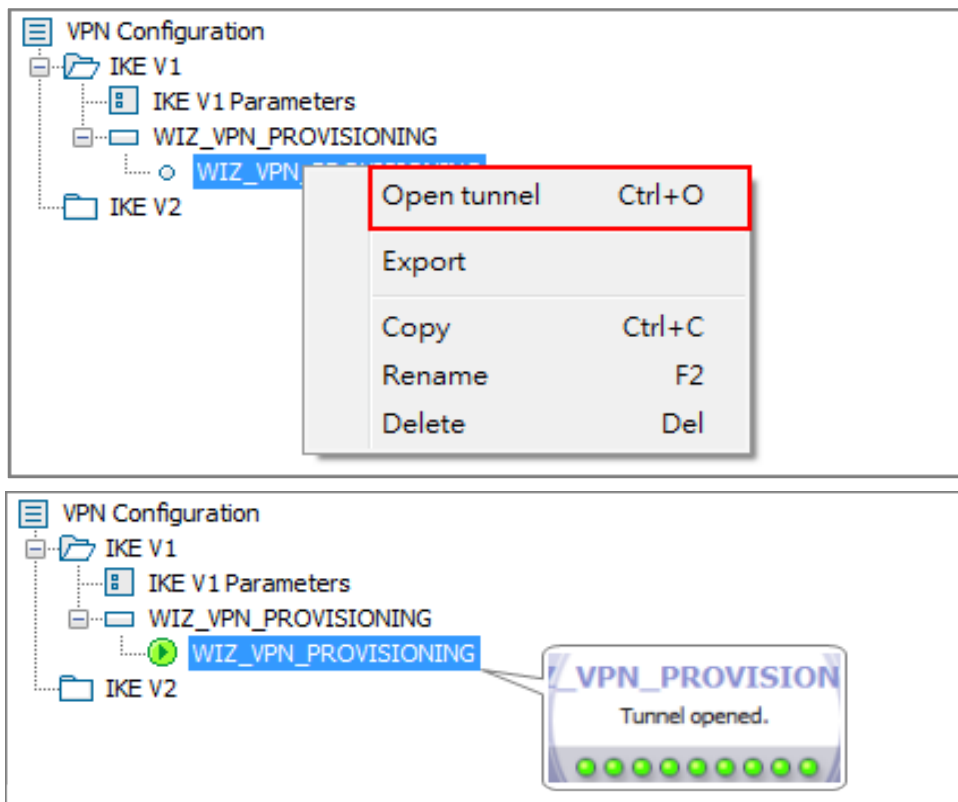
Then, you will see the **Configuration successful** page, click **OK** to exit the wizard.

CONFIGURATION > Get from Server > Configuration successful



Go to **VPN Configuration > IKEv1**, right click the **WIZ_VPN_PROVISIONING** and select **Open tunnel**. You will see the **Tunnel opened** on the bottom right of the screen.

VPN CONFIGURATION > IKE V1 > WIZ_VPN_PROVISIONING > Open tunnel



Test the IPSec VPN Tunnel

Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, the **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

| IPv4 Configuration | | | | |
|--|--------|----------------------|----------------------|---|
| Add Edit Remove Activate Inactivate Connect Disconnect Object References | | | | |
| # | Status | Name | VPN Gateway | Policy |
| 1 | | WIZ_VPN_PROVISIONING | WIZ_VPN_PROVISIONING | WIZ_VPN_PROVISIONING_LOCAL/ |
| Page 1 of 1 Show 50 Items Displaying 1 - 1 of 1 | | | | |

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and **Inbound(Bytes)/Outbound(Bytes)** Traffic.

MONITOR > VPN Monitor > IPSec

| Disconnect | | Connection Check | | | | | | | | |
|------------|-----|------------------|----------------------|--------------------------------|----------------|-----------------|---------|---------|----------------|-----------------|
| # | S | Sy | Name | Policy | My Address | Secure Gateway | Up Time | Timeout | Inbound(Bytes) | Outbound(Bytes) |
| 1 | N/A | N/A | WIZ_VPN_PROVISIONING | 192.168.1.0/24<=>172.101.30.73 | 172.101.30.150 | D:172.101.30.73 | 6 | 86414 | 21(1854 bytes) | 0(0 bytes) |

To test whether or not a tunnel is working, ping from a computer at one site to a computer at the other. Ensure that both computers have Internet access (via the IPSec devices).

PC with ZyWALL IPSec VPN Client installed > Window 7 > cmd > ping 192.168.1.33

```
C:\Documents and Settings\ZYXEL>ping 192.168.1.33

Pinging 192.168.1.33 with 32 bytes of data:

Reply from 192.168.1.33: bytes=32 time=27ms TTL=43
Reply from 192.168.1.33: bytes=32 time=32ms TTL=43
Reply from 192.168.1.33: bytes=32 time=26ms TTL=43
Reply from 192.168.1.33: bytes=32 time=27ms TTL=43

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 32ms, Average = 28ms
```

PC behind ZyWALL/USG > Window 7 > cmd > ping 172.101.30.73

```
C:\Documents and Settings\ZYXEL>ping 172.101.30.73

Pinging 172.101.30.73 with 32 bytes of data:

Reply from 172.101.30.73: bytes=32 time=18ms TTL=54
Reply from 172.101.30.73: bytes=32 time=17ms TTL=54
Reply from 172.101.30.73: bytes=32 time=17ms TTL=54
Reply from 172.101.30.73: bytes=32 time=16ms TTL=54

Ping statistics for 172.101.30.73:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 18ms, Average = 17ms
```

What Can Go Wrong?

If you see [info] log message such as below, please make sure both ZyWALL/USG and ZyWALL IPSec VPN Client use the same **Pre-Shared Key** to establish the IKE SA.

MONITOR > Log

| Priority | Category | Message | Note |
|----------|----------|--|---------|
| info | IKE | Send:[NOTIFY:INVALID_PAYLOAD_TYPE] | IKE_LOG |
| info | IKE | Invalid payload type in encrypted payload chain, possibly because of different pre-shared keys | IKE_LOG |

If you see [info] or [error] log message such as below, please check ZyWALL/USG Phase 1 Settings. ZyWALL/USG and ZyWALL IPSec VPN Client must use the same Encryption, Authentication method, DH key group and ID Type/Content to establish the IKE SA.

MONITOR > Log

| | | | |
|------|-----|--|---------|
| info | IKE | [SA] : No proposal chosen | IKE_LOG |
| info | IKE | [SA] : Tunnel [WIZ_VPN_PROVISIONING] Phase 1 proposal mismatch | IKE_LOG |

If you see that Phase 1 IKE SA process done but still get [alert] or [info] log message as below, please check ZyWALL/USG Phase 2 Settings. ZyWALL/USG and ZyWALL IPSec VPN Client must use the same Active Protocol, Encapsulation, Proposal, PFS and set correct Local Policy to establish the IKE SA.

MONITOR > Log

| | | | |
|------|-----|--|---------|
| info | IKE | [SA] : No proposal chosen | IKE_LOG |
| info | IKE | [SA] : Tunnel [WIZ_VPN_PROVISIONING] Phase 2 proposal mismatch | IKE_LOG |

| | | | |
|------|-----|--|---------|
| info | IKE | [SA] : No proposal chosen | IKE_LOG |
| info | IKE | [ID] : Tunnel [WIZ_VPN_PROVISIONING] Phase 2 Local policy mismatch | IKE_LOG |

If you see [alert] log message as below, please make sure you create a user account for the ZyWALL IPSec VPN Client user on ZyWALL/USG or the external authentication server. Or please check your password matches the settings in the user account.

MONITOR > Log

| Priority | Cate... | Message | Note |
|----------|---------|--|------------------------|
| alert | User | Failed login attempt to Device from http/https (incorrect password or inexistent username) | Account: Remote_Client |

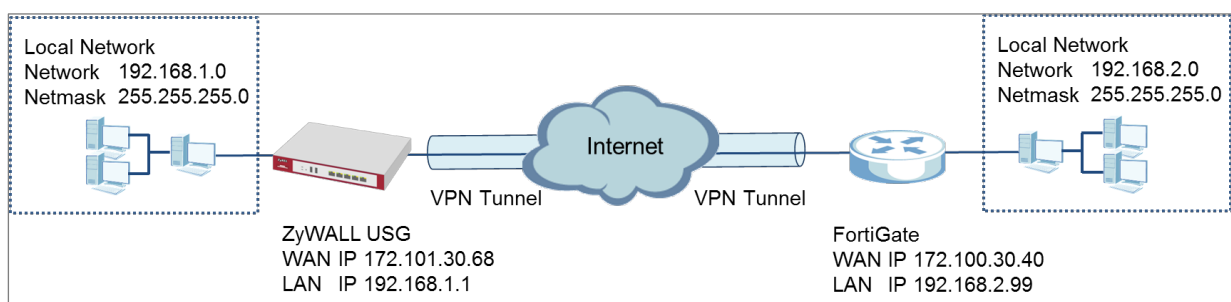
Make sure the service HTTPS **Port** on IPSec VPN Client application is available.

Make sure the To-ZyWALL security policies allow IPSec VPN traffic to the ZyWALL/USG. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.


The ZyWALL/USG supports UDP port 500 and UDP port 4500 for NAT traversal. If you enable this, make sure the To-ZyWALL security policies allow UDP port 4500 too.

How to Configure Site-to-site IPSec VPN with FortiGate

This example shows how to use the VPN Setup Wizard to create a site-to-site VPN between a ZYWALL/USG and a FortiGate router. The example instructs how to configure the VPN tunnel between each site. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



ZyWALL Site-to-site IPSec VPN with FortiGate Connected

 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25) and FortiGate 100D (Firmware Version: 6.2.0).

Set Up the IPSec VPN Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the FortiGate. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Please select the type of VPN policy you wish to setup.

Type of VPN policy

- ☒ Express
- ☐ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway).

You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name:

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

Configure **Secure Gateway** IP as the FortiGate's WAN IP address (in the example, 172.100.30.40). Then, type a secure **Pre-Shared Key** (8-32 characters).

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the FortiGate.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

Configuration

Secure Gateway: (IP or FQDN)

Pre-Shared Key:

Local Policy (IP/Mask): /

Remote Policy (IP/Mask): /

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

**Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings
(Summary)**

VPN Setup Wizard

Wizard Type

VPN Settings

Wizard Completed

1

2

3

Express Settings

Summary

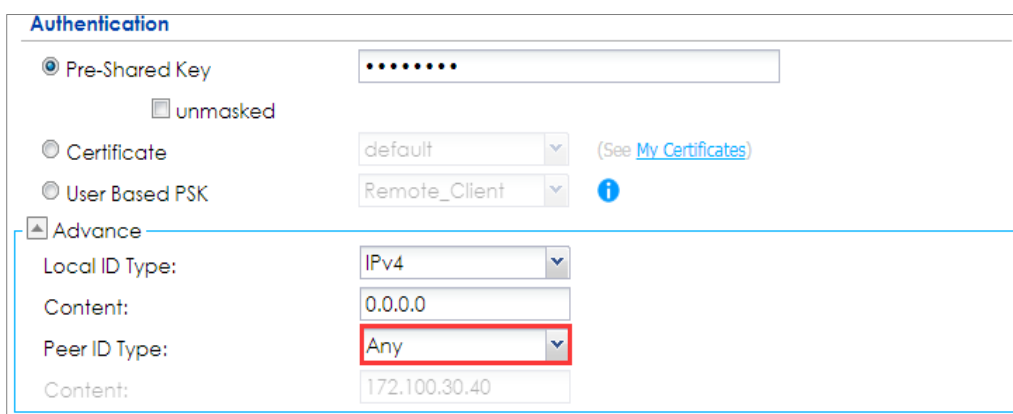
| | |
|--------------------------|-----------------------------|
| Rule Name: | WIZ_VPN_Fortigate |
| Secure Gateway: | 172.100.30.40 |
| Pre-Shared Key: | ZyXEL123 |
| Local Policy (IP/Mask): | 192.168.1.0 / 255.255.255.0 |
| Remote Policy (IP/Mask): | 192.168.2.0 / 255.255.255.0 |

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** and click **Show Advanced Settings**. Configure **Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPSec router.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type



The screenshot shows the 'Authentication' configuration page for a ZyXEL VPN Gateway. The 'Pre-Shared Key' is masked with dots. The 'Certificate' dropdown is set to 'default' and the 'User Based PSK' dropdown is set to 'Remote_Client'. The 'Advance' section is expanded, showing 'Local ID Type' as 'IPv4', 'Content' as '0.0.0.0', 'Peer ID Type' as 'Any' (highlighted with a red box), and 'Content' as '172.100.30.40'.

Set Up the IPSec VPN Tunnel on the FortiGate

In the FortiGate **VPN > IPsec > Wizard > Custom VPN Tunnel (No Template)**, use the **VPN Setup** to create a **Site-to-site VPN** rule **Name**.

VPN > IPsec > Wizard > Custom VPN Tunnel (No Template)



The screenshot shows the 'VPN Setup' wizard in FortiGate. The 'Name' field is set to 'WIZ_VPN_ZyWALL' (highlighted with a red box). The 'Template' section lists several options, with 'Custom VPN Tunnel (No Template)' selected (highlighted with a red box). The 'Back', 'Next >', and 'Cancel' buttons are visible at the bottom.

Type the **Name** used to identify this VPN connection, configure **Remote Gateway** IP as the peer ZyWALL/USG's WAN IP address. Select the **Interface** which is connected to the Internet.

VPN > IPsec > Wizard > Custom VPN Tunnel (No Template) > Network

Name WIZ_VPN_ZyWALL

Comments

Network

IP Version ☒ IPv4 ☐ IPv6

Remote Gateway Static IP Address

IP Address 172.101.30.68

Interface wan1

Mode Config ☐

NAT Traversal ☒

Keepalive Frequency

Dead Peer Detection ☒

Static IP Address
 Dialup User
 Dynamic DNS

Interface Selection:
 dmz
 ha1
 ha2
 lan
wan1
 wan2

Go to **Authentication** section, enter **Pre-shared Key** and choose negotiation **Mode** the same as the peer ZyWALL/USG's.

VPN > IPsec > Wizard > Custom VPN Tunnel (No Template) > Authentication

Authentication

Method Pre-shared Key

Pre-shared Key ZyXEL123 ☒ Show Key

IKE

Version ☒ 1 ☐ 2

Mode ☐ Aggressive ☒ Main (ID protection)

Configure Phase 1 Proposal and Diffie-Hellman Group as the peer ZyWALL/USG Advanced Settings' **Phase 1 Settings > Proposal** and **Key Group**.

VPN > IPsec > Wizard > Custom VPN Tunnel (No Template) > Phase 1 Proposal

Phase 1 Proposal

| Encryption | Authentication | Action |
|------------|----------------|--------|
| DES | MD5 | Add |
| AES256 | SHA256 | Remove |
| 3DES | SHA256 | Remove |
| AES128 | SHA1 | Remove |
| AES256 | SHA1 | Remove |
| 3DES | SHA1 | Remove |

Diffie-Hellman Group: ☐ 21 ☐ 20 ☐ 19 ☐ 18 ☐ 17 ☐ 16 ☒ 15 ☐ 14 ☐ 5 ☐ 2 ☒ 1

Key Lifetime (seconds): 86400

Local ID:

Go to **Phase 2 Selectors > Advanced** and configure **Phase 2 Proposal** as the peer ZyWALL/USG Advanced Settings' **Phase 2 Settings > Proposal**.

Set **Local Address** to be the IP address range of the network connected to the FortiGate and **Remote Address** to be the IP address range of the network connected to the ZyWALL/USG.

Make sure you uncheck **Enable Perfect Forward Secrecy (PFS)** if this function is disabled in the peer ZyWALL/USG.

VPN > IPsec > Wizard > Custom VPN Tunnel (No Template) > Phase 2 Selectors

Phase 2 Selectors

| Name | Local Address | Remote Address |
|----------------|---------------------------|---------------------------|
| WIZ_VPN_ZyWALL | 192.168.2.0/255.255.255.0 | 192.168.1.0/255.255.255.0 |

Edit Phase 2

Name

WIZ_VPN_ZyWALL

Comments

Comments

Local Address

Subnet

192.168.2.0/255.255.255.0

Remote Address

Subnet

192.168.1.0/255.255.255.0

Advanced...

Phase 2 Proposal

Encryption

DES

Authentication

SHA1

Remove

Encryption

AES256

Authentication

SHA1

Remove

Encryption

3DES

Authentication

SHA1

Remove

Encryption

AES128

Authentication

SHA256

Remove

Encryption

AES256

Authentication

SHA256

Remove

Encryption

3DES

Authentication

SHA256

Remove

Enable Replay Detection

☒

Enable Perfect Forward Secrecy (PFS)

☐

This screen provides a summary of the VPN tunnel. Click **OK** to exit the configuration page.

VPN > IPsec > Wizard > Custom VPN Tunnel (No Template)

Name
WIZ_VPN_ZyWALL
Comments
Comments

Network

IP Version
☒ IPv4 ☐ IPv6
Remote Gateway
Static IP Address
IP Address
172.101.30.68
Interface
wan1
Mode Config
☐
NAT Traversal
☒
Keepalive Frequency
10
Dead Peer Detection
☒

Authentication
Authentication Method : Pre-shared Key (Your_Pre-Shared_Key)
IKE Version : 1 , Mode : Main (ID protection)

Phase 1 Proposal
Algorithms : DES-MD5 AES256-SHA256, 3DES-SHA256, AES128-SHA1, AES256-SHA1, 3DES-SHA1
Diffie-Hellman Group 1

XAUTH
Type : Disabled

Phase 2 Selectors

| Name | Local Address | Remote Address | |
|----------------|----------------------------|---------------------------|-----|
| WIZ_VPN_ZyWALL | 192.168.2.99/255.255.255.0 | 192.168.1.1/255.255.255.0 | Add |

OK
Cancel

Test the IPsec VPN Tunnel

Go to ZyWALL/USG **CONFIGURATION > VPN > IPsec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPsec VPN > VPN Connection

| # | Status | Name | VPN Gateway | Policy |
|---|--------|-------------------|-------------------|--|
| 1 | | WIZ_VPN_FortiGate | WIZ_VPN_FortiGate | WIZ_VPN_Fortigate_Local/WIZ_VPN_Fortigate_REMOTE |

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPsec** and verify the tunnel **Up Time** and **Inbound(Bytes)/Outbound(Bytes)** traffic.

MONITOR > VPN Monitor > IPsec

| # | Serial Number | System Name | Name | Policy | My Address | Secure Gatew... | Up Time | Timeout | Inbound... | Outbound... |
|---|---------------|-------------|-------------------|-----------------|---------------|------------------|---------|---------|------------|-------------|
| 1 | N/A | N/A | WIZ_VPN_FortiGate | 192.168.1.0/... | 172.101.30.68 | P: 172.100.30.40 | 68 | 79132 | 0(0 bytes) | 0(0 bytes) |

Go to FortiGate **VPN > Monitor > IPsec Monitor** and check the tunnel **Status** is up and **Incoming Data/Outgoing Data** traffic.

VPN > Monitor > IPsec Monitor

| Name | Type | Remote Gateway | Status | Incoming Data | Outgoing Data |
|----------------|--------------------------|----------------|--------|---------------|---------------|
| WIZ_VPN_ZyWALL | Static IP or Dynamic DNS | 172.101.30.68 | Up | 8.09 KB | 13.78 KB |

To test whether or not a tunnel is working, ping from a computer at one site to a computer at the other. Ensure that both computers have Internet access (via the IPsec devices).

PC behind ZyWALL/USG > Window 7 > cmd > ping 192.168.2.33

```
C:\Documents and Settings\ZyXEL>ping 192.168.2.33

Pinging 192.168.2.33 with 32 bytes of data:

Reply from 192.168.2.33: bytes=32 time=27ms TTL=43
Reply from 192.168.2.33: bytes=32 time=32ms TTL=43
Reply from 192.168.2.33: bytes=32 time=26ms TTL=43
Reply from 192.168.2.33: bytes=32 time=27ms TTL=43

Ping statistics for 192.168.2.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 32ms, Average = 28ms
```

PC behind FortiGate> Window 7 > cmd > ping 192.168.1.33

```
C:\Documents and Settings\ZyXEL>ping 192.168.1.33

Pinging 192.168.1.33 with 32 bytes of data:

Reply from 192.168.1.33: bytes=32 time=27ms TTL=43
Reply from 192.168.1.33: bytes=32 time=32ms TTL=43
Reply from 192.168.1.33: bytes=32 time=26ms TTL=43
Reply from 192.168.1.33: bytes=32 time=27ms TTL=43

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 32ms, Average = 28ms
```

What Could Go Wrong?

If you see below [info] or [error] log message, please check ZyWALL/USG Phase 1 Settings. Both ZyWALL/USG and FortiGate must use the same Pre-Shared Key, Encryption, Authentication method, DH key group and ID Type to establish the IKE SA.

MONITOR > Log

| Priority | Category | Message | Note |
|----------|----------|--|---------|
| info | IKE | Send:[NOTIFY:NO_PROPOSAL_CHOSEN] | IKE_LOG |
| info | IKE | [SA] : No proposal chosen | IKE_LOG |
| info | IKE | [SA] : Tunnel [WIZ_VPN_FortiGate] Phase 1 proposal mismatch | IKE_LOG |
| info | IKE | The cookie pair is : 0x70fb3b31ed922dc4 / 0x07f7812272f2e1a2 [count=3] | IKE_LOG |
| info | IKE | Recv IKE sa: SA([0] protocol = IKE (1), AES CBC key len = 192, HMAC-SHA256 PRF, HMAC-SHA256-1... | IKE_LOG |

If you see that Phase 1 IKE SA process done but still get below [info] log message,

please check ZyWALL/USG and FortiGate Phase 2 Settings. Both ZyWALL/USG and FortiGate must use the same Protocol, Encapsulation, Encryption, Authentication method and PFS to establish the IKE SA.

MONITOR > Log

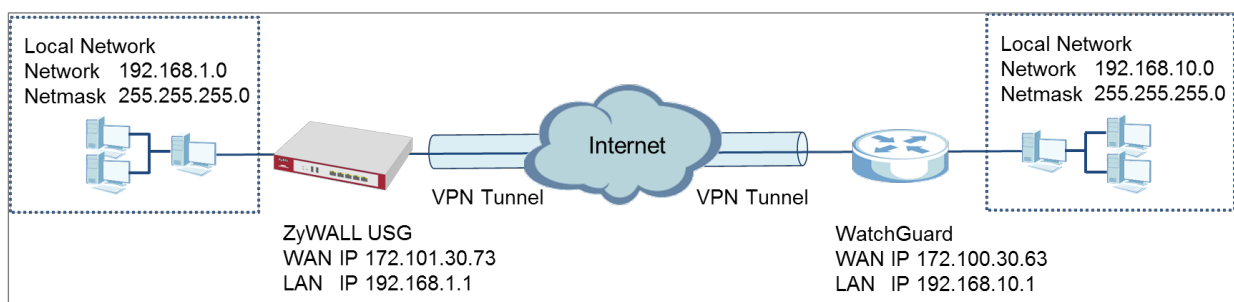
| | | | |
|------|-----|---|---------|
| info | IKE | [SA] : No proposal chosen | IKE_LOG |
| info | IKE | [SA] : Tunnel [WIZ_VPN_FortiGate] Phase 2 proposal mismatch | IKE_LOG |
| info | IKE | Recv:[HASH][SA][NONCE][ID][ID] | IKE_LOG |
| info | IKE | Phase 1 IKE SA process done | IKE_LOG |

Make sure the both ZyWALL/USG and FortiGate security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.


Default NAT traversal is enable on ZyWALL/USG, please make sure the remote IPSec device must also have NAT traversal enabled.

How to Configure Site-to-site IPSec VPN with WatchGuard

This example shows how to use the VPN Setup Wizard to create a site-to-site VPN between a ZYWALL/USG and a WatchGuard router. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



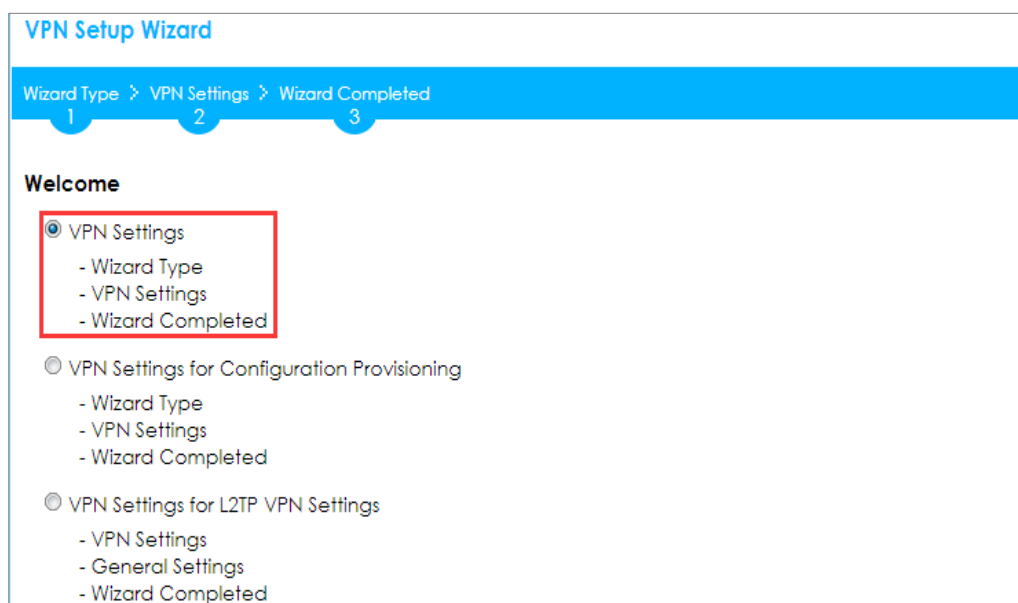
ZyWALL Site-to-site IPSec VPN with WatchGuard Connected

 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25) and WatchGuard XTM 515 (Firmware Version: 11.10.4).

Set Up the IPSec VPN Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the WatchGuard. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

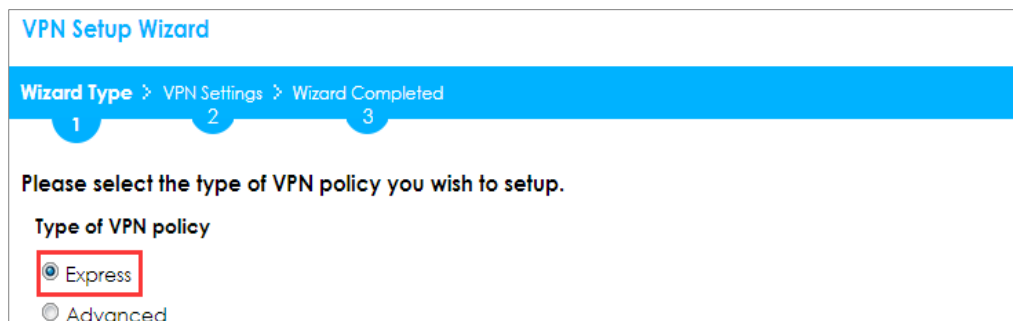
1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Please select the type of VPN policy you wish to setup.

Type of VPN policy

- ☒ Express
- ☐ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway).

You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name:

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

Configure **Secure Gateway** IP as the WatchGuard's WAN IP address (in the example, 172.100.30.63). Then, type a secure **Pre-Shared Key** (8-32 characters).

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the WatchGuard. Click **OK**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

Configuration

Secure Gateway: (IP or FQDN)

Pre-Shared Key:

Local Policy (IP/Mask):

Remote Policy (IP/Mask):

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Summary

Rule Name: VPN_to_WatchGuard

Secure Gateway: 172.100.30.63

Pre-Shared Key: ZyXEL123

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings > Wizard completed

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Congratulations. The VPN Access wizard is completed

Summary

Rule Name: VPN_to_WatchGuard

Secure Gateway: 172.100.30.63

Pre-Shared Key: ZyXEL123

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway**, click **Show Advanced Settings**. Configure **Authentication > Local ID Type** as **IPv4** and set the **Content** as

your ZyWALL/USG's **WAN IP Address** (in the example, 172.101.30.73). Then, configure **Authentication > Remote ID Type** as **IPv4** and set the **Content** as your WatchGuard's **External IP Address** (in the example, 172.100.30.63). Click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type

Authentication

☒ Pre-Shared Key
☐ unmasked

☐ Certificate (See [My Certificates](#))

☐ User Based PSK ⓘ

Advance

Local ID Type:
 Content:
 Peer ID Type:
 Content:

Set Up the IPSec VPN Tunnel on the WatchGuard

Go to **Dashboard > Network Interfaces** to check your **External IP Address** (the Internet-facing interface) and **Trusted IP Address** (the Local IP address).

Dashboard > Network Interfaces

| Link Status | Alias | IPv4 Address | Gateway |
|-------------|------------|------------------|--------------|
| Up | External | 172.100.30.63/24 | 172.100.30.1 |
| Up | Trusted | 192.168.10.1/24 | 0.0.0.0 |
| Down | Optional-1 | 0.0.0.0/0 | 0.0.0.0 |
| Down | Optional-2 | 0.0.0.0/0 | 0.0.0.0 |
| Down | Optional-3 | 0.0.0.0/0 | 0.0.0.0 |
| Down | Optional-4 | 0.0.0.0/0 | 0.0.0.0 |
| Down | Optional-5 | 0.0.0.0/0 | 0.0.0.0 |

In the WatchGuard **VPN > Branch Office VPN > Gateway > General Settings** create a Site-to-site VPN **Gateway Name** and set a secure **Pre-Shared Key**.

VPN > Branch Office VPN > Gateway > General Settings > Credential Method

Gateway Name: **VPN_to_ZyWALL**

General Settings | Phase 1 Settings

Credential Method

☒ Use Pre-Shared Key: *********

☐ Use IPSec Firebox Certificate

| ID | Certificate Name | Algorithm |
|----|------------------|-----------|
| | | |
| | | |
| | | |
| | | |

To add a **Gateway Endpoint**, click **Add**.

VPN > Branch Office VPN > Gateway > General Settings > Gateway Endpoints

Gateway Endpoints

| Local Type | Local ID | Local Interface | Remote IP | Remote Type | Remote ID |
|------------|----------|-----------------|-----------|-------------|-----------|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Add | Edit | Remove

The new **Gateway Endpoint** dialog box appears. Configure your **Local Gateway** identity as WatchGuard's **External IP Address** (in the example, 172.100.30.63) and **Remote Gateway** identity as your ZyWALL/USG's **WAN IP Address** (in the example, 172.101.30.73). Click **OK**.

VPN > Branch Office VPN > Gateway > General Settings > Gateway Endpoints

Gateway Endpoint Settings

A tunnel needs authentication on each side of the tunnel. Provide the configuration details for the gateway endpoints below.

Local Gateway

Specify the gateway ID for tunnel authentication.

☒ By IP Address 172.100.30.63
 ☐ By Domain Name
 ☐ By User ID on Domain
 ☐ By x500 Name

External Interface External

Remote Gateway

Specify the remote gateway IP address for a tunnel.

☒ Static IP Address 172.101.30.73
 ☐ Dynamic IP Addresss

Specify the gateway ID for tunnel authentication.

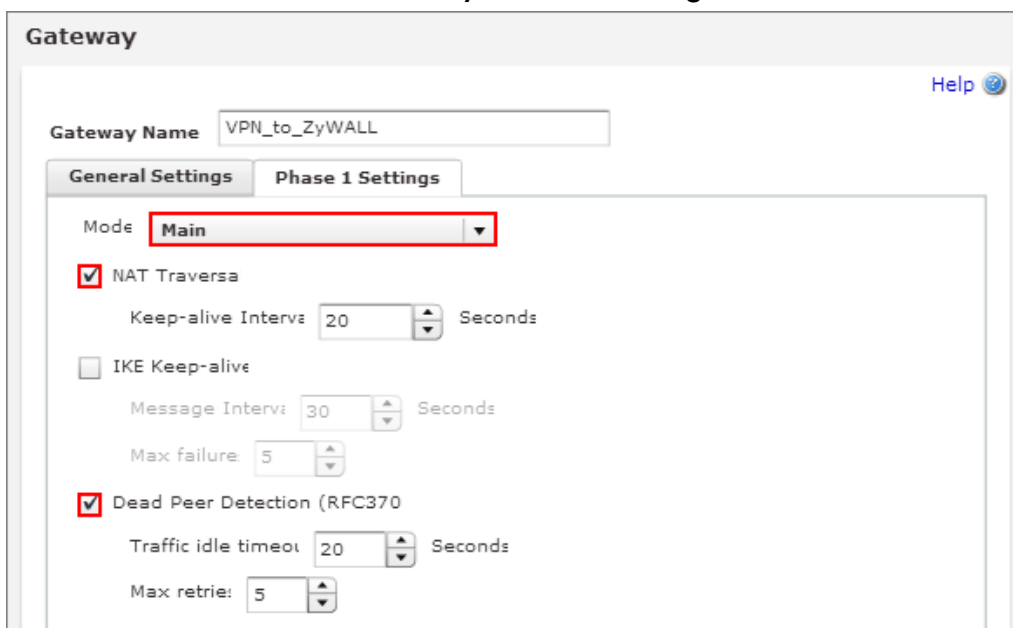
☒ By IP Address 172.101.30.73
 ☐ By Domain Name
 ☐ By User ID on Domain
 ☐ By x500 Name

☐ Attempt to resolve domain

OK Cancel

Then, go to **VPN > Branch Office VPN > Gateway > Phase 1 Settings** to select negotiation **Mode** the same as your ZyWALL/USG's Phase 1 Settings. Make sure you enable both **NAT Traversal** and **Dead Peer Detection** options if both options are enabled in the ZyWALL/USG.

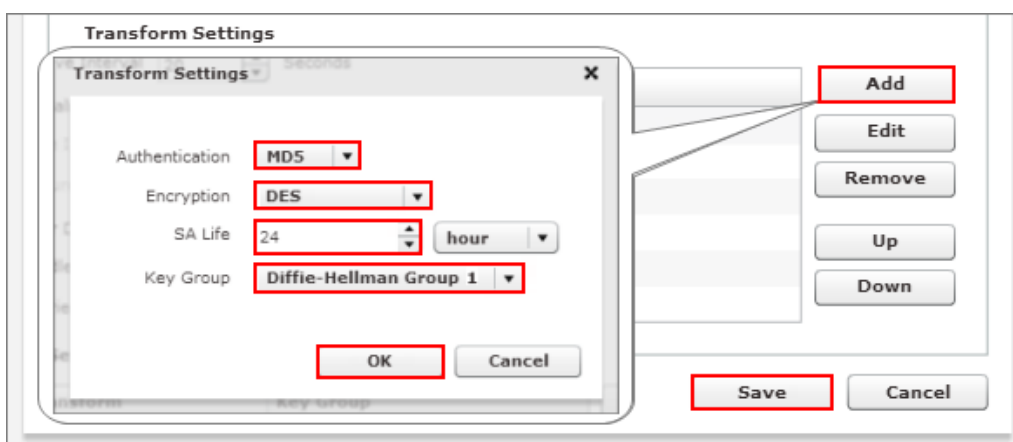
VPN > Branch Office VPN > Gateway > Phase 1 Settings



The screenshot shows the 'Gateway' configuration window with the 'Phase 1 Settings' tab selected. The 'Gateway Name' is 'VPN_to_ZyWALL'. The 'Mode' is set to 'Main'. The 'NAT Traversal' checkbox is checked, with 'Keep-alive Interval' set to 20 seconds. The 'IKE Keep-alive' checkbox is unchecked, with 'Message Interval' set to 30 seconds and 'Max failure' set to 5. The 'Dead Peer Detection (RFC370)' checkbox is checked, with 'Traffic idle timeout' set to 20 seconds and 'Max retries' set to 5.

Use **Transform Settings** to create the same security settings as in the ZyWALL/USG Phase 1 settings. Click **OK** and **Save** to exit the **Transform Settings** page.

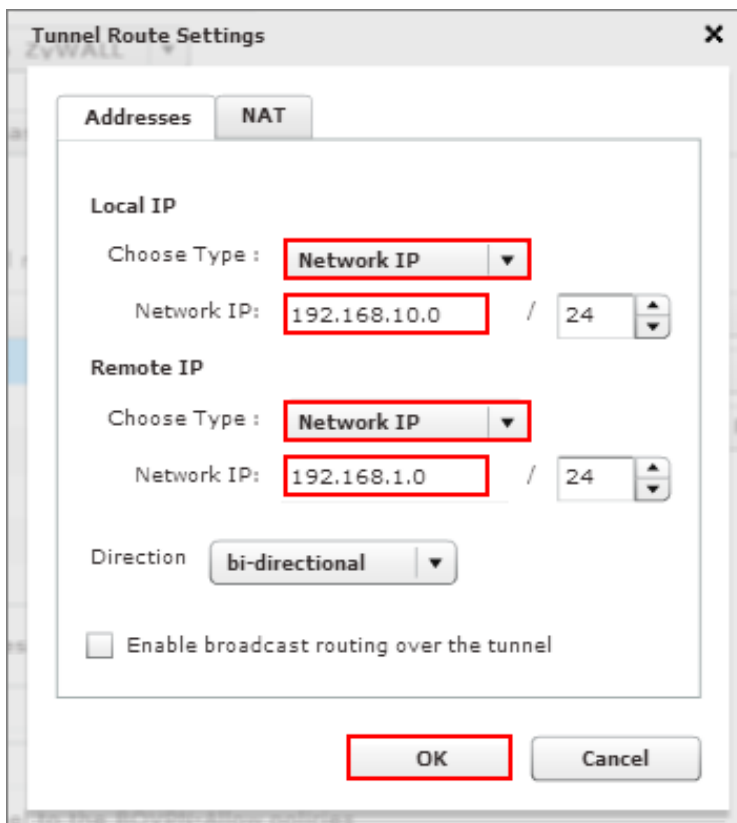
VPN > Branch Office VPN > Gateway > Phase 1 Settings > Transform Settings



The screenshot shows the 'Transform Settings' dialog box. The 'Authentication' is set to 'MD5', 'Encryption' is set to 'DES', 'SA Life' is set to 24 hours, and 'Key Group' is set to 'Diffie-Hellman Group 1'. The 'Add' button is highlighted with a red box. The 'OK' and 'Save' buttons are also highlighted with red boxes.

Then, go to **VPN > Branch Office VPN > Tunnel** to add a Tunnel Route Settings. In the **Local IP** section, set **the Network IP** to be the IP address range of the network connected to the WatchGuard. In the **Remote IP** section, set **the Network IP** to be the IP address range of the network connected to the ZyWALL/USG. Click **OK**.

VPN > Branch Office VPN > Tunnel > Address



Tunnel Route Settings

Addresses NAT

Local IP

Choose Type : **Network IP**

Network IP: **192.168.10.0** / 24

Remote IP

Choose Type : **Network IP**

Network IP: **192.168.1.0** / 24

Direction: **bi-directional**

☐ Enable broadcast routing over the tunnel

OK Cancel

Go to **VPN > Branch Office VPN > Tunnel > Phase 2 Settings** to create a **Tunnel Name**. Then, select the **Gateway**. Make sure you enable **Perfect Forward Secrecy** and select **Diffie-Hellman Group 2**. Then, scroll down **Phase 2 Proposals** and add the encryption types to match your ZyWALL/USG's **VPN Connection > Phase 2 Settings**. Click **Save**.

VPN > Branch Office VPN > Tunnel > Phase 2 Settings

Test the IPsec VPN Tunnel

Go to ZyWALL/USG **CONFIGURATION** > **VPN** > **IPSec VPN** > **VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPsec VPN > VPN Connection

| # | Status | Name | VPN Gateway | Policy |
|---|--------|-------------------|-------------------|--|
| 1 | | VPN_to_WatchGuard | VPN_to_WatchGuard | VPN_to_WatchGuard_LOCAL/VPN_to_WatchGuard_REMOTE |

Go to ZyWALL/USG **MONITOR** > **VPN Monitor** > **IPSec** and verify the tunnel **Up Time** and **Inbound(Bytes)/Outbound(Bytes)** traffic.

MONITOR > VPN Monitor > IPsec

| # | Serial Num... | System Na... | Name | Policy | My Address | Secure Gateway | Up Time | Timeout | Inbound(B... | Outbound(... |
|---|---------------|--------------|-------------------|-------------------|---------------|------------------|---------|---------|--------------|--------------|
| 1 | N/A | N/A | VPN_to_WatchGuard | 192.168.1.0/24... | 172.101.30.73 | P: 172.100.30.63 | 97 | 76223 | 0[0 bytes] | 0[0 bytes] |

Go to WatchGuard **System Status** > **VPN Statistics** > **Branch Office VPN** and check the tunnel **Status** is up and **Bytes In** (Incoming Data) and **Bytes Out** (Outgoing Data).

System Status > VPN Statistics > Branch Office

| Name | Local | Remote | Gateway | Packets In | Bytes In | Packets Out | Bytes Out | Rekeys |
|---------------|-----------------|----------------|-------------------------------|------------|----------|-------------|-----------|--------|
| VPN_to_ZyWALL | 192.168.10.0/24 | 192.168.1.0/24 | 172.100.30.63 - 172.101.30.73 | 265 | 15900 | 384 | 23635 | 0 |

To test whether or not a tunnel is working, ping from a computer at one site to a computer at the other. Ensure that both computers have Internet access (via the IPsec devices).

PC behind ZyWALL/USG > Window 7 > cmd > ping 192.168.10.33

```
C:\Documents and Settings\ZyXEL>ping 192.168.10.33

Pinging 192.168.10.33 with 32 bytes of data:

Reply from 192.168.10.33: bytes=32 time=18ms TTL=54
Reply from 192.168.10.33: bytes=32 time=17ms TTL=54
Reply from 192.168.10.33: bytes=32 time=17ms TTL=54
Reply from 192.168.10.33: bytes=32 time=16ms TTL=54

Ping statistics for 192.168.10.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 18ms, Average = 17ms
```

PC behind WatchGuard> Window 7 > cmd > ping 192.168.1.33

```
C:\Documents and Settings\ZyXEL>ping 192.168.1.33

Pinging 192.168.1.33 with 32 bytes of data:

Reply from 192.168.1.33: bytes=32 time=27ms TTL=43
Reply from 192.168.1.33: bytes=32 time=32ms TTL=43
Reply from 192.168.1.33: bytes=32 time=26ms TTL=43
Reply from 192.168.1.33: bytes=32 time=27ms TTL=43

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 32ms, Average = 28ms
```

What Could Go Wrong?

If you see below [info] or [error] log message, please check ZyWALL/USG Phase 1 Settings. Both ZyWALL/USG and WatchGuard must use the same Pre-Shared Key, Encryption, Authentication method, DH key group and ID Type to establish the IKE SA.

MONITOR > Log

| Priority | Category | Message | Source | Destination | Note |
|----------|----------|---|-------------------|-------------------|---------|
| info | IKE | Send:[NOTIFY:NO_PROPOSAL_CHOSEN] | 172.101.30.73:500 | 172.100.30.63:500 | IKE_LOG |
| info | IKE | [SA] : No proposal chosen | 172.101.30.73:500 | 172.100.30.63:500 | IKE_LOG |
| info | IKE | [SA] : Tunnel [VPN_to_WatchGuard] Phase 1 proposal mismatch | 172.101.30.73:500 | 172.100.30.63:500 | IKE_LOG |

If you see that Phase 1 IKE SA process done but still get below [info] log message,

please check ZyWALL/USG and WatchGuard Phase 2 Settings. Both ZyWALL/USG and WatchGuard must use the same Protocol, Encapsulation, Encryption, Authentication method and PFS to establish the IKE SA.

MONITOR > Log

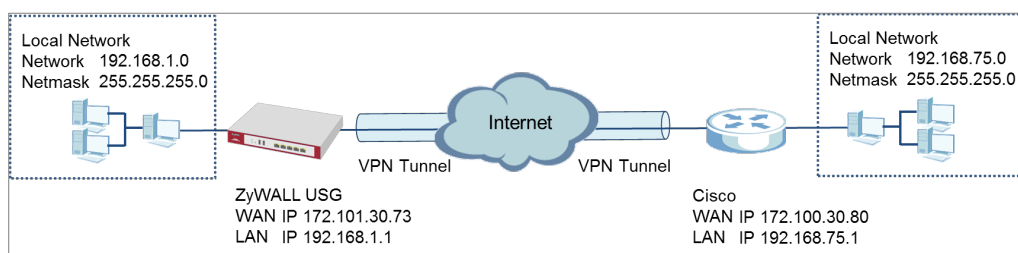
| | | | | | |
|------|-----|---|-------------------|-------------------|---------|
| info | IKE | [SA] : No proposal chosen | 172.101.30.73:500 | 172.100.30.63:500 | IKE_LOG |
| info | IKE | [SA] : Tunnel [VPN_to_WatchGuard] Phase 2 proposal mismatch | 172.101.30.73:500 | 172.100.30.63:500 | IKE_LOG |
| info | IKE | Recv:[HASH][SA][NONCE][ID][ID] | 172.100.30.63:500 | 172.101.30.73:500 | IKE_LOG |
| info | IKE | Phase 1 IKE SA process done | 172.101.30.73:500 | 172.100.30.63:500 | IKE_LOG |

Make sure the both ZyWALL/USG and WatchGuard security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.


Default NAT traversal is enable on ZyWALL/USG, please make sure the remote IPSec device must also have NAT traversal enabled.

How to Configure Site-to-site IPSec VPN with Cisco

This example shows how to use the VPN Setup Wizard to create a site-to-site VPN between a ZYWALL/USG and a Cisco router. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



ZyWALL Site-to-site IPSec VPN with Cisco Connected

 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25) and ISA500 (Firmware Version: 1.0.3).

Set Up the IPSec VPN Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the Cisco. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

Choose **Advanced** to create a VPN rule with the customize phase 1, phase 2 settings and authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Please select the type of VPN policy you wish to setup.

Type of VPN policy

- ☐ Express
- ☒ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway).

You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Advanced Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name:

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

Then, configure the **Secure Gateway** IP as the Cisco's Gateway IP address (in the example, 172.100.30.80); select **My Address** to be the interface connected to the Internet.

Set the desired **Negotiation**, **Encryption**, **Authentication**, **Key Group** and **SA Life Time** settings. Type a secure **Pre-Shared Key** (8-32 characters) which must match your Cisco **Pre-Shared Key**. Click **OK**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Phase 1 Setting)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Advanced Settings

Phase 1 Setting

Secure Gateway: (IP or FQDN)

My Address (Interface):

Negotiation Mode:

Encryption Algorithm:

Authentication Algorithm:

Key Group:

SA Life Time: (180 - 3000000 seconds)

☒ NAT Traversal

☒ Dead Peer Detection (DPD)

Authentication Method

☒ Pre-Shared Key

☐ Certificate

Continue to **Phase 2 Settings** to select the desired **Encapsulation**, **Encryption**, **Authentication**, and **Perfect Forward Secrecy (PFS)** settings.

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the Cisco. Click **OK**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Phase 2 Setting)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Advanced Settings

Phase 2 Setting

Active Protocol: ESP

Encapsulation: Tunnel

Encryption Algorithm: 3DES

Authentication Algorithm: MD5

SA Life Time: 86400 (180 - 3000000 seconds)

Perfect Forward Secrecy (PFS): DH2

Policy Setting

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.75.0 / 255.255.255.0

Property

☒ Nailed-Up

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Advanced Settings

Summary

Rule Name: VPN_to_Cisco

Secure Gateway: 172.100.30.80

Pre-Shared Key: ZyXEL123

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.75.0 / 255.255.255.0

Phase 1

Negotiation Mode: main

Encryption Algorithm: des

Authentication Algorithm: md5

Key Group: DH2

Phase 2

Active Protocol: esp

Encapsulation: tunnel

Encryption Algorithm: 3des

Authentication Algorithm: md5

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Advanced Settings

Congratulations. The VPN Access wizard is completed

Summary

| | |
|-------------------------|---------------|
| Rule Name: | VPN_to_Cisco |
| Secure Gateway: | 172.100.30.80 |
| My Address (Interface): | ge1 |
| Pre-Shared Key: | ZyXEL123 |

Phase 1

| | |
|----------------------------|-------|
| Negotiation Mode: | main |
| Encryption Algorithm: | des |
| Authentication Algorithm: | md5 |
| Key Group: | DH2 |
| SA Life Time: | 86400 |
| NAT Traversal: | true |
| Dead Peer Detection (DPD): | true |

Phase 2

| | |
|--------------------------------|--------|
| Active Protocol: | esp |
| Encapsulation: | tunnel |
| Encryption Algorithm: | 3des |
| Authentication Algorithm: | md5 |
| SA Life Time: | 86400 |
| Perfect Forward Secrecy (PFS): | DH2 |

Policy

| | |
|--------------------------|------------------------------|
| Local Policy (IP/Mask): | 192.168.1.0 / 255.255.255.0 |
| Remote Policy (IP/Mask): | 192.168.75.0 / 255.255.255.0 |
| Naïve-Up: | true |

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** and click **Show Advanced Settings**. Configure **Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPSec router.

Authentication

☒ Pre-Shared Key ☐ unmasked

☐ Certificate (See [My Certificates](#))

☐ User Based PSK ⓘ

☒ Advance

Local ID Type:

Content:

Peer ID Type:

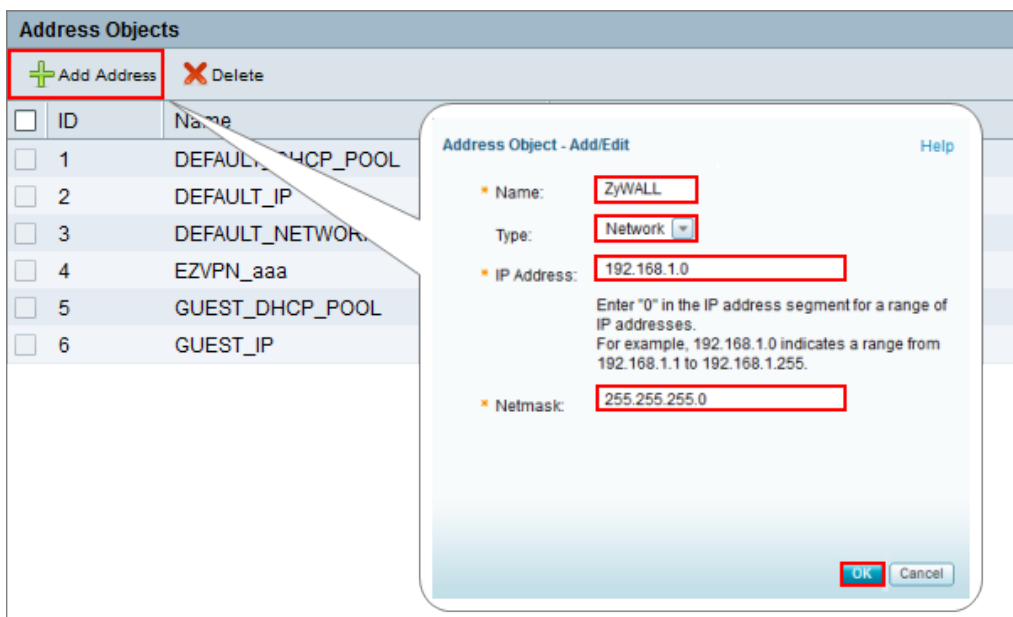
Content:

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type

Set Up the IPSec VPN Tunnel on the Cisco

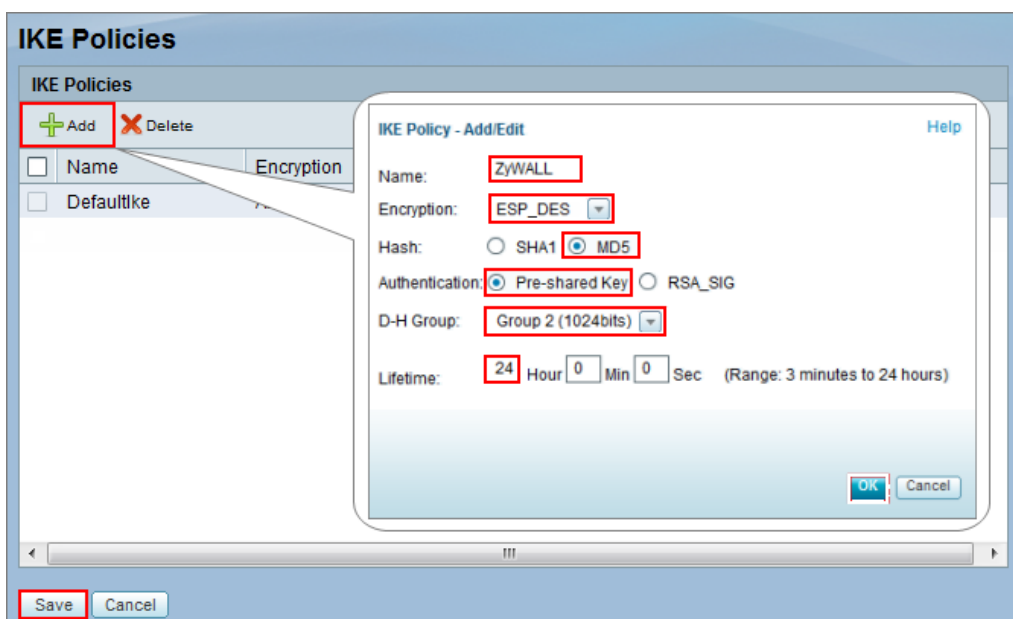
To create an **Address Object Name** of your peer ZyWALL/USG Local IP address, go to **Networking > Address Management > Address Objects** and click **Add Address**. Select **Network** as the **Type**. Configure **IP Address** and **Netmask** to be the IP address range of the network connected to the ZyWALL/USG. Click **OK**.

Networking > Address Management > Address Objects



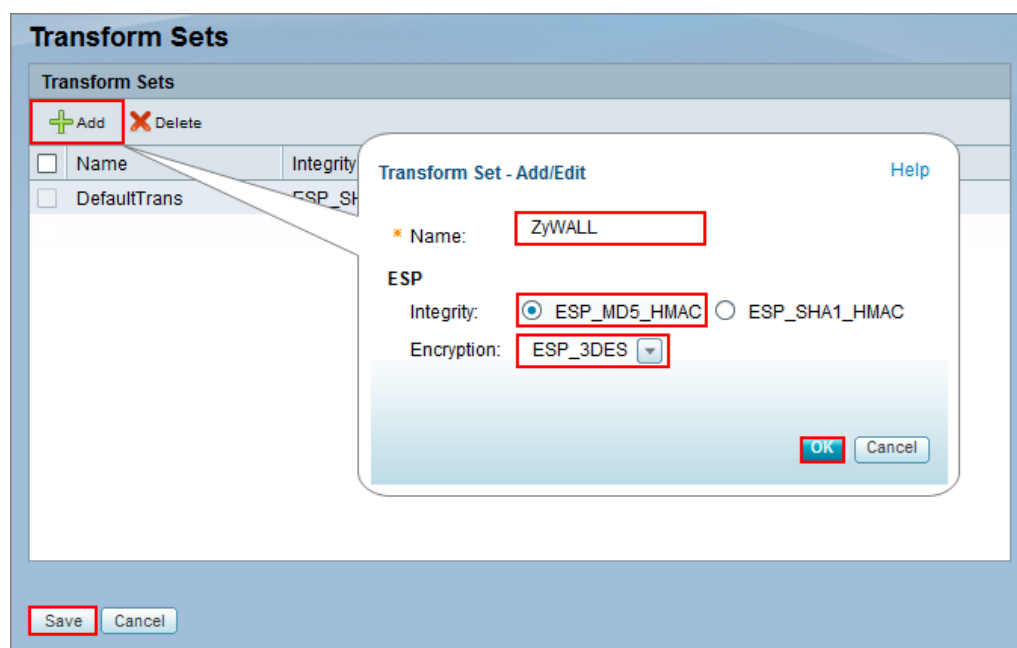
Go to **VPN > Site-to-site > IKE Policies**, click **Add** to create a new IKE Policy **Name**. Then, select **Encryption**, **Hash**, **Pre-shared Key** and **D-H Group** to match your ZyWALL/USG's **VPN Gateway > Phase 1 Settings**. Set **Lifetime** to **24** hours and click **OK** then click **Save** to exit the **IKE Policies** page.

VPN > Site-to-site > IKE Policies



Go to **VPN > Site-to-site > Transform Sets**, click **Add** to create a new **Transform Set** name. Then, select **Integrity** and **Encryption** to match your ZyWALL/USG's **VPN Connection > Phase 2 Settings**. Click **OK** and click **Save** to exit the **Transform Sets** page.

VPN > Site-to-site > Transform Sets



Go to **VPN > Site-to-site > IPsec Policies** and click **Add**. The new **IPsec Policies** dialog box appears. Go to **Basic Settings**, create IPsec policy **Description** name and click **On** the **IPsec Policy Enable** option.

Select **Static IP** as the **Remote Type**. Set **Remote Address** to be your ZyWALL/USG's WAN IP Address (in the example, 172.101.30.73). Enter the same **Pre-Shared Key** as you created in ZyWALL/USG. Then, set **WAN Interface** to the Internet-facing interface (found under **Status > WAN Interface**).

Select **Local network** to be the IP address range of the network connected to the Cisco (found under **Status > LAN Interface**) and **Remote network** to be the IP

address range of the network connected to the ZyWALL/USG (**Address Object** created in Step 1)

VPN > Site-to-site > IPsec Policies > Basic Settings

IPsec Policies - Add/Edit Help

Basic Settings | Advanced Settings | VPN Failover

* Description:

* IPsec Policy Enable: ☒ On ☐ Off

* Remote Type:

Remote Address:

* Authentication Method: ☒ Pre-Shared Key

* Key:

☐ Certificate

Local Certificate:

Remote Certificate:

WAN Interface:

* Local network:

* Remote network:

Then, go to **Advanced Settings** enable **PFS** and **DPD** if you enable both options in the ZyWALL/USG. Set **IKE Policy** to be the **IKE Policy** created in Step 2 (found under **IKE Policy Link**); set **Transform** to be the **Transform Set** created in Step 3 (found under **Transform Link**) and **SA-Lifetime** to be **24** hours.

Click **OK**. The connection active dialog box appears. Click **Activate Connection**.


VPN > Site-to-site > IPsec Policies > Advanced Settings

IPsec Policies - Add/Edit
[Help](#)

Basic Settings
Advanced Settings
VPN Failover

PFS Enable: ☒ On ☐ Off
DPD Enable: ☒ On ☐ Off
Delay Time: (Range: 10-300 s)
Detection Timeout: (Range: 30-1800 s)
DPD Action:

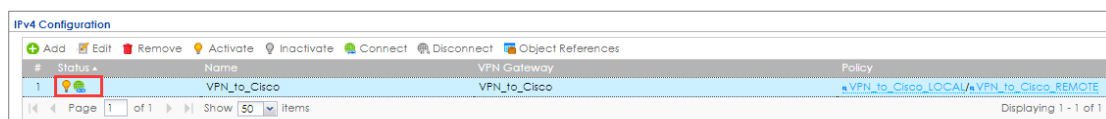
Apply NAT Policies: ☐ On ☒ Off
Translates Local Network:
Translates Remote Network:
IKE Policy: [IKE Policy Link](#)
Transform: [Transform Link](#)
SA-Lifetime: Hour Min Sec (Range: 3 minutes to 24 hours)


Do you want to make this connection active when the settings are saved?

Test the IPsec VPN Tunnel

Go to ZyWALL/USG **CONFIGURATION > VPN > IPsec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

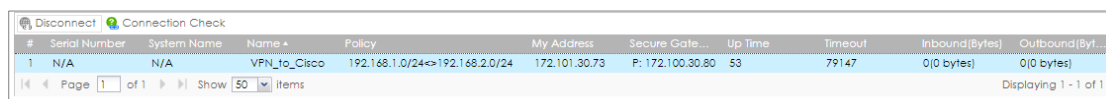
CONFIGURATION > VPN > IPsec VPN > VPN Connection



| # | Status | Name | VPN Gateway | Policy |
|---|--------|--------------|--------------|--|
| 1 | | VPN_to_Cisco | VPN_to_Cisco | VPN_to_Cisco_LOCAL/VPN_to_Cisco_REMOTE |

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPsec** and verify the tunnel **Up Time** and **Inbound(Bytes)/Outbound(Bytes)** traffic.

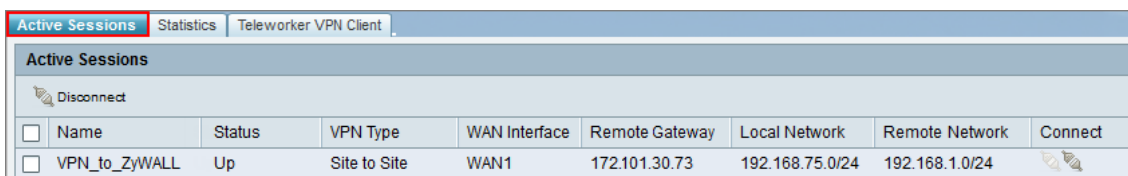
MONITOR > VPN Monitor > IPsec



| # | Serial Number | System Name | Name | Policy | My Address | Secure Gate... | Up Time | Timeout | Inbound(Bytes) | Outbound(Byte... |
|---|---------------|-------------|--------------|---------------------------------|---------------|------------------|---------|---------|----------------|------------------|
| 1 | N/A | N/A | VPN_to_Cisco | 192.168.1.0/24<->192.168.2.0/24 | 172.101.30.73 | P: 172.100.30.80 | 53 | 79147 | 0(0 bytes) | 0(0 bytes) |

Go to Cisco **VPN > VPN Status > IPsec VPN Status > Active Sessions** and check the tunnel **Status** is up.

VPN > VPN Status > IPsec VPN Status > Active Sessions



| Name | Status | VPN Type | WAN Interface | Remote Gateway | Local Network | Remote Network | Connect |
|---------------|--------|--------------|---------------|----------------|-----------------|----------------|---------|
| VPN_to_ZyWALL | Up | Site to Site | WAN1 | 172.101.30.73 | 192.168.75.0/24 | 192.168.1.0/24 | |

Go to Cisco **VPN > VPN Status > IPsec VPN Status > Statics** and check the **Tx Packets** (Transmit data) and **Rx Packets** (Receive data).

VPN > VPN Status > IPsec VPN Status > Statics

Active Sessions

Statistics

Teleworker VPN Client

IPsec VPN Statistic

| Name | VPN Type | WAN Interface | Remote Gateway | Tx Bytes | Rx Bytes | Tx Packets | Rx Packets |
|---------------|--------------|---------------|----------------|----------|----------|------------|------------|
| VPN_to_ZyWALL | Site to Site | WAN1 | 172.101.30.73 | 60665 | 45180 | 758 | 753 |

To test whether a tunnel is working, ping from a computer at one site to a computer at the other. Ensure that both computers have Internet access (via the IPsec devices).

PC behind ZyWALL/USG > Window 7 > cmd > ping 192.168.75.33

```
C:\Documents and Settings\ZyXEL>ping 192.168.75.33

Pinging 192.168.75.33 with 32 bytes of data:

Reply from 192.168.75.33: bytes=32 time=18ms TTL=54
Reply from 192.168.75.33: bytes=32 time=17ms TTL=54
Reply from 192.168.75.33: bytes=32 time=17ms TTL=54
Reply from 192.168.75.33: bytes=32 time=16ms TTL=54

Ping statistics for 192.168.75.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 18ms, Average = 17ms
```

PC behind Cisco> Window 7 > cmd > ping 192.168.1.33

```
C:\Documents and Settings\ZyXEL>ping 192.168.1.33

Pinging 192.168.1.33 with 32 bytes of data:

Reply from 192.168.1.33: bytes=32 time=27ms TTL=43
Reply from 192.168.1.33: bytes=32 time=32ms TTL=43
Reply from 192.168.1.33: bytes=32 time=26ms TTL=43
Reply from 192.168.1.33: bytes=32 time=27ms TTL=43

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 26ms, Maximum = 32ms, Average = 28ms
```

What Could Go Wrong?

If you see below [info] or [error] log message, please check ZyWALL/USG Phase 1 Settings. Both ZyWALL/USG and Cisco must use the same Pre-Shared Key, Encryption, Authentication method, DH key group and ID Type to establish the IKE SA.

MONITOR > Log

| Priority | Category | Message | Source | Destination | Note |
|----------|----------|--|-------------------|-------------------|---------|
| info | IKE | Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN] | 172.101.30.73:500 | 172.100.30.80:500 | IKE_LOG |
| info | IKE | [SA] : No proposal chosen | 172.101.30.73:500 | 172.100.30.80:500 | IKE_LOG |
| info | IKE | [SA] : Tunnel [VPN_to_Cisco] Phase 1 proposal mismatch | 172.101.30.73:500 | 172.100.30.80:500 | IKE_LOG |

If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG and Cisco Phase 2 Settings. Both ZyWALL/USG and Cisco must use the same Protocol, Encapsulation, Encryption, Authentication method and PFS to establish the IKE SA.

MONITOR > Log

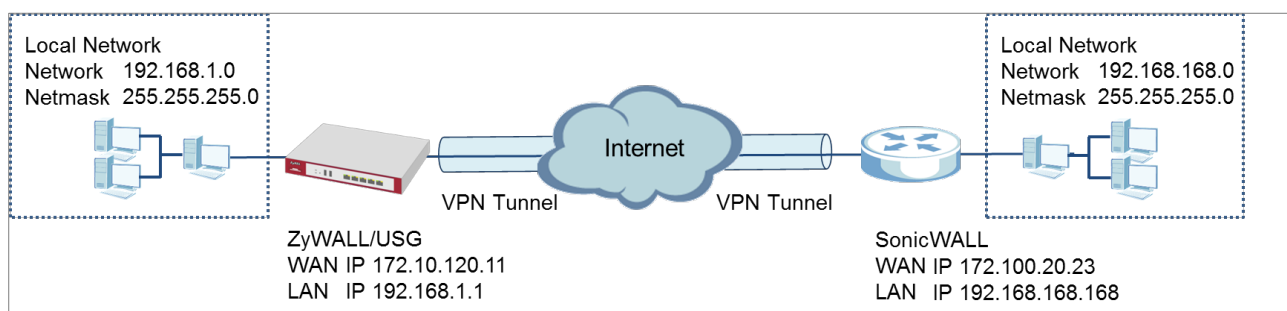
| | | | | | |
|------|-----|--|-------------------|-------------------|---------|
| info | IKE | Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN] | 172.101.30.73:500 | 172.100.30.80:500 | IKE_LOG |
| info | IKE | [SA] : No proposal chosen | 172.101.30.73:500 | 172.100.30.80:500 | IKE_LOG |
| info | IKE | [SA] : Tunnel [VPN_to_Cisco] Phase 2 proposal mismatch | 172.101.30.73:500 | 172.100.30.80:500 | IKE_LOG |
| info | IKE | Recv:[HASH][SA][NONCE][ID][ID] | 172.100.30.80:500 | 172.101.30.73:500 | IKE_LOG |
| info | IKE | Phase 1 IKE SA process done | 172.101.30.73:500 | 172.100.30.80:500 | IKE_LOG |

Make sure the both ZyWALL/USG and Cisco security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.


Default NAT traversal is enable on ZyWALL/USG, please make sure the remote IPSec device must also have NAT traversal enabled.

How to Configure Site-to-site IPsec VPN with a SonicWALL router

This example shows how to use the VPN Setup Wizard to create a site-to-site VPN between a ZYWALL/USG and a SonicWALL router. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



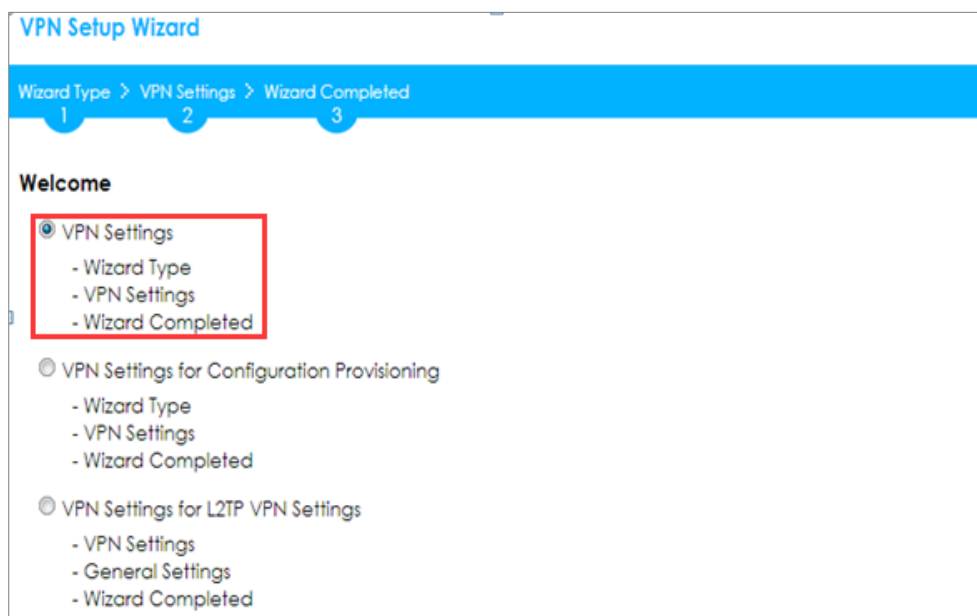
ZyWALL/USG Site-to-site IPsec VPN with SonicWALL

 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25) and NSA240 (Firmware Version: SonicOS Enhanced 5.8.0.1-31o)

Set Up the IPSec VPN Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the SonicWALL. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

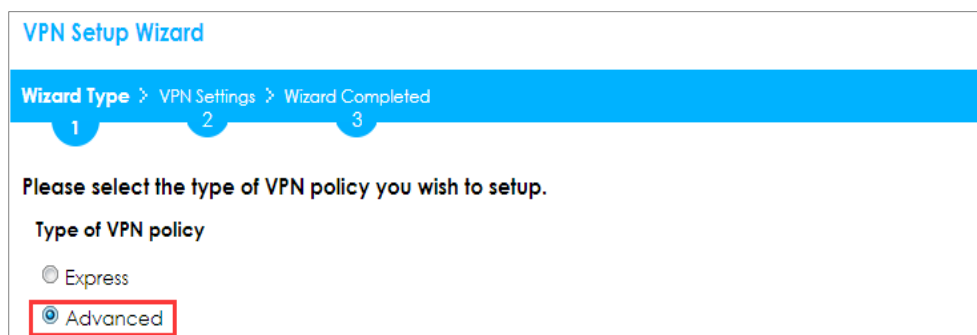
1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

Choose **Advanced** to create a VPN rule with the customize phase 1, phase 2 settings and authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

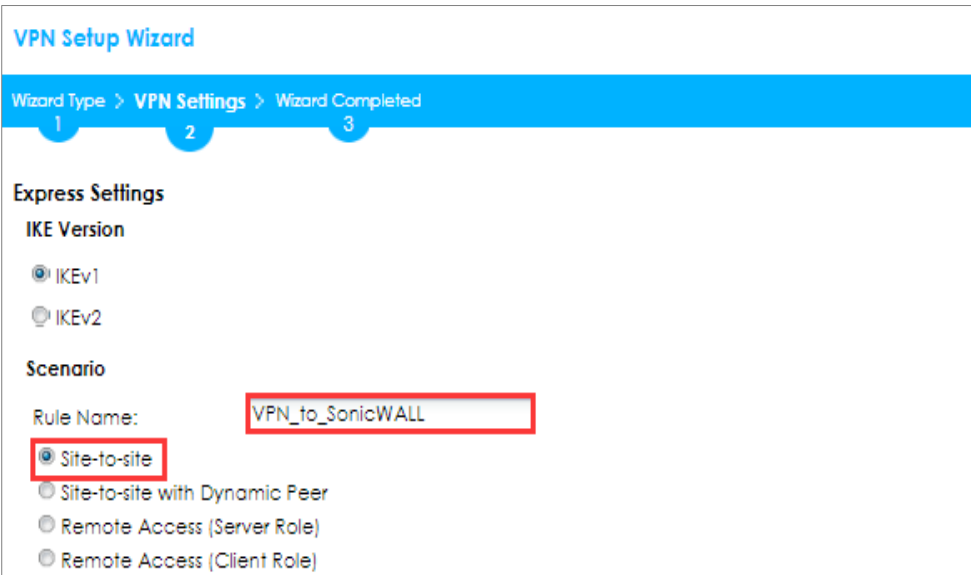
Please select the type of VPN policy you wish to setup.

Type of VPN policy

- ☐ Express
- ☒ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway).
You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name:

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

Then, configure the **Secure Gateway** IP as the SonicWALL's Gateway IP address (in the example, 172.100.20.23); select **My Address** to be the interface connected to the Internet.

Set the desired **Negotiation**, **Encryption**, **Authentication**, **Key Group** and **SA Life Time** settings. Type a secure **Pre-Shared Key** (8-32 characters) which must match your SonicWALL **Shared Secret**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Phase 1 Setting)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Advanced Settings

Phase 1 Setting

Secure Gateway: 172.100.20.23 (IP or FQDN)

My Address (interface): ge1

Negotiation Mode: Main

Encryption Algorithm: AES256

Authentication Algorithm: SHA1

Key Group: DH2

SA Life Time: 86400 (180 - 3000000 seconds)

☒ NAT Traversal

☒ Dead Peer Detection (DPD)

Authentication Method

☒ Pre-Shared Key 5k4u;4e.40fm06xk718

☐ Certificate default

Continue to **Phase 2 Settings** to select the desired **Encapsulation**, **Encryption**, **Authentication**, and **SA Life Time** settings.

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the SonicWALL. Click **OK**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Phase 2 Setting)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Advanced Settings

Phase 2 Setting

Active Protocol: ESP

Encapsulation: Tunnel

Encryption Algorithm: AES128

Authentication Algorithm: SHA1

SA Life Time: 86400 (180 - 3000000 seconds)

Perfect Forward Secrecy (PFS): None

Policy Setting

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.168.0 / 255.255.255.0

Property

☒ Nailed-Up

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1

2

3

Advanced Settings

Summary

Rule Name: VPN_to_SonicWall
 Secure Gateway: 172.100.20.23
 Pre-Shared Key: 5k4u;4e.40fm06xk7187!
 Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0
 Remote Policy (IP/Mask): 192.168.168.0 / 255.255.255.0

Phase 1

Negotiation Mode: main
 Encryption Algorithm: aes256
 Authentication Algorithm: sha
 Key Group: DH2

Phase 2

Active Protocol: esp
 Encapsulation: tunnel
 Encryption Algorithm: aes128
 Authentication Algorithm: sha



Note: The Phase 1 and Phase 2 settings established here must match the Phase 1 and Phase 2 settings configured later in the SonicWALL.

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Advanced Settings

Congratulations. The VPN Access wizard is completed

Summary

| | |
|-------------------------|-----------------------|
| Rule Name: | VPN_to_SonicWall |
| Secure Gateway: | 172.100.20.23 |
| My Address (interface): | ge1 |
| Pre-Shared Key: | 5k4u;4e.40fm06xk7187! |

Phase 1

| | |
|----------------------------|--------|
| Negotiation Mode: | main |
| Encryption Algorithm: | aes256 |
| Authentication Algorithm: | sha |
| Key Group: | DH2 |
| SA Life Time: | 86400 |
| NAT Traversal: | true |
| Dead Peer Detection (DPD): | true |

Phase 2

| | |
|--------------------------------|--------|
| Active Protocol: | esp |
| Encapsulation: | tunnel |
| Encryption Algorithm: | aes128 |
| Authentication Algorithm: | sha |
| SA Life Time: | 86400 |
| Perfect Forward Secrecy (PFS): | None |

Policy

| | |
|--------------------------|-------------------------------|
| Local Policy (IP/Mask): | 192.168.1.0 / 255.255.255.0 |
| Remote Policy (IP/Mask): | 192.168.168.0 / 255.255.255.0 |
| Nailed-Up: | true |

Go to **VPN Gateway > Show Advanced Settings > Authentication** to configure **your Local ID Type** and **Peer ID Type** to match your SonicWALL's **VPN > Settings > VPN Policies > General > IKE Authentication > Local IKE ID** and **Peer IKE ID**.

VPN Gateway > Show Advanced Settings > Authentication

Authentication

☒ Pre-Shared Key

☒ unmasked

☐ Certificate

 (See [My Certificates](#))

☐ User Based PSK

Advance

Local ID Type:

Content:

Peer ID Type:

Content:

Set Up the IPSec VPN Tunnel on the SonicWALL

In the SonicWALL **VPN > Settings > VPN Policies**, click **Add** to create a new VPN policy. Select **Policy Type** to be the **Site to Site**, select **Authentication Method** to

be the **IKE using Preshared Secret**. Type the ZyWALL/USG's WAN IP Address to be the **IPsec Primary Gateway Name or Address** (in the example, 172.10.120.11).

In the **IKE Authentication** section, set the **Shared Secret** to be the same as your ZyWALL/USG's **Pre-Shared Key**. Then, set the **Local IKE ID** and the **Peer IKE ID** to match your ZyWALL/USG's **VPN Gateway > Show Advanced Settings > Authentication > Local ID Type** and **Peer ID Type**.

VPN > Settings > VPN Policies > General

SONICWALL | Network Security Appliance

General | Network | Proposals | Advanced

Security Policy

Policy Type: Site to Site

Authentication Method: IKE using Preshared Secret

Name: VPN_to_ZyWALL

IPsec Primary Gateway Name or Address: 172.10.120.11

IPsec Secondary Gateway Name or Address: 0.0.0.0

IKE Authentication

Shared Secret: 5k4u;4e.40fm06xk7187!

Confirm Shared Secret: 5k4u;4e.40fm06xk7187! ☒ Mask Shared Secret

Local IKE ID: IP Address 192.168.168.0

Peer IKE ID: IP Address 192.168.1.0

In the SonicWALL **VPN > Settings > VPN Policies > Network**, choose **Local Network** to be the IP address range of the network connected to the **SonicWALL** (found under **SonicWALL > Network > Interfaces > LAN**).

Go to **Remote Network** and create a new address IP address range of the network connected to the ZyWALL/USG. Then, scroll down the list to choose the newly created **Address Object** to be the **Remote Network**.

VPN > Settings > VPN Policies > Network

SONICWALL | Network Security Appliance

General Network Proposals Advanced

Local Networks

- ☒ Choose local network from list
- ☐ Local network obtains IP addresses using DHCP through this VPN Tunnel
- ☐ Any address

--Select Local Network--
 ==== Address Objects ====
 X0 IP
X0 Subnet
 X1 Default Gateway
 X1 IP
 ==== Address Objects ====

Remote Networks

- ☐ Use this VPN Tunnel as default route for all Internet traffic
- ☐ Destination network obtains IP addresses using DHCP through this VPN Tunnel
- ☒ Choose destination network from list

SONICWALL | Network Security Appliance

Name: ZyWALL
 Zone Assignment: LAN
 Type: Network
 Network: 192.168.1.0
 Netmask: 255.255.255.0

--Select Remote Network--
 --Select Remote Network--
Create new address object...
 Create new address group...
 ==== Address Groups ====
 allIP
 relayagent
 ==== Address Objects ====

Remote Networks

- ☐ Use this VPN Tunnel as default route for all Internet traffic
- ☐ Destination network obtains IP addresses using DHCP through this VPN Tunnel
- ☒ Choose destination network from list

ZyWALL
 --Select Remote Network--
 Create new address object...
 Create new address group...
 ==== Address Groups ====
 allIP
 relayagent
 ==== Address Objects ====
ZyWALL

In the SonicWALL **VPN > Settings > VPN Policies > Proposals > IKE (Phase 1) Proposal** and set **Exchange**, **DH Group**, **Encryption** and **Authentication** to match your ZyWALL/USG's **VPN Gateway > Show Advanced Settings > Phase 1 Settings**.

Go to **IKE (Phase 2) Proposal** and set the **Protocol**, **Encryption** and **Authentication** to match your ZyWALL/USG's **VPN Connection > Show Advanced Settings > Phase 2 Settings**.

VPN > Settings > VPN Policies > Proposals

SONICWALL | Network Security Appliance

General | Network | **Proposals** | Advanced

IKE (Phase 1) Proposal

Exchange: Main Mode ▼

DH Group: Group 2 ▼

Encryption: AES-256 ▼

Authentication: SHA1 ▼

Life Time (seconds): 28800

Ipssec (Phase 2) Proposal

Protocol: ESP ▼

Encryption: AES-128 ▼

Authentication: SHA1 ▼

☐ Enable Perfect Forward Secrecy

Life Time (seconds): 28800

Select **Enable VPN** and click **Refresh Active**.

VPN > Settings > VPN Global Settings

VPN Global Settings

☒ Enable VPN
Unique Firewall Identifier:

VPN Policies

Refresh Interval (secs) Items per page Items to 3

| # | Name | Gateway | Destinations | Refresh Active | Crypto Suite | Enable |
|---|---------------|---------------|-----------------------------|----------------|--------------------------|-------------------------------------|
| 3 | VPN_to_ZyWALL | 172.10.120.11 | 192.168.1.0 - 192.168.1.255 | | ESP: DES/HMAC SHA1 (IKE) | <input checked="" type="checkbox"/> |

Test the IPSec VPN Tunnel

Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

IPv4 Configuration

[Add](#) [Edit](#) [Remove](#) [Activate](#) [Inactivate](#) [Connect](#) [Disconnect](#) [Object References](#)

| # | Status | Name | VPN Gateway | Policy |
|---|--------|------------------|------------------|--|
| 1 | | VPN_to_SonicWALL | VPN_to_SonicWALL | VPN_to_Cisco_LOCAL / VPN_to_Cisco_REMOTE |

Page 1 of 1 | Show 50 items | Displaying 1 - 1 of 1

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic.

MONITOR > VPN Monitor > IPSec

[Disconnect](#) [Connection Check](#)

| # | Serial N... | Syste... | Name | Policy | My Address | Secure Gat... | Up Time | Timeout | Inbound[B... | Outbound[... |
|---|-------------|----------|------------------|--------------------------------|---------------|----------------|---------|---------|--------------|--------------|
| 1 | N/A | N/A | VPN_to_SonicWALL | 192.168.1.0/24<>192.168.2.0/24 | 172.101.30.73 | P: 172.100.... | 104 | 86316 | 0[0 bytes] | 0[0 bytes] |

Page 1 of 1 | Show 50 items | Displaying 1 - 1 of 1

Go to SonicWALL **VPN > VPN Settings > VPN Policies**, the status green light is on.

VPN > VPN Settings > VPN Policies

VPN Policies

Refresh Interval (secs)

10

Items per page

50

Items

1

 to 3 (of 3)

| <div><input type="checkbox"/></div> | # | Name | Gateway | Destinations | Crypto Suite | Enable |
|-------------------------------------|---|---------------|---------------|--|------------------------------|--|
| <div><input type="checkbox"/></div> | 1 | VPN_to_ZyWALL | 172.10.120.11 | <div><div></div></div> 192.168.1.0 - 192.168.1.255 | ESP: AES-128/HMAC SHA1 (IKE) | <div><input checked="" type="checkbox"/></div> |

Go to SonicWALL **VPN > VPN Settings > Currently Active VPN Tunnels > VPN Tunnel Statics** to check **Tunnel valid time**, **Bytes In** (Incoming Data) and **Bytes Out** (Outgoing Data).

VPN > VPN Settings > Currently Active VPN Tunnels

| Currently Active VPN Tunnels | | | | | | |
|------------------------------|---------------------|----------------------------|---------------------------------|-----------------------------|---------------|-------------|
| | | Refresh Interval (secs) 10 | | Items per page 50 | Items 1 | to 1 (of 1) |
| # | Created | Name | Local | Remote | Gateway | Actions |
| 1 | 10/04/2015 15:07:06 | VPN_to_ZyWALL | 192.168.168.0 - 192.168.168.255 | 192.168.1.0 - 192.168.1.255 | 172.10.120.11 | Renegotiate |

VPN Tunnel Statistics

Create Time 10/04/2015 15:07:06

Tunnel valid until 10/04/2015 23:07:06

Packets In 378

Packets Out 370

Bytes In 20080

Bytes Out 16640

Fragments In 0

Fragments Out 0

To test whether a tunnel is working, ping from a computer at one site to a computer at the other. Ensure that both computers have Internet access (via the IPSec devices).

PC behind ZyWALL/USG > Window 7 > cmd > ping 192.168.168.33

```
C:\Documents and Settings\ZyXEL>ping 192.168.168.33

Pinging 192.168.168.33 with 32 bytes of data:

Reply from 192.168.168.33: bytes=32 time=18ms TTL=54
Reply from 192.168.168.33: bytes=32 time=17ms TTL=54
Reply from 192.168.168.33: bytes=32 time=17ms TTL=54
Reply from 192.168.168.33: bytes=32 time=16ms TTL=54

Ping statistics for 192.168.168.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 18ms, Average = 17ms
```

PC behind SonicWALL> Window 7 > cmd > ping 192.168.1.33

```
C:\Documents and Settings\ZyXEL>ping 192.168.1.33

Pinging 192.168.1.33 with 32 bytes of data:

Reply from 192.168.1.33: bytes=32 time=27ms TTL=43
Reply from 192.168.1.33: bytes=32 time=32ms TTL=43
Reply from 192.168.1.33: bytes=32 time=26ms TTL=43
Reply from 192.168.1.33: bytes=32 time=27ms TTL=43

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 32ms, Average = 28ms
```

What Could Go Wrong?

If you see below [info] or [error] log message, please check ZyWALL/USG Phase 1 Settings. Both ZyWALL/USG and SonicWALL must use the same Pre-Shared Key, Encryption, Authentication method, DH key group and ID Type to establish the IKE SA.

MONITOR > Log

| Priority | Category | Message | Source | Destination | Note |
|----------|----------|--|-------------------|-------------------|---------|
| info | IKE | Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN] | 172.101.30.73:... | 172.100.30.80:... | IKE_LOG |
| info | IKE | [SA] : No proposal chosen | 172.101.30.73:... | 172.100.30.80:... | IKE_LOG |
| info | IKE | [SA] : Tunnel [VPN_to_SonicWALL] Phase 1 proposal mismatch | 172.101.30.73:... | 172.100.30.80:... | IKE_LOG |

If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG and SonicWALL Phase 2 Settings. Both ZyWALL/USG and SonicWALL must use the same Protocol, Encapsulation, Encryption, Authentication method and PFS to establish the IKE SA.

MONITOR > Log

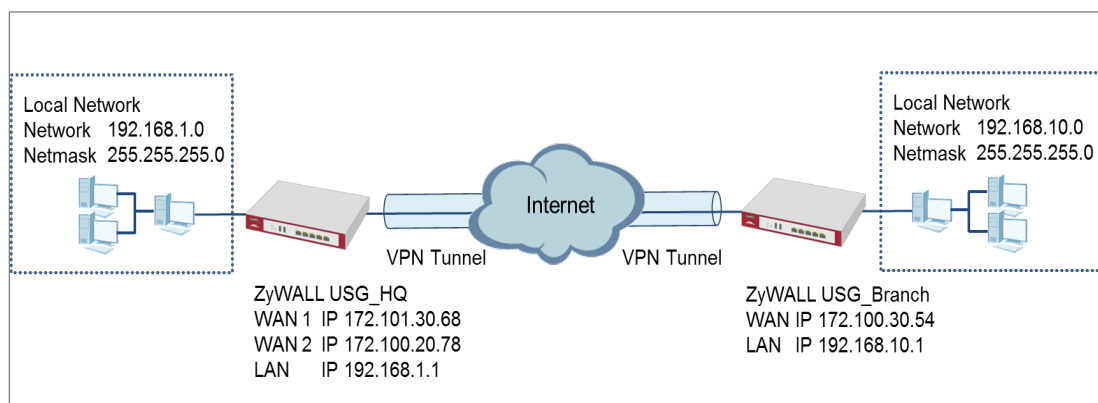
| Priority | Category | Message | Source | Destination | Note |
|----------|----------|--|-------------------|-------------------|---------|
| info | IKE | Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN] | 172.101.30.73:... | 172.100.30.80:... | IKE_LOG |
| info | IKE | [SA] : No proposal chosen | 172.101.30.73:... | 172.100.30.80:... | IKE_LOG |
| info | IKE | [SA] : Tunnel [VPN_to_SonicWALL] Phase 2 proposal mismatch | 172.101.30.73:... | 172.100.30.80:... | IKE_LOG |
| info | IKE | Recv:[HASH][SA][NONCE][ID][ID] | 172.100.30.80:... | 172.101.30.73:... | IKE_LOG |
| info | IKE | Phase 1 IKE SA process done | 172.101.30.73:... | 172.100.30.80:... | IKE_LOG |

Make sure the both ZyWALL/USG and SonicWALL security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.


Default NAT traversal is enable on ZyWALL/USG, please make sure the remote IPSec device must also have NAT traversal enabled.

How to Configure IPsec VPN Failover

This example shows how to use the VPN Setup Wizard to create a site-to-site VPN with failover. The example instructs how to configure the VPN tunnel between each site if one site has multi-WAN. When the multi-WAN VPN failover is configured, IPsec VPN tunnels automatically fail over to a backup WAN interface if the primary WAN interface becomes unavailable.



ZyWALL Site-to-site IPsec VPN with multiple WAN failover

 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG110 (Firmware Version: ZLD 4.25).

Set Up the ZyWALL/USG IPSec VPN Tunnel of Corporate Network (HQ)

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Please select the type of VPN policy you wish to setup.

Type of VPN policy

- ☒ Express
- ☐ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name:

WIZ_VPN_HQ

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

Configure **Secure Gateway** IP as the peer ZyWALL/USG's WAN IP address (in the example, 172.100.30.54). Type a secure **Pre-Shared Key** (8-32 characters).

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the peer ZyWALL/USG.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Configuration

Secure Gateway: 172.100.30.54 (IP or FQDN)

Pre-Shared Key: ZyXEL123

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Summary

Rule Name: WIZ_VPN_HQ

Secure Gateway: 172.100.30.54

Pre-Shared Key: ZyXEL123

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Congratulations. The VPN Access wizard is completed

Summary

| | |
|--------------------------|------------------------------|
| Rule Name: | WIZ_VPN_HQ |
| Secure Gateway: | 172.100.30.54 |
| Pre-Shared Key: | ZyXEL123 |
| Local Policy (IP/Mask): | 192.168.1.0 / 255.255.255.0 |
| Remote Policy (IP/Mask): | 192.168.10.0 / 255.255.255.0 |

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** and click **Show Advanced Settings**. Configure **Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPSec router.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type

Authentication

☒ Pre-Shared Key

.....

☐ unmasked

☐ Certificate

default

(See [My Certificates](#))

☐ User Based PSK

Remote_Client

i

☐ Advance

Local ID Type:

IPv4

Content:

0.0.0.0

Peer ID Type:

Any

Content:

172.100.30.54

Set Up the ZyWALL/USG IPSec VPN Tunnel of Corporate Network (Branch)

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Welcome

☒ VPN Settings

- Wizard Type
- VPN Settings
- Wizard Completed

☐ VPN Settings for Configuration Provisioning

- Wizard Type
- VPN Settings
- Wizard Completed

☐ VPN Settings for L2TP VPN Settings

- VPN Settings
- General Settings
- Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and to use a pre-shared key. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Please select the type of VPN policy you wish to setup.

Type of VPN policy

☒ Express

☐ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name: WIZ_VPN_Branch

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

Configure **Secure Gateway** IP as the peer ZyWALL/USG's WAN IP address (in the example, 172.101.30.68). Type a secure **Pre-Shared Key** (8-32 characters).

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the peer ZYWALL/USG.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Configuration

Secure Gateway: 172.101.30.68 (IP or FQDN)

Pre-Shared Key: ZyXEL123

Local Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings
Summary
Rule Name: WIZ_VPN_Branch
Secure Gateway: 172.101.30.68
Pre-Shared Key: ZyXEL123
Local Policy (IP/Mask): 192.168.10.0 / 255.255.255.0
Remote Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed

VPN Setup Wizard

Wizard Type > VPN Settings > **Wizard Completed**

1 2 3

Express Settings
Congratulations. The VPN Access wizard is completed
Summary
Rule Name: WIZ_VPN_Branch
Secure Gateway: 172.101.30.68
Pre-Shared Key: ZyXEL123
Local Policy (IP/Mask): 192.168.10.0 / 255.255.255.0
Remote Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** and click **Show Advanced Settings**. Configure **Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPSec router.

CONFIGURATION > VPN > IPsec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type

Authentication

☒ Pre-Shared Key

.....

unmasked

☐ Certificate

default

(See [My Certificates](#))

☐ User Based PSK

Remote_Client

☒ Advance

Local ID Type: IPv4

Content: 0.0.0.0

Peer ID Type: Any

Content: 172.101.30.68

Go to **Configuration > VPN > IPsec VPN > VPN Gateway > Gateway Settings**. Set **My Address** to be **Domain Name/IP** "0.0.0.0" (ZyWALL/USG will dial-up with the active WAN interface first). Set **Peer Gateway Address > Static Address > Primary** to be ZyWALL/USG_HQ WAN1 IP address and **Secondary** to be ZyWALL/USG_HQ WAN2 IP address.

Configuration > VPN > IPsec VPN > VPN Gateway > Gateway Settings

General Settings

☒ Enable

VPN Gateway Name: WIZ_VPN_Branch

IKE Version

☒ IKEv1
 ☐ IKEv2

Gateway Settings

My Address

☐ Interface

ge1

Static -- 0.0.0.0/0.0.0.0

☒ Domain Name / IPv4

0.0.0.0

Peer Gateway Address

☒ Static Address

Primary 172.101.30.68

Secondary 172.100.20.78

☒ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: 300 (60-86400 seconds)

☐ Dynamic Address

Set up the WAN Trunk (ZyWALL/USG_HQ)

Go to **CONFIGURATION > Interface > Trunk > User Configuration > Add**. Select wan1 and wan2 into the trunk **Member** and set wan2 **Mode** to be **Passive**.

CONFIGURATION > Interface > Trunk > User Configuration > Add

+ Add Trunk

Name: Multi_WAN_Failover

Load Balancing Algorithm: Least Load First

Load Balancing Index(es): Outbound

| # | Member | Mode | Egress Bandwidth |
|---|--------|---------|------------------|
| 1 | wan1 | Active | 1048576 kbps |
| 2 | wan2 | Passive | 1048576 kbps |

Page 0 of 0 Show 50 items No data to display

OK Cancel

Go to **CONFIGURATION > Interface > Trunk > Configuration**. Select **Disconnect Connection before Falling Back**. In the **Default WAN Trunk**, select **User Configured Trunk** to be the customized WAN trunk added in the previous step (Multi_WAN_Failover in this example).

CONFIGURATION > Interface > Trunk > User Configuration > Add

Configuration

☒ Disconnect Connections Before Falling Back i

Default WAN Trunk

☐ Advance

Default Trunk Selection

☐ SYSTEM_DEFAULT_WAN_TRUNK
☒ User Configured Trunk Multi_WAN_Failover

User Configuration

| # | Name | Algorithm |
|---|--------------------|-----------|
| 1 | Multi_WAN_Failover | lbf |

+ Add ✎ Edit ✖ Remove 🔗 Object References

Page 1 of 1 | Show 50 items | Displaying 1 - 1 of 1

Set up the Failover Command Line (ZyWALL/USG HQ)

Go to **CONFIGURATION > Security Policy > Policy Control** and add a **To ZyWALL** rule to allow **SSH** service.

CONFIGURATION > Security Policy > Policy Control > Add corresponding

+ Add corresponding ? X

🔗 Create new Object ▼

☒ Enable

Name: Any_to_ZyWall_SSH
 Description: (Optional)
 From: any ▼
 To: ZyWALL ▼
 Source: any ▼
 Destination: any ▼
 Service: SSH ▼
 User: any ▼
 Schedule: none ▼
 Action: allow ▼
 Log matched traffic: no ▼

OK Cancel

If the **Security Policy** is created but still cannot access to ZyWALL, please go to **CONFIGURAITON > System > SSH** to check do you **Enable** the **General Settings** and make sure the **Service Port** is correct and the same in your terminal program. Then, check the **Service Control Action** should be **Accept**.

CONFIGURAITON > System > SSH

General Settings

☒ Enable

☐ Version 1

Server Port:

Server Certificate:

Service Control

+ Add Edit Remove Move

| # | Zone | Address | Action |
|---|------|---------|--------|
| - | ALL | ALL | Accept |

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

Enter the command line in terminal mode (Using Tera Term in this example).

Tera Term command

```
Welcome to USG110

Username: admin
Password:
Router> configure terminal
Router(config)# client-side-vpn-failover-fallback activate
```

Test the IPSec VPN Tunnel

- Go to ZYWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

IPv4 Configuration

+ Add Edit Remove Activate Inactivate Connect Disconnect Object References

| # | Status | Name | VPN Gateway | Policy |
|---|--------|------------|-------------|--|
| 1 | | WIZ_VPN_HQ | WIZ_VPN_HQ | VPN_to_Cisco_LOCAL/VPN_to_Cisco_REMOTE |

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

- Go to ZyWALL/USG MONITOR > VPN Monitor > IPSec and verify the tunnel Up Time and Inbound(Bytes)/Outbound(Bytes) Traffic.

MONITOR > VPN Monitor > IPSec

| Disconnect | | Connection Check | | | | | | |
|------------|------|----------------------------------|---------------|------------------|---------|---------|----------------|-----------------|
| # | Name | Policy | My Address | Secure Gateway | Up Time | Timeout | Inbound(Bytes) | Outbound(Bytes) |
| 1 | test | 192.168.10.0/24<>192.168.10.0/24 | 172.101.30.54 | P: 172.101.30.68 | 10 | 79190 | 0(0 bytes) | 0(0 bytes) |

- Go to ZyWALL/USG_Branch **MONITOR > Log**. Try to disconnect WAN1 interface (172.1.1.30.68) and you will see the VPN tunnel failover to WAN2 interface (172.100.20.78).

MONITOR > Log

| # | Time | Priority | Cat. | Message | Source | Destination | Note |
|----|---------------------|----------|------|---|---------------|---------------|--------|
| 1 | 2017-07-28 16:33:40 | info | DE | Tunnel [172.101.30.54] [172.101.30.68] bulk successful | 172.101.30.54 | 172.101.30.68 | NE_LOG |
| 2 | 2017-07-28 16:33:40 | info | DE | [ESP] desc: hmac-sha1-MD5 [SPI: 0x00000000] [SA: 172.101.30.54] [TA: 172.101.30.68] | 172.101.30.54 | 172.101.30.68 | NE_LOG |
| 3 | 2017-07-28 16:33:40 | info | DE | [PktInfo] [SPI: 0x00000000] [SA: 172.101.30.54] [TA: 172.101.30.68] [P: 172.101.30.68] [D: 172.101.30.54] | 172.101.30.54 | 172.101.30.68 | NE_LOG |
| 4 | 2017-07-28 16:33:40 | info | DE | [Response] 172.101.30.54 [172.101.30.68] | 172.101.30.54 | 172.101.30.68 | NE_LOG |
| 5 | 2017-07-28 16:33:40 | info | DE | Recv [4096] | 172.101.30.68 | 172.101.30.54 | NE_LOG |
| 6 | 2017-07-28 16:33:40 | info | DE | Send [4096] [172.101.30.68] | 172.101.30.54 | 172.101.30.68 | NE_LOG |
| 7 | 2017-07-28 16:33:40 | info | DE | Recv: [172.101.30.68] [172.101.30.54] [172.101.30.68] [172.101.30.54] | 172.101.30.68 | 172.101.30.54 | NE_LOG |
| 8 | 2017-07-28 16:33:40 | info | DE | Recv: [172.101.30.68] [172.101.30.54] [172.101.30.68] [172.101.30.54] | 172.101.30.68 | 172.101.30.54 | NE_LOG |
| 9 | 2017-07-28 16:33:40 | info | DE | Recv: [172.101.30.68] [172.101.30.54] [172.101.30.68] [172.101.30.54] | 172.101.30.68 | 172.101.30.54 | NE_LOG |
| 10 | 2017-07-28 16:33:40 | info | DE | Phase 1 IKE SA process done | 172.101.30.54 | 172.101.30.68 | NE_LOG |
| 11 | 2017-07-28 16:33:40 | info | DE | Send [172.101.30.68] | 172.101.30.54 | 172.101.30.68 | NE_LOG |
| 12 | 2017-07-28 16:33:40 | info | DE | Recv: [172.101.30.68] [172.101.30.54] [172.101.30.68] [172.101.30.54] | 172.101.30.68 | 172.101.30.54 | NE_LOG |
| 13 | 2017-07-28 16:33:40 | info | DE | Send [172.101.30.68] [172.101.30.54] [172.101.30.68] [172.101.30.54] | 172.101.30.68 | 172.101.30.54 | NE_LOG |
| 14 | 2017-07-28 16:33:40 | info | DE | Recv [172.101.30.68] [172.101.30.54] [172.101.30.68] [172.101.30.54] | 172.101.30.68 | 172.101.30.54 | NE_LOG |
| 15 | 2017-07-28 16:33:40 | info | DE | Send [172.101.30.68] [172.101.30.54] [172.101.30.68] [172.101.30.54] | 172.101.30.68 | 172.101.30.54 | NE_LOG |
| 16 | 2017-07-28 16:33:40 | info | DE | The cookie pair is: [0x00000000] [0x00000000] [0x00000000] [0x00000000] | 172.101.30.54 | 172.101.30.68 | NE_LOG |
| 17 | 2017-07-28 16:33:40 | info | DE | Recv: [172.101.30.68] [172.101.30.54] [172.101.30.68] [172.101.30.54] | 172.101.30.68 | 172.101.30.54 | NE_LOG |
| 18 | 2017-07-28 16:33:40 | info | DE | Recv: [172.101.30.68] [172.101.30.54] [172.101.30.68] [172.101.30.54] | 172.101.30.68 | 172.101.30.54 | NE_LOG |
| 19 | 2017-07-28 16:33:40 | info | DE | The cookie pair is: [0x00000000] [0x00000000] [0x00000000] [0x00000000] | 172.101.30.54 | 172.101.30.68 | NE_LOG |
| 20 | 2017-07-28 16:33:40 | info | DE | Recv: [172.101.30.68] [172.101.30.54] [172.101.30.68] [172.101.30.54] | 172.101.30.68 | 172.101.30.54 | NE_LOG |
| 21 | 2017-07-28 16:33:40 | info | DE | The cookie pair is: [0x00000000] [0x00000000] [0x00000000] [0x00000000] | 172.101.30.54 | 172.101.30.68 | NE_LOG |
| 22 | 2017-07-28 16:33:40 | info | DE | [IKE] [172.101.30.68] [172.101.30.54] [172.101.30.68] [172.101.30.54] | 172.101.30.68 | 172.101.30.54 | NE_LOG |
| 23 | 2017-07-28 16:33:40 | info | DE | ISAKMP SA [172.101.30.68] is disconnected | 172.101.30.54 | 172.101.30.68 | NE_LOG |
| 24 | 2017-07-28 16:33:40 | info | DE | Received data notification | 172.101.30.54 | 172.101.30.68 | NE_LOG |
| 25 | 2017-07-28 16:33:40 | info | DE | Recv: [172.101.30.68] [172.101.30.54] [172.101.30.68] [172.101.30.54] | 172.101.30.68 | 172.101.30.54 | NE_LOG |
| 26 | 2017-07-28 16:33:40 | info | DE | Send: [172.101.30.68] [172.101.30.54] [172.101.30.68] [172.101.30.54] | 172.101.30.68 | 172.101.30.54 | NE_LOG |
| 27 | 2017-07-28 16:33:40 | info | DE | Recv: [172.101.30.68] [172.101.30.54] [172.101.30.68] [172.101.30.54] | 172.101.30.68 | 172.101.30.54 | NE_LOG |
| 28 | 2017-07-28 16:33:40 | info | DE | Recv: [172.101.30.68] [172.101.30.54] [172.101.30.68] [172.101.30.54] | 172.101.30.68 | 172.101.30.54 | NE_LOG |
| 29 | 2017-07-28 16:33:40 | info | DE | The cookie pair is: [0x00000000] [0x00000000] [0x00000000] [0x00000000] | 172.101.30.54 | 172.101.30.68 | NE_LOG |
| 30 | 2017-07-28 16:33:40 | info | DE | Send: [172.101.30.68] [172.101.30.54] [172.101.30.68] [172.101.30.54] | 172.101.30.68 | 172.101.30.54 | NE_LOG |
| 31 | 2017-07-28 16:33:40 | info | DE | The cookie pair is: [0x00000000] [0x00000000] [0x00000000] [0x00000000] | 172.101.30.54 | 172.101.30.68 | NE_LOG |
| 32 | 2017-07-28 16:33:40 | info | DE | Send: [172.101.30.68] [172.101.30.54] [172.101.30.68] [172.101.30.54] | 172.101.30.68 | 172.101.30.54 | NE_LOG |
| 33 | 2017-07-28 16:33:40 | info | DE | Recv: [172.101.30.68] [172.101.30.54] [172.101.30.68] [172.101.30.54] | 172.101.30.68 | 172.101.30.54 | NE_LOG |
| 34 | 2017-07-28 16:33:40 | info | DE | Recv: [172.101.30.68] [172.101.30.54] [172.101.30.68] [172.101.30.54] | 172.101.30.68 | 172.101.30.54 | NE_LOG |
| 35 | 2017-07-28 16:33:40 | info | DE | The cookie pair is: [0x00000000] [0x00000000] [0x00000000] [0x00000000] | 172.101.30.54 | 172.101.30.68 | NE_LOG |
| 36 | 2017-07-28 16:33:40 | info | DE | Send: [172.101.30.68] [172.101.30.54] [172.101.30.68] [172.101.30.54] | 172.101.30.68 | 172.101.30.54 | NE_LOG |
| 37 | 2017-07-28 16:33:40 | info | DE | The cookie pair is: [0x00000000] [0x00000000] [0x00000000] [0x00000000] | 172.101.30.54 | 172.101.30.68 | NE_LOG |
| 38 | 2017-07-28 16:33:40 | info | DE | ISAKMP SA [172.101.30.68] is disconnected | 172.101.30.54 | 172.101.30.68 | NE_LOG |
| 39 | 2017-07-28 16:33:40 | info | DE | Tunnel [172.101.30.54] [172.101.30.68] bulk successful | 172.101.30.54 | 172.101.30.68 | NE_LOG |
| 40 | 2017-07-28 16:33:40 | info | DE | [ESP] desc: hmac-sha1-MD5 [SPI: 0x00000000] [SA: 172.101.30.54] [TA: 172.101.30.68] | 172.101.30.54 | 172.101.30.68 | NE_LOG |
| 41 | 2017-07-28 16:33:40 | info | DE | [PktInfo] [SPI: 0x00000000] [SA: 172.101.30.54] [TA: 172.101.30.68] [P: 172.101.30.68] [D: 172.101.30.54] | 172.101.30.54 | 172.101.30.68 | NE_LOG |
| 42 | 2017-07-28 16:33:40 | info | DE | [Response] 172.101.30.54 [172.101.30.68] | 172.101.30.54 | 172.101.30.68 | NE_LOG |
| 43 | 2017-07-28 16:33:40 | info | DE | Recv [4096] [172.101.30.68] | 172.101.30.68 | 172.101.30.54 | NE_LOG |
| 44 | 2017-07-28 16:33:40 | info | DE | Tunnel [172.101.30.54] [172.101.30.68] bulk successful | 172.101.30.54 | 172.101.30.68 | NE_LOG |
| 45 | 2017-07-28 16:33:40 | info | DE | The cookie pair is: [0x00000000] [0x00000000] [0x00000000] [0x00000000] | 172.101.30.54 | 172.101.30.68 | NE_LOG |
| 46 | 2017-07-28 16:33:40 | info | DE | Recv: [172.101.30.68] [172.101.30.54] [172.101.30.68] [172.101.30.54] | 172.101.30.68 | 172.101.30.54 | NE_LOG |

What Could Go Wrong?

- 11** If you see below [info] or [error] log message, please check ZyWALL/USG Phase 1 Settings. Both ZyWALL/USG at the HQ and Branch sites must use the same Pre-Shared Key, Encryption, Authentication method, DH key group and ID Type to establish the IKE SA.

MONITOR > Log

| Priority | Category | Message | Note |
|----------|----------|--|---------|
| Info | IKE | Send:[NOTIFY:NO_PROPOSAL_CHOSEN] | IKE_LOG |
| Info | IKE | [SA] : No proposal chosen | IKE_LOG |
| Info | IKE | [SA] : Tunnel [WIZ_VPN_HQ] Phase 1 proposal mismatch | IKE_LOG |

- 12** If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG Phase 2 Settings. Both ZyWALL/USG at the HQ and Branch sites must use the same Protocol, Encapsulation, Encryption, Authentication method and PFS to establish the IKE SA.

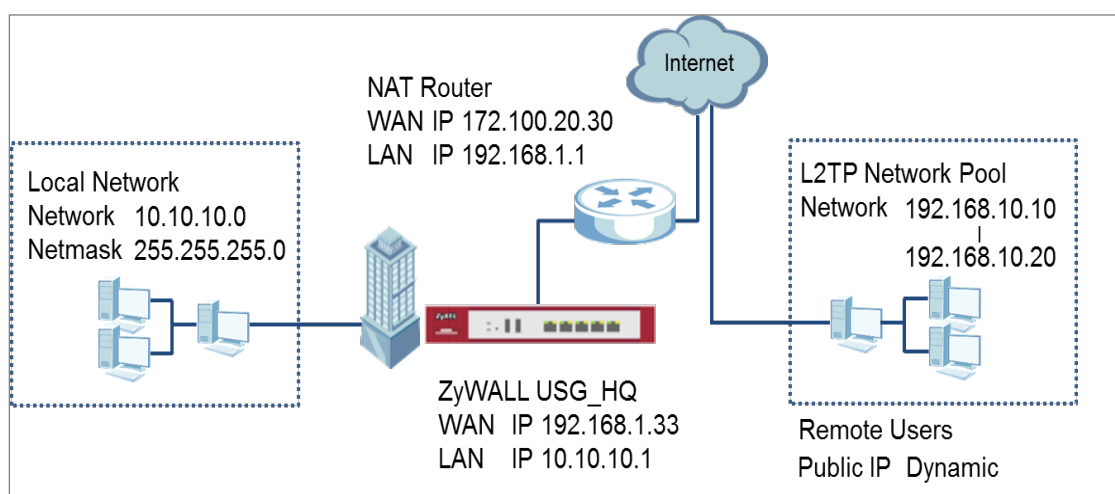
MONITOR > Log

| Priority | Category | Message | Note |
|----------|----------|--|---------|
| Info | IKE | Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN] | IKE_LOG |
| Info | IKE | [SA] : No proposal chosen | IKE_LOG |
| Info | IKE | [SA] : Tunnel [WIZ_VPN_HQ] Phase 2 proposal mismatch | IKE_LOG |
| Info | IKE | Recv:[HASH][SA][NONCE][ID][ID] | IKE_LOG |
| Info | IKE | Phase 1 IKE SA process done | IKE_LOG |

- 13** Make sure the both ZyWALL/USG at the HQ and Branch sites security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.
- 14** Default NAT traversal is enable on ZyWALL/USG, please make sure the remote IPSec device must also have NAT traversal enabled.

How to Configure L2TP over IPsec VPN while the ZyWALL/USG is behind a NAT router

This example shows how to use the VPN Setup Wizard to create a L2TP over IPsec VPN tunnel between ZyWALL/USG devices. The example instructs how to configure the VPN tunnel between each site while the ZyWALL/USG is behind a NAT router. When the L2TP over IPsec VPN tunnel is configured, each site can be accessed securely.



ZyWALL/USG L2TP over IPsec VPN while the ZyWALL/USG is behind a NAT router



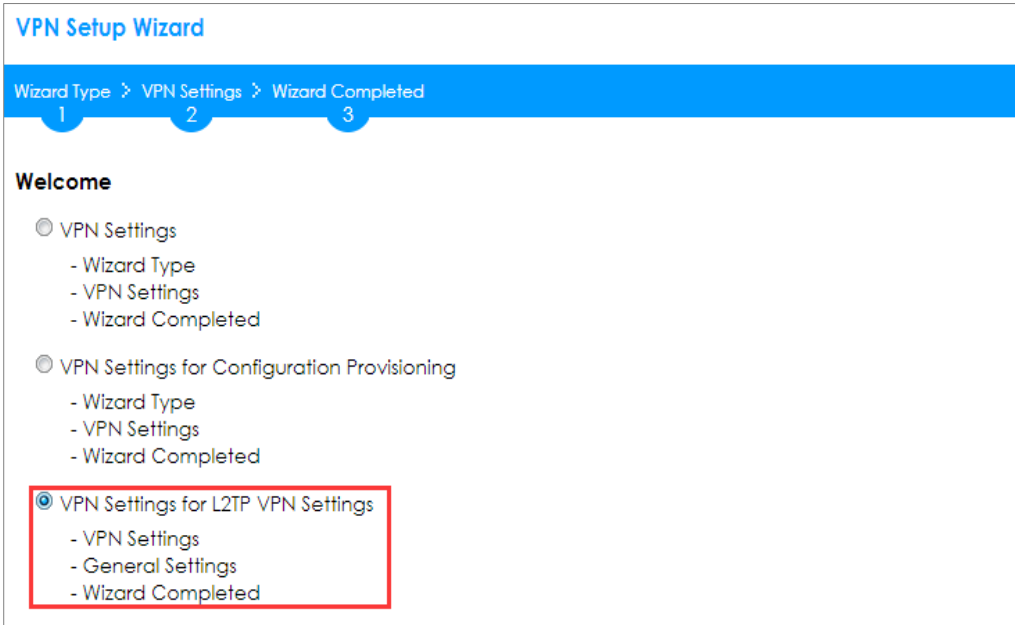
Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG110 (Firmware Version: ZLD 4.25).

Set Up the L2TP VPN Tunnel on the ZyWALL/USG_HQ

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings for L2TP VPN Settings** wizard to create a **L2TP VPN** rule that can be used with the remote Android Mobile Devices. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Welcome

- ☐ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☒ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

Then, configure the **Rule Name** and set **My Address** to be the **wan1** interface which is connected to the Internet. Type a secure **Pre-Shared Key** (8-32 characters).

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings

VPN Setup Wizard

VPN Settings > General Settings > Wizard Completed

1 2 3

L2TP VPN Settings

Rule Name:

Phase 1 Setting

My Address (interface):

Authentication Method

Pre-Shared Key:

Assign the remote users IP addresses range from 192.168.10.10 to 192.168.10.20 for use in the L2TP VPN tunnel and check **Allow L2TP traffic Through WAN** to allow traffic from L2TP clients to go to the Internet. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (L2TP VPN Settings)

VPN Setup Wizard

VPN Settings > General Settings > Wizard Completed

1 2 3

L2TP VPN Settings

IP Address Pool: ⓘ

Starting IP Address:

End IP Address:

First DNS Server (Optional):

Second DNS Server (Optional):

☒ Allow L2TP traffic Through WAN

15 This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (Summary)

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

Summary

Rule Name: WIZ_L2TP_VPN
Secure Gateway: Any
Pre-Shared Key: xyz12345
My Address (interface): wan1
IP Address Pool: RANGE, 192.168.10.10 - 192.168.10.20

Now the rule is configured on the ZyWALL/USG. The rule settings appear in the **VPN > L2TP VPN** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings > Wizard Completed

VPN Setup Wizard

Wizard Type > VPN Settings > **Wizard Completed**

1 2 3

L2TP VPN Settings

Congratulations. The VPN Access wizard is completed

Summary

Rule Name: WIZ_L2TP_VPN
My Address (interface): wan1
Pre-Shared Key: xyz12345
IP Address Pool: RANGE, 192.168.10.10 - 192.168.10.20

Go to **CONFIGURATION > VPN Connection > Create new Object > Create Address**, create an address object as the NAT router's WAN IP address (in the example, 172.100.20.30).

CONFIGURATION > VPN Connection > Create new Object > Create Address

+
Add Address Rule
?
X

Name:

Address Type:

IP Address:

OK
Cancel

Go to **CONFIGURATION > VPN Connection > Policy > Local Policy**, select it be to the NAT router's WAN IP address (in the example, 172.100.20.30).

CONFIGURATION > VPN Connection > Policy > Local Policy

General Settings

☒ Enable

Connection Name:

☒ Advance

VPN Gateway

Application Scenario

☐ Site-to-site
 ☐ Site-to-site with Dynamic Peer
 ☒ Remote Access (Server Role)
 ☐ Remote Access (Client Role)
 ☐ Vpn Tunnel Interface

VPN Gateway:

Policy

Local policy:

Go to **CONFIGURATION > VPN > L2TP VPN > Create new Object > User** to add **User Name** and **Password** (4-24 characters). Then, set **Allowed User** to the newly created object (L2TP_Remote_Users/zyx168 in this example).

CONFIGURATION > VPN > L2TP VPN > Create new Object > User

The image shows two screenshots from the ZyXEL web interface. The top screenshot is the 'L2TP VPN' configuration page. It has a blue header with 'L2TP VPN' and a 'Show Advanced Settings' button. Below the header is a 'Create new Object' dropdown menu with 'User' selected. The 'General Settings' section includes: 'Enable L2TP Over IPSec' (checked), 'VPN Connection' (WIZ_L2TP_VPN), 'IP Address Pool' (WIZ_L2TP_VPN_IP_1), 'Authentication Method' (default), 'Advance' (expanded), 'Allowed User' (any), 'Keep Alive Timer' (60 seconds), and DNS/WINS servers. The bottom screenshot is the 'Add A User' dialog box. It has a 'User Configuration' section with: 'User Name' (L2TP_Remote_Users), 'User Type' (user), 'Password' (masked), 'Retype' (masked), 'Description' (Local User), and 'Authentication Timeout Settings' (Use Default Settings, Lease Time: 1440 minutes, Reauthentication Time: 1440 minutes). OK and Cancel buttons are at the bottom.

Set Up the NAT Router (Using ZyWALL USG device in this example)

Go to **CONFIGURATION > Network > NAT > Add**. Select the **Incoming Interface** on which packets for the NAT rule must be received. Specified the **User-Defined Original IP** field and Type the translated destination IP address that this NAT rule supports.

CONFIGURATION > Network > NAT > Add

| General Settings | |
|---|--|
| <input checked="" type="checkbox"/> Enable Rule | |
| Rule Name: | VPN_NAT |
| Port Mapping Type | |
| Classification: | <input type="radio"/> Virtual Server <input checked="" type="radio"/> 1:1 NAT <input type="radio"/> Many 1:1 NAT |
| Mapping Rule | |
| Incoming Interface: | wan1 |
| Original IP: | User Defined |
| User-Defined Original IP: | 172.100.20.30 (IP Address) |
| Mapped IP: | User Defined |
| User-Defined Mapped IP: | 192.168.1.33 (IP Address) |
| Port Mapping Type: | any |

Go to **CONFIGURATION > Object > Address > Add**, create an address object as the ZyWALL/USU_HQ's WAN IP address (in the example, 192.168.1.33).

CONFIGURATION > Object > Address

| + Add Address Rule | |
|---|--------------|
| Name: | L2TP_WAN_IP |
| Address Type: | HOST |
| IP Address: | 192.168.1.33 |
| <input type="button" value="OK"/> <input type="button" value="Cancel"/> | |

Go to **CONFIGURATION > Object > Service > Service Group**, create a service group for the following UDP ports:

UDP Port Number = 1701 → Used by L2TP

UDP Port Number = 500 → Used by IKE

UDP Port Number = 4500 → Used by NAT-T

CONFIGURATION > Service > Service Group

+ Add Service Group Rule

Configuration

Name: **L2TP-Allow**

Description:

Configuration

Available

=== Object ===

- AH
- AIM
- AUTH
- Any_TCP
- Any_UDP
- BGP
- BONJOUR
- BOOTP_CLIENT

Member

=== Object ===

- NATT**
- IKE**
- L2TP-UDP**

OK **Cancel**

Go to **CONFIGURATION > Security Policy > Policy Control**, add corresponding rule to allow L2TP services.

CONFIGURATION > Security Policy > Policy Control

+ Add corresponding

Create new Object ▼

☒ **Enable**

Name: **L2TP-Allow**

Description: (Optional)

From: any

To: any (Excluding ZyV)

Source: any

Destination: **L2TP_WAN_IP**

Service: **L2TP-Allow**

User: **L2TP_Remote_User**

Schedule: none

Action: allow

Log matched traffic: no

Test the L2TP over IPSec VPN Tunnel

Use a smartphone or a PC to establish a L2TP VPN connection to the ZyWALL/USG. Configure the NAT's public IP address as the L2TP server address on the client. In this example using iOS device to test the result:

To configure L2TP VPN in an iOS 8.4 device, go to **Menu > Settings > VPN > Add VPN Configuration** and configure as follows.

Description is for you to identify the VPN configuration.

Set **Server** to the ZyWALL/USG's WAN IP address (172.100.20.30 in this example).

Enter **Account** and **Password** which the same as **Allowed User** created in ZyWALL/USG (L2TP_Remote_Users/zyx168 in this example).

Set **Secret** to the **Pre-Shared Key** of the IPSec VPN gateway the ZyWALL/USG uses for L2TP VPN over IPSec (xyz12345 in this example).

<

VPN

ZyXEL_L2TP

Type

L2TP

Description

ZyXEL_L2TP

Server

172.100.20.30

Account

L2TP_Remote_Users

RSA SecurID

☐

Password

••••••

Secret

••••••••

Send All Traffic

☒

After you create a VPN configuration, slide the button right to the on position to initiate L2TP VPN session.

<

Settings

VPN

VPN CONFIGURATIONS

Not Connected

☐

✓

ZyXEL_L2TP

Custom

i

<

Settings

VPN

VPN CONFIGURATIONS

Connected

☒

✓

ZyXEL_L2TP

Custom

i

Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

| IPv4 Configuration | | | | |
|--|---|--------------|--------------|-------------------------------------|
| Add Edit Remove Activate Inactivate Connect Disconnect Object References | | | | |
| # | Status | Name | VPN Gateway | Policy |
| 1 |  | WIZ_L2TP_VPN | WIZ_L2TP_VPN | WIZ_L2TP_VPN_LOCAL/ |

Go to ZyWALL/USG **MONITOR > VPN Monitor > L2TP over IPSec** and verify the **Current L2TP Session**.

MONITOR > VPN Monitor > L2TP over IPSec > L2TP_Remote_Users

| Current L2TP Session | | | | |
|---|-------------------|----------|---------------|--------------|
| Disconnect Refresh | | | | |
| # | User Name | Hostname | Assigned IP | Public IP |
| 1 | L2TP_Remote_Users | Android | 192.168.10.10 | 10.214.30.69 |
| < < Page 1 of 1 > > Show 50 items Displaying 1 - 1 of 1 | | | | |

Go to iOS mobile device **Menu > Settings > VPN > ZyXEL_L2TP** and verify the **Assigned IP Address** and **Connect Time**.

Menu > Settings > VPN > ZyXEL_L2TP

< VPN

ZyXEL_L2TP

| | |
|---------------------|---------------|
| Type | L2TP |
| Server | 172.100.20.30 |
| Assigned IP Address | 192.168.10.10 |
| Connect Time | 0:06 |

Description

ZyXEL_L2TP

| | |
|------------------|-------------------------------------|
| Server | 172.100.20.30 |
| Account | L2TP_Remote_Users |
| RSA SecurID | <input type="checkbox"/> |
| Password | •••••• |
| Secret | •••••••• |
| Send All Traffic | <input checked="" type="checkbox"/> |

What Could Go Wrong?

If you see [alert] log message such as below, please check ZyWALL/USG L2TP

Allowed User or **User/Group Settings**. iOS Mobile users must use the same Username and Password as configured in ZyWALL/USG to establish the L2TP VPN.

| Priority | Category | Message | Note |
|----------|-----------------|---|----------|
| alert | L2TP Over IPSec | User L2TP_Remote_Users has been denied from L2TP service.(Incorrect Username or Password) | L2TP_LOG |

If you see [info] or [error] log message such as below, please check ZyWALL/USG Phase 1 Settings. iOS Mobile users must use the same **Secret** as configured in ZyWALL/USG to establish the IKE SA.

| Priority | Category | Message | Note |
|----------|----------|--|---------|
| Info | IKE | Send:[NOTIFY:INVALID_PAYLOAD_TYPE] | IKE_LOG |
| Info | IKE | Invalid payload type in encrypted payload chain, possibly because of different pre-shared keys | IKE_LOG |

If you see that Phase 1 IKE SA process has completed but still get [info] log message as below, please check ZyWALL/USG Phase 2 Settings. ZyWALL/USG unit must set correct **Local Policy** to establish the IKE SA.

| Priority | Category | Message | Note |
|----------|----------|--|---------|
| Info | IKE | ISAKMP SA [WIZ_L2TP_VPN] is disconnected | IKE_LOG |
| Info | IKE | Received delete notification | IKE_LOG |
| Info | IKE | Recv:[HASH][DEL] | IKE_LOG |
| Info | IKE | Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN] | IKE_LOG |
| Info | IKE | [SA] : No proposal chosen | IKE_LOG |
| Info | IKE | [ID] : Tunnel [WIZ_L2TP_VPN] Phase 2 Local policy mismatch | IKE_LOG |

Ensure that the L2TP Address Pool does not conflict with any existing LAN1, LAN2, DMZ, or WLAN zones, even if they are not in use.

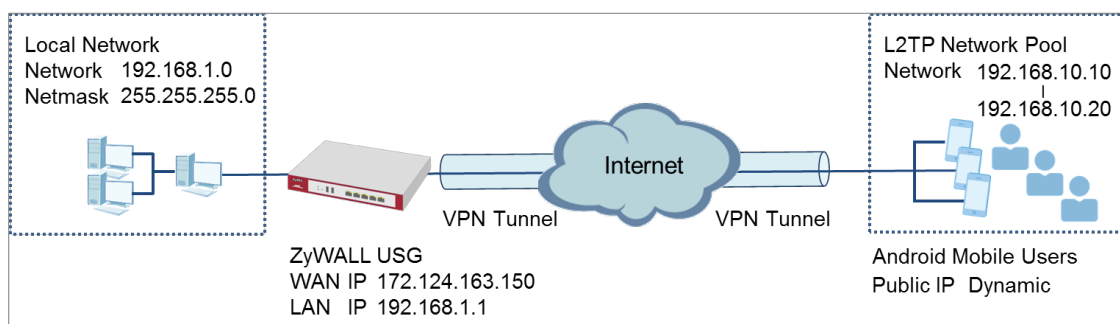
If you cannot access devices in the local network, verify that the devices in the local network set the USG's IP as their default gateway to utilize the L2TP tunnel.

Make sure the ZyWALL/USG units' security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.


Verify that the **Zone** is set correctly in the **Zone** object. This should be set to IPSec_VPN Zone so that security policies are applied properly.

How to Configure L2TP VPN with Android 5.0 Mobile Devices

This example shows how to use the VPN Setup Wizard to create a L2TP VPN between a ZyWALL/USG and an Android 5.0 Mobile Device. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely and allow traffic from L2TP clients to go to the Internet.



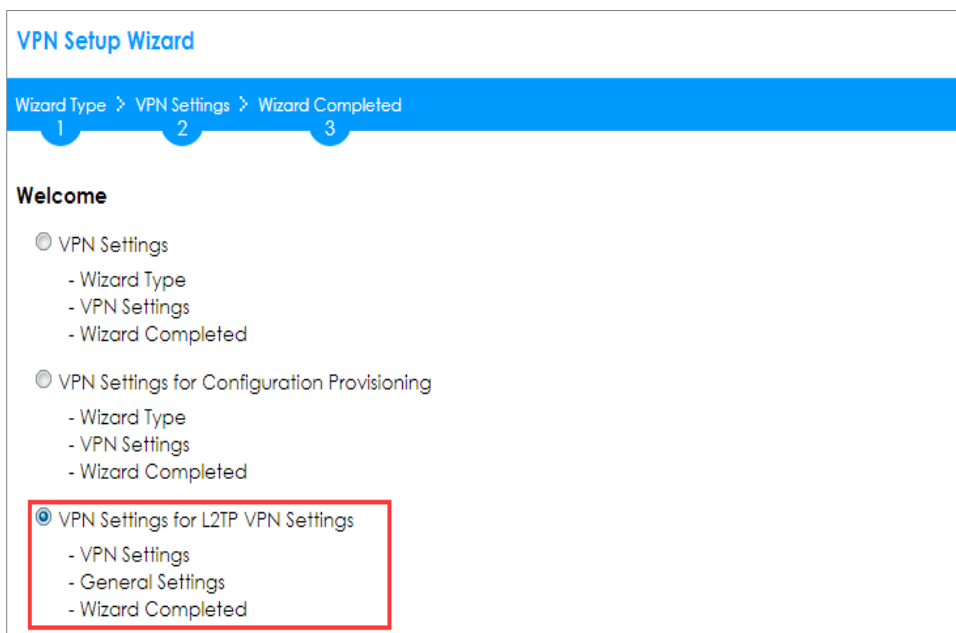
ZyWALL/USG L2TP VPN with Android Mobile Devices Example

 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: 4.25) and Android version (Firmware Version: 5.0)

Set Up the L2TP VPN Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings for L2TP VPN Settings** wizard to create a **L2TP VPN** rule that can be used with the remote Android Mobile Devices. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Welcome

- ☐ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☒ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

Then, configure the **Rule Name** and set **My Address** to be the **wan1** interface which is connected to the Internet. Type a secure **Pre-Shared Key** (8-32 characters).

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings

VPN Setup Wizard

VPN Settings > General Settings > Wizard Completed

1 2 3

L2TP VPN Settings

Rule Name:

Phase 1 Setting

My Address (interface):

Authentication Method

Pre-Shared Key:

Assign the remote users IP addresses range from 192.168.10.10 to 192.168.10.20 for use in the L2TP VPN tunnel and check **Allow L2TP traffic Through WAN** to allow traffic from L2TP clients to go to the Internet. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (L2TP VPN Settings)

VPN Setup Wizard

VPN Settings > General Settings > Wizard Completed

1 2 3

L2TP VPN Settings

IP Address Pool: ⓘ

Starting IP Address:

End IP Address:

First DNS Server (Optional):

Second DNS Server (Optional):

☒ Allow L2TP traffic Through WAN

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (Summary)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Express Settings

Summary

| | |
|-------------------------|--------------------------------------|
| Rule Name: | WIZ_L2TP_VPN |
| Secure Gateway: | Any |
| Pre-Shared Key: | xyz12345 |
| My Address (interface): | wan1 |
| IP Address Pool: | RANGE, 192.168.10.10 - 192.168.10.20 |

Now the rule is configured on the ZyWALL/USG. The rule settings appear in the **VPN > L2TP VPN** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings > Wizard Completed

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

L2TP VPN Settings

Congratulations. The VPN Access wizard is completed

Summary

| | |
|-------------------------|--------------------------------------|
| Rule Name: | WIZ_L2TP_VPN |
| My Address (interface): | wan1 |
| Pre-Shared Key: | xyz12345 |
| IP Address Pool: | RANGE, 192.168.10.10 - 192.168.10.20 |

Go to **CONFIGURATION > VPN > L2TP VPN > Create new Object > User** to add **User Name** and **Password** (4-24 characters). Then, set **Allowed User** to the newly created object (L2TP_Remote_Users/zyx168 in this example).

CONFIGURATION > VPN > L2TP VPN > Create new Object > User

The screenshot shows the 'L2TP VPN' configuration page with the 'Create new Object' dropdown menu open, highlighting the 'User' option. The 'General Settings' section includes:

- ☒ Enable L2TP Over IPSec
- VPN Connection: WIZ_L2TP_VPN
- IP Address Pool: WIZ_L2TP_VPN_IP_1 (Range: 192.168.100.10-192.168.100.20)
- Authentication Method: default (local)

The 'Advance' section includes:

- Allowed User: any
- Keep Alive Timer: 60 (1-180 seconds)
- First DNS Server (Optional): Custom Defined
- Second DNS Server (Optional): Custom Defined
- First WINS Server (Optional):
- Second WINS Server (Optional):

The 'User Configuration' dialog box shows the following fields:

- User Name: L2TP_Remote_Users
- User Type: user
- Password: (masked with dots)
- Retype: (masked with dots)
- Description: Local User
- Authentication Timeout Settings:
 - ☒ Use Default Settings
 - Lease Time: 1440 minutes
 - Reauthentication Time: 1440 minutes
 - ☐ Use Manual Settings

Buttons: OK, Cancel

If some of the traffic from the L2TP clients need to go to the Internet, create a policy route to send traffic from the L2TP tunnels out through a WAN trunk. Set **Incoming** to **Tunnel** and select your L2TP VPN connection. Set the **Source Address** to be the L2TP address pool. Set the **Next-Hop Type** to **Trunk** and select the appropriate WAN trunk.

CONFIGURATION > Network > Routing > Policy Route

Edit Policy Route

Show Advanced Settings
Create new Object ▼

Configuration

☒ Enable

Description: L2TP_VPN_to_Internet (Optional)

Criteria

User: L2TP_Remote_User ▼

Incoming: Tunnel ▼

Please select one member: WIZ_L2TP_VPN ▼

Source Address: WIZ_L2TP_VPN_IP_4 ▼

Destination Address: any ▼

DSCP Code: any ▼

Schedule: none ▼

Service: any ▼

Next-Hop

Type: Trunk ▼

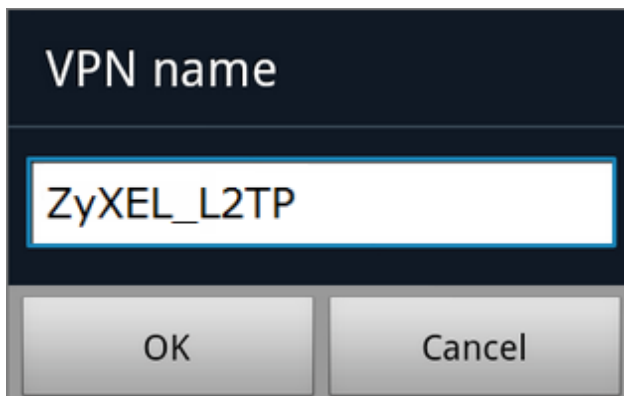
Trunk: SYSTEM_DEFAULT_V ▼

OK Cancel

Set Up the L2TP VPN Tunnel on the Android Device

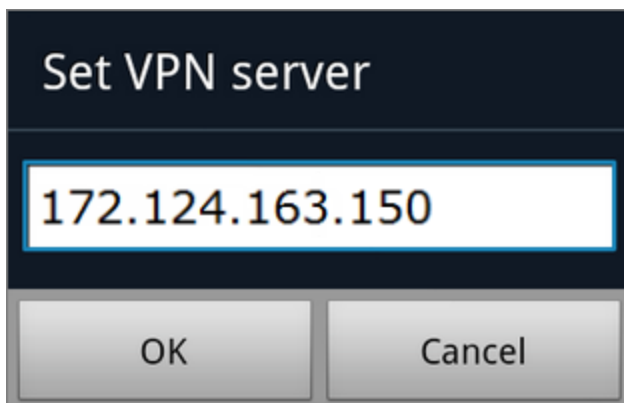
To configure L2TP VPN on an Android device, go to **Menu > Settings > Wireless & Networks > VPN settings > Add VPN > Add L2TP/IPSec PSK VPN** and configure as follows.

VPN name is for the user to identify the VPN configuration.



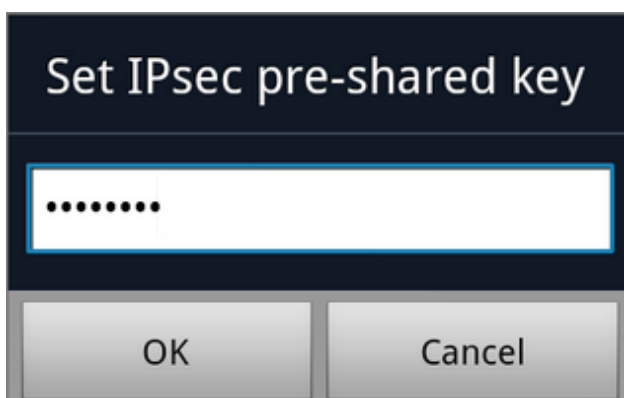
A dialog box titled "VPN name" with a dark blue header. Below the header is a text input field containing "ZyXEL_L2TP". At the bottom are two buttons: "OK" and "Cancel".

Set **VPN server** to the ZyWALL/USG's WAN IP address.



A dialog box titled "Set VPN server" with a dark blue header. Below the header is a text input field containing the IP address "172.124.163.150". At the bottom are two buttons: "OK" and "Cancel".

Set **IPSec pre-shared key** to the pre-shared key of the IPSec VPN gateway the ZyWALL/USG uses for L2TP VPN over IPSec (zyx12345 in this example).



A dialog box titled "Set IPsec pre-shared key" with a dark blue header. Below the header is a text input field containing seven dots ".....". At the bottom are two buttons: "OK" and "Cancel".

Leave **Enable L2TP secret disabled** as default and turn on **DNS search domains** if you need to use the internal DNS servers once your connection is made, enter the DNS server address here. Click **Save**.

Add L2TP/IPSec PSK VPN

VPN name
ZyXEL_L2TP

Set VPN server
172.124.163.150

Set IPsec pre-shared key
IPsec pre-shared key is set

Enable L2TP secret
L2TP secret disabled

Set L2TP secret
L2TP secret not set

DNS search domains
DNS search domains not set

Save **Cancel**

Click the VPN rule **ZyXEL_L2TP** to begin the VPN connection.

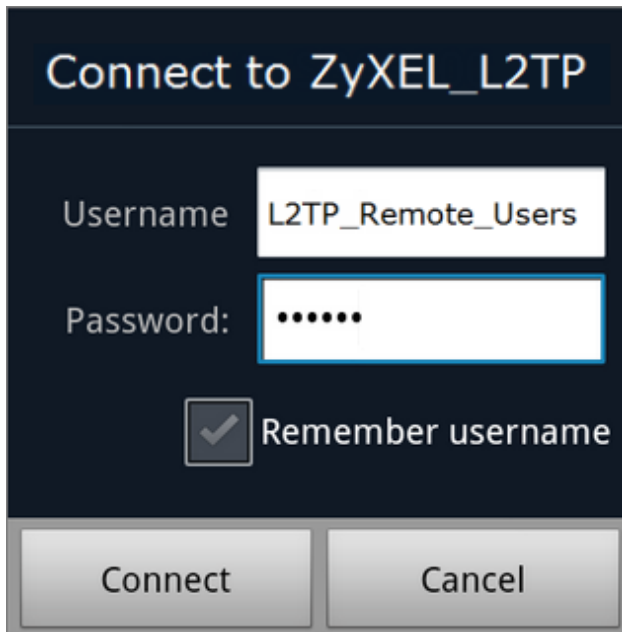
VPN settings

Add VPN

VPNs

ZyXEL_L2TP
Connect to network

When dialing the L2TP VPN, the user will have to enter Username/Password. They are the same as **Allowed User** created in ZyWALL/USG (L2TP_Remote_Users/zyx168 in this example).



Connect to ZyXEL_L2TP

Username: L2TP_Remote_Users

Password:

☒ Remember username

Connect Cancel

Test the L2TP over IPSec VPN Tunnel

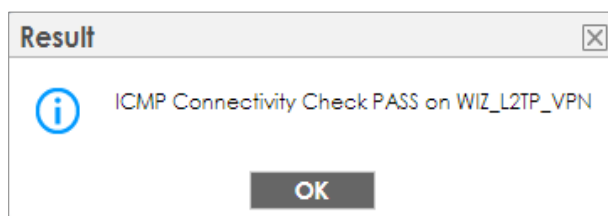
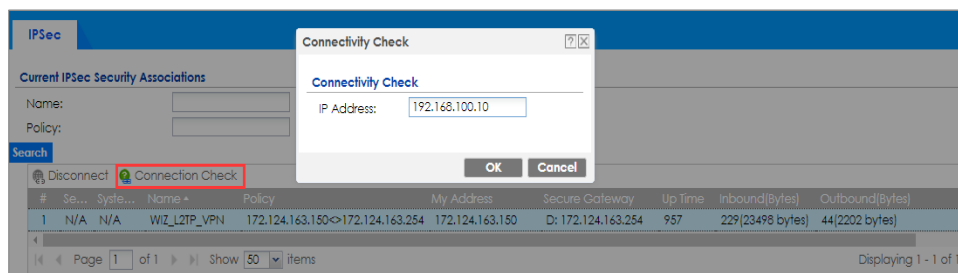
Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, the **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

| IPv4 Configuration | | | | |
|--|---|--------------|--------------|-------------------------------------|
| Add Edit Remove Activate Inactivate Connect Disconnect Object References | | | | |
| # | Status | Name | VPN Gateway | Policy |
| 1 |  | WIZ_L2TP_VPN | WIZ_L2TP_VPN | WIZ_L2TP_VPN_LOCAL/ |

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic. Click **Connectivity Check** to verify the result of ICMP Connectivity.

Hub_HQ > MONITOR > VPN Monitor > WIZ_L2TP_VPN



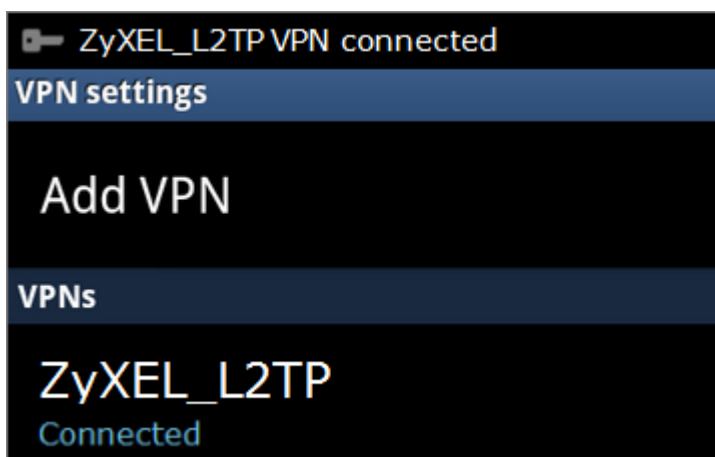
Go to ZyWALL/USG **MONITOR > VPN Monitor > L2TP over IPSec** and verify the **Current L2TP Session**.

MONITOR > VPN Monitor > L2TP over IPSec > L2TP_Remote_Users

| Current L2TP Session | | | | |
|---|-------------------|----------|---------------|-----------------|
| <div> Disconnect Refresh </div> | | | | |
| # | User Name | Hostname | Assigned IP | Public IP |
| 1 | L2TP_Remote_Users | Android | 192.168.10.10 | 172.124.163.254 |

Go to Android mobile device **Menu > Settings > Wireless & Networks > VPN** and verify the connection status.

Menu > Settings > Wireless & Networks > VPN



What Could Go Wrong?

If you see [alert] log message such as below, please check ZyWALL/USG L2TP **Allowed User** or **User/Group Settings**. Android Mobile users must use the same Username and Password as configured in ZyWALL/USG to establish the L2TP VPN.

| Priority | Category | Message | Note |
|----------|-----------------|---|----------|
| alert | L2TP Over IPSec | User L2TP_Remote_Users has been denied from L2TP service.(Incorrect Username or Password) | L2TP_LOG |

If you see [info] or [error] log message such as below, please check ZyWALL/USG Phase 1 Settings. Android Mobile users must use the same **Secret** as configured in ZyWALL/USG to establish the IKE SA.

| Priority | Category | Message | Note |
|----------|----------|--|---------|
| info | IKE | Send:[NOTIFY:INVALID_PAYLOAD_TYPE] | IKE_LOG |
| info | IKE | Invalid payload type in encrypted payload chain, possibly because of different pre-shared keys | IKE_LOG |

If you see that Phase 1 IKE SA process has completed but still get [info] log message as below, please check ZyWALL/USG Phase 2 Settings. ZyWALL/USG unit must set correct **Local Policy** to establish the IKE SA.

| Priority | Category | Message | Note |
|----------|----------|--|---------|
| info | IKE | ISAKMP SA [WIZ_L2TP_VPN] is disconnected | IKE_LOG |
| info | IKE | Received delete notification | IKE_LOG |
| info | IKE | Recv:[HASH][DEL] | IKE_LOG |
| info | IKE | Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN] | IKE_LOG |
| info | IKE | [SA] : No proposal chosen | IKE_LOG |
| info | IKE | [ID] : Tunnel [WIZ_L2TP_VPN] Phase 2 Local policy mismatch | IKE_LOG |

Ensure that the L2TP Address Pool does not conflict with any existing LAN1, LAN2, DMZ, or WLAN zones, even if they are not in use.

If you cannot access devices in the local network, verify that the devices in the local network set the USG's IP as their default gateway to utilize the L2TP tunnel.

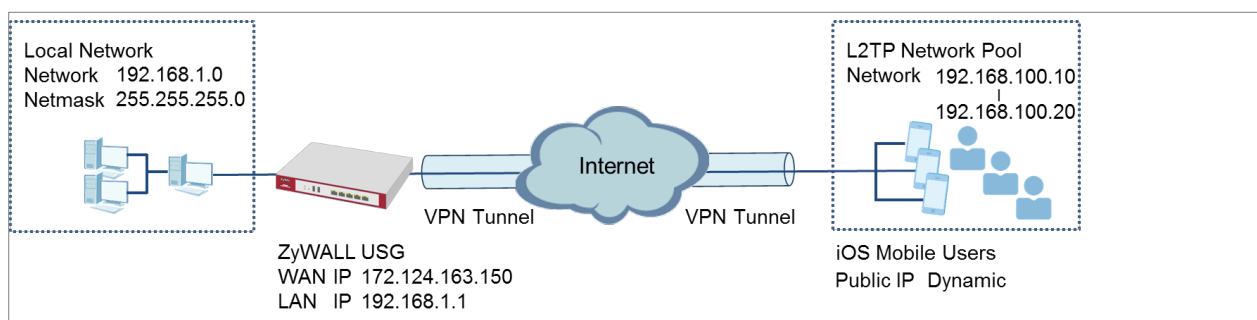
Make sure the ZyWALL/USG units' security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.


Verify that the **Zone** is set correctly in the **Zone** object. This should be set to IPSec_VPN Zone so that security policies are applied properly.

How to Configure L2TP VPN with iOS 8.4 Mobile Devices

This example shows how to use the VPN Setup Wizard to create a L2TP VPN between a ZyWALL/USG and an iOS 8.4 Mobile Device. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely and allow traffic from L2TP clients to go to the Internet.

ZyWALL/USG L2TP VPN with iOS Mobile Devices Example



 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: 4.25) and iOS (Firmware Version: 8.4).

Set Up the L2TP VPN Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings for L2TP VPN Settings** wizard to create a **L2TP VPN** rule that can be used with the remote iOS Mobile Devices. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Welcome

☐ VPN Settings

- Wizard Type
- VPN Settings
- Wizard Completed

☐ VPN Settings for Configuration Provisioning

- Wizard Type
- VPN Settings
- Wizard Completed

☒ VPN Settings for L2TP VPN Settings

- VPN Settings
- General Settings
- Wizard Completed

Then, configure the **Rule Name** and set **My Address** to be the **wan1** interface which is connected to the Internet. Type a secure **Pre-Shared Key** (8-32 characters).

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings

VPN Setup Wizard

VPN Settings > General Settings > Wizard Completed

1 2 3

L2TP VPN Settings

Rule Name: WIZ_L2TP_VPN

Phase 1 Setting

My Address (interface): wan1

Authentication Method

Pre-Shared Key: xyz12345

Assign the remote users IP addresses range from 192.168.100.10 to 192.168.100.20 for use in the L2TP VPN tunnel and check **Allow L2TP traffic Through WAN** to allow traffic from L2TP clients to go to the Internet. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (L2TP VPN Settings)

VPN Setup Wizard

VPN Settings > General Settings > Wizard Completed

1 2 3

L2TP VPN Settings

IP Address Pool: RANGE ⓘ

Starting IP Address: 192.168.100.10

End IP Address: 192.168.100.20

First DNS Server (Optional):

Second DNS Server (Optional):

☒ Allow L2TP traffic Through WAN

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (Summary)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Express Settings

Summary

Rule Name: WIZ_L2TP_VPN

Secure Gateway: Any

Pre-Shared Key: xyz12345

My Address (interface): wan1

IP Address Pool: RANGE, 192.168.10.10 - 192.168.10.20

Now the rule is configured on the ZyWALL/USG. The rule settings appear in the **VPN > L2TP VPN** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings > Summary > Wizard Completed

VPN Setup Wizard

Wizard Type >

VPN Settings >

Wizard Completed

1

2

3

L2TP VPN Settings

Congratulations. The VPN Access wizard is completed
 Summary

| | |
|-------------------------|--|
| Rule Name: | WIZ_L2TP_VPN |
| My Address (interface): | wan1 |
| Pre-Shared Key: | xyz12345 |
| IP Address Pool: | RANGE, 192.168.100.10 - 192.168.100.20 |

Go to **CONFIGURATION > VPN > L2TP VPN > Create new Object > User** to add **User Name** and **Password** (4-24 characters). Then, set **Allowed User** to the newly created object (L2TP_Remote_Users/zyx168 in this example).

CONFIGURATION > VPN > L2TP VPN > Create new Object > User

L2TP VPN

Show Advanced Settings Create new Object ▼

User

Config Walkthrough Address Reshooting

General Settings

☒ Enable L2TP Over IPSec

VPN Connection: WIZ_L2TP_VPN ▼

IP Address Pool: WIZ_L2TP_VPN_IP_A ▼ RANGE, 192.168.100.10-192.168.100.20 ⓘ

Authentication Method: default ▼ local

☐ Advance

Allowed User: any ▼

Keep Alive Timer: 60 (1-180 seconds)

First DNS Server (Optional): Custom Defined ▼

Second DNS Server (Optional): Custom Defined ▼

First WINS Server (Optional):

Second WINS Server (Optional):

User Configuration

User Name : L2TP_Remote_Users

User Type: User ▼

Password:

Retype:

Description: Local User

Authentication Timeout Settings

☒ Use Default Settings ☐ Use Manual Settings

Lease Time: 1440 minutes

Reauthentication Time: 1440 minutes

OK Cancel

If some of the traffic from the L2TP clients need to go to the Internet, create a policy route to send traffic from the L2TP tunnels out through a WAN trunk. Set **Incoming** to **Tunnel** and select your L2TP VPN connection. Set the **Source Address** to be the L2TP address pool. Set the **Next-Hop Type** to **Trunk** and select the appropriate WAN trunk.

CONFIGURATION > Network > Routing > Policy Route

Edit Policy Route

Show Advanced Settings
Create new Object ▼

Configuration

☒ Enable

Description:
L2TP_VPN_to_Internet (Optional)

Criteria

User:
L2TP_Remote_User ▼

Incoming:
Tunnel ▼

Please select one member:
WIZ_L2TP_VPN ▼

Source Address:
WIZ_L2TP_VPN_IP_4 ▼

Destination Address:
any ▼

DSCP Code:
any ▼

Schedule:
none ▼

Service:
any ▼

Next-Hop

Type:
Trunk ▼

Trunk:
SYSTEM_DEFAULT_V ▼

OK Cancel

Set Up the L2TP VPN Tunnel on the iOS Device

To configure L2TP VPN in an iOS 8.4 device, go to **Menu > Settings > VPN > Add VPN Configuration** and configure as follows.

Description is for you to identify the VPN configuration.

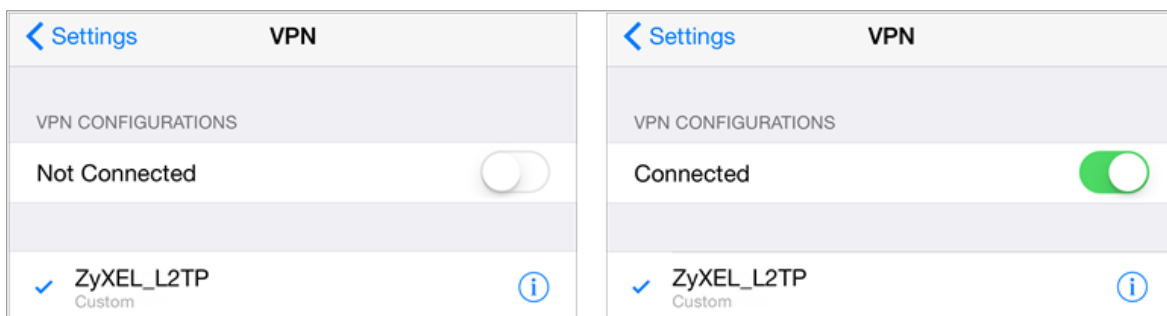
Set **Server** to the ZyWALL/USG's WAN IP address (172.124.163.150 in this example).

Enter **Account** and **Password** which the same as **Allowed User** created in ZyWALL/USG (L2TP_Remote_Users/zyx168 in this example).

Set **Secret** to the **Pre-Shared Key** of the IPsec VPN gateway the ZyWALL/USG uses for L2TP VPN over IPsec (zyx12345 in this example).

| < VPN ZyXEL_L2TP | |
|--|-------------------------------------|
| Type | L2TP |
| Description | ZyXEL_L2TP |
| Server | 172.124.163.150 |
| Account | L2TP_Remote_Users |
| RSA SecurID | <input type="checkbox"/> |
| Password | ••••• |
| Secret | ••••••• |
| Send All Traffic | <input checked="" type="checkbox"/> |


After you create a VPN configuration, slide the button right to the on position to initiate L2TP VPN session.



Test the L2TP over IPSec VPN Tunnel

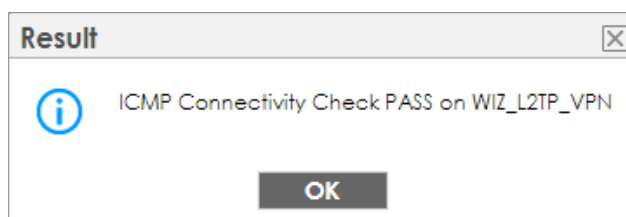
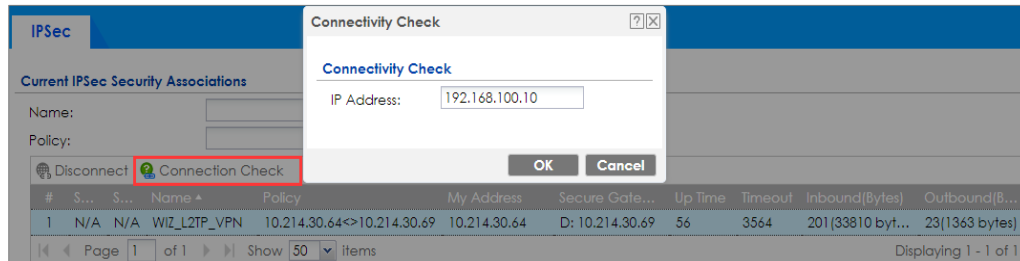
Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, the **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

| IPv4 Configuration | | | | |
|--|---|--------------|--------------|-------------------------------------|
| Add Edit Remove Activate Inactivate Connect Disconnect Object References | | | | |
| # | Status | Name | VPN Gateway | Policy |
| 1 |  | WIZ_L2TP_VPN | WIZ_L2TP_VPN | WIZ_L2TP_VPN_LOCAL/ |

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic. Click **Connectivity Check** to verify the result of ICMP Connectivity.

Hub_HQ > MONITOR > VPN Monitor > IPSec > WIZ_L2TP_VPN



Go to ZyWALL/USG **MONITOR > VPN Monitor > L2TP over IPSec** and verify the **Current L2TP Session**.

MONITOR > VPN Monitor > L2TP over IPSec > L2TP_Remote_Users

| Current L2TP Session | | | | |
|---------------------------------|-------------------|----------|----------------|--------------|
| <div> Disconnect Refresh </div> | | | | |
| # | User Name | Hostname | Assigned IP | Public IP |
| 1 | L2TP_Remote_Users | IPhone | 192.168.100.10 | 10.214.30.69 |

Go to iOS mobile device **Menu > Settings > VPN > ZyXEL_L2TP** and verify the **Assigned IP Address** and **Connect Time**.

Menu > Settings > VPN > ZyXEL_L2TP

| ZyXEL_L2TP | |
|------------------------|-------------------------------------|
| Type | L2TP |
| Server | 172.124.163.150 |
| Assigned IP Address | 192.168.100.10 |
| Connect Time | 0:06 |
| Description ZyXEL_L2TP | |
| Server | 172.124.163.150 |
| Account | L2TP_Remote_Users |
| RSA SecurID | <input type="checkbox"/> |
| Password | •••••• |
| Secret | •••••••• |
| Send All Traffic | <input checked="" type="checkbox"/> |

What Could Go Wrong?

If you see [alert] log message such as below, please check ZyWALL/USG L2TP

Allowed User or **User/Group Settings**. iOS Mobile users must use the same Username and Password as configured in ZyWALL/USG to establish the L2TP VPN.

| Priority | Category | Message | Note |
|----------|-----------------|---|----------|
| alert | L2TP Over IPSec | User L2TP_Remote_Users has been denied from L2TP service.(Incorrect Username or Password) | L2TP_LOG |

If you see [info] or [error] log message such as below, please check ZyWALL/USG Phase 1 Settings. iOS Mobile users must use the same **Secret** as configured in ZyWALL/USG to establish the IKE SA.

| Priority | Category | Message | Note |
|----------|----------|--|---------|
| info | IKE | Send:[NOTIFY:INVALID_PAYLOAD_TYPE] | IKE_LOG |
| info | IKE | Invalid payload type in encrypted payload chain, possibly because of different pre-shared keys | IKE_LOG |

If you see that Phase 1 IKE SA process has completed but still get [info] log message as below, please check ZyWALL/USG Phase 2 Settings. ZyWALL/USG unit must set correct **Local Policy** to establish the IKE SA.

| Priority | Category | Message | Note |
|----------|----------|--|---------|
| info | IKE | ISAKMP SA [WIZ_L2TP_VPN] is disconnected | IKE_LOG |
| info | IKE | Received delete notification | IKE_LOG |
| info | IKE | Recv:[HASH][DEL] | IKE_LOG |
| info | IKE | Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN] | IKE_LOG |
| info | IKE | [SA] : No proposal chosen | IKE_LOG |
| info | IKE | [ID] : Tunnel [WIZ_L2TP_VPN] Phase 2 Local policy mismatch | IKE_LOG |

Ensure that the L2TP Address Pool does not conflict with any existing LAN1, LAN2, DMZ, or WLAN zones, even if they are not in use.

If you cannot access devices in the local network, verify that the devices in the local network set the USG's IP as their default gateway to utilize the L2TP tunnel.

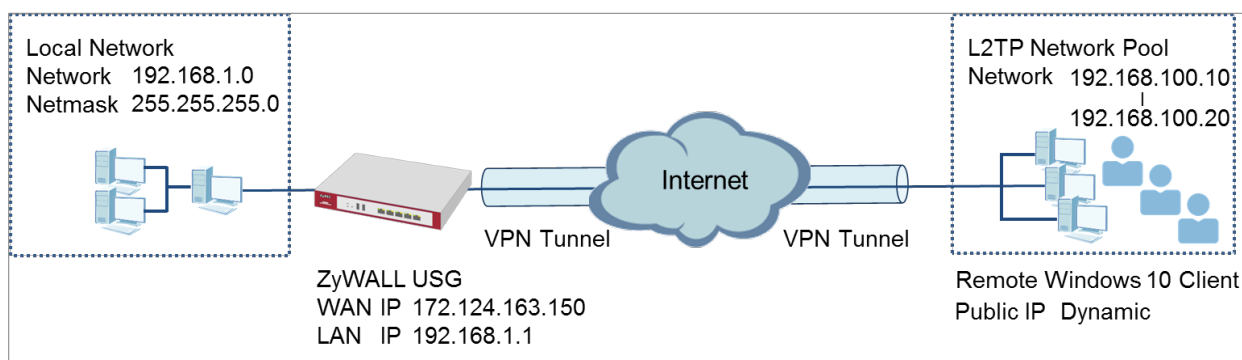
Make sure the ZyWALL/USG units' security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.


Verify that the **Zone** is set correctly in the **Zone** object. This should be set to IPSec_VPN Zone so that security policies are applied properly.

How to Import ZyWALL/USG Certificate for L2TP over IPsec in Windows 10

This is an example of using the L2TP VPN and VPN client software included in Windows 10 operating systems. When the VPN tunnel is configured, users can securely access the network behind the ZyWALL/USG and allow traffic from L2TP clients to go to the Internet from a Windows 10 computer.

ZyWALL/USG L2TP VPN with Remote Windows 10 Client Example



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: 4.25) and Windows 10 Pro (Version: 10.0.10240)

Set Up the L2TP VPN Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings for L2TP VPN Settings** wizard to create a **L2TP VPN** rule that can be used with the Windows 10 clients. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Welcome

- ☐ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☒ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

Then, configure the **Rule Name** and set **My Address** to be the **wan1** interface which is connected to the Internet. Type a secure **Pre-Shared Key** (8-32 characters).

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings

VPN Setup Wizard

VPN Settings > General Settings > Wizard Completed

123

L2TP VPN Settings

Rule Name:
WIZ_L2TP_VPN

Phase 1 Setting

My Address (interface):
wan1

Authentication Method

Pre-Shared Key:
xyz12345

Assign the L2TP users' IP address range from 192.168.100.10 to 192.168.100.20 for use in the L2TP VPN tunnel and select **Allow L2TP traffic Through WAN** to allow traffic from L2TP clients to go to the Internet. Click **OK**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (L2TP VPN Settings)

VPN Setup Wizard

VPN Settings > General Settings > Wizard Completed

123

L2TP VPN Settings

IP Address Pool: RANGE ⓘ

Starting IP Address: 192.168.100.10

End IP Address: 192.168.100.20

First DNS Server (Optional):

Second DNS Server (Optional):

☒ Allow L2TP traffic Through WAN

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (Summary)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Summary

Rule Name: WIZ_L2TP_VPN

Secure Gateway: Any

Pre-Shared Key: xyz12345

My Address (interface): wan1

IP Address Pool: RANGE, 192.168.10.10 - 192.168.10.20

Now the rule is configured on the ZyWALL/USG. The rule settings appear in the **VPN > L2TP VPN** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings > Wizard Completed

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

Summary

| | |
|-------------------------|--------------------------------------|
| Rule Name: | WIZ_L2TP_VPN |
| Secure Gateway: | Any |
| Pre-Shared Key: | xyz12345 |
| My Address (interface): | wan1 |
| IP Address Pool: | RANGE, 192.168.10.10 - 192.168.10.20 |

Go to **CONFIGURATION > VPN > VPN Gateway > WIZ_L2TP_VPN**, change **Authentication** method to be **Certificate** and select the certificate which ZyWALL/USG uses to identify itself to the Window 10 computer.

CONFIGURATION > VPN > VPN Gateway > WIZ_L2TP_VPN > Authentication > Certificate

Authentication

☐ Pre-Shared Key

☐ unmasked

☒ Certificate default (See [My Certificates](#))

☐ User Based PSK admin ⓘ

Go to **CONFIGURATION > VPN > L2TP VPN > Create new Object > User** to add **User Name** and **Password** (4-24 characters). Then, set **Allowed User** to the newly created object (L2TP_Remote_Users/zyx168 in this example).

CONFIGURATION > VPN > L2TP VPN > Create new Object > User

The screenshot displays the ZyXEL L2TP VPN configuration interface. At the top, the 'L2TP VPN' tab is active. Below it, the 'Create new Object' dropdown menu is open, showing 'User' as the selected option. The 'General Settings' section is visible, with 'Enable L2TP Over IPSec' checked. The 'VPN Connection' is set to 'WIZ_L2TP_VPN', the 'IP Address Pool' is 'WIZ_L2TP_VPN_IP_1', and the 'Authentication Method' is 'default'. The 'Advance' section is expanded, showing 'Allowed User' as 'any', 'Keep Alive Timer' as '60' seconds, and optional DNS and WINS servers. Below this, the 'User Configuration' dialog box is open, showing 'User Name' as 'L2TP_Remote_Users', 'User Type' as 'User', and 'Password' and 'Retype' fields with masked characters. The 'Description' is 'Local User', and 'Authentication Timeout Settings' are set to 'Use Default Settings' with a 'Lease Time' of '1440' minutes and a 'Reauthentication Time' of '1440' minutes. The 'OK' button is highlighted.

If some of the traffic from the L2TP clients need to go to the Internet, create a policy route to send traffic from the L2TP tunnels out through a WAN trunk. Set **Incoming** to **Tunnel** and select your L2TP VPN connection. Set the **Source Address** to be the L2TP address pool. Set the **Next-Hop Type** to **Trunk** and select the appropriate WAN trunk.

CONFIGURATION > Network > Routing > Policy Route

Edit Policy Route

Show Advanced Settings
Create new Object ▼

Configuration

☒ Enable

Description: L2TP_VPN_to_Internet (Optional)

Criteria

User: L2TP_Remote_User ▼

Incoming: Tunnel ▼

Please select one member: WIZ_L2TP_VPN ▼

Source Address: WIZ_L2TP_VPN_IP_4 ▼

Destination Address: any ▼

DSCP Code: any ▼

Schedule: none ▼

Service: any ▼

Next-Hop

Type: Trunk ▼

Trunk: SYSTEM_DEFAULT_V ▼

OK Cancel

Export a Certificate from ZyWALL/USG and Import it to Windows 10 Operating System

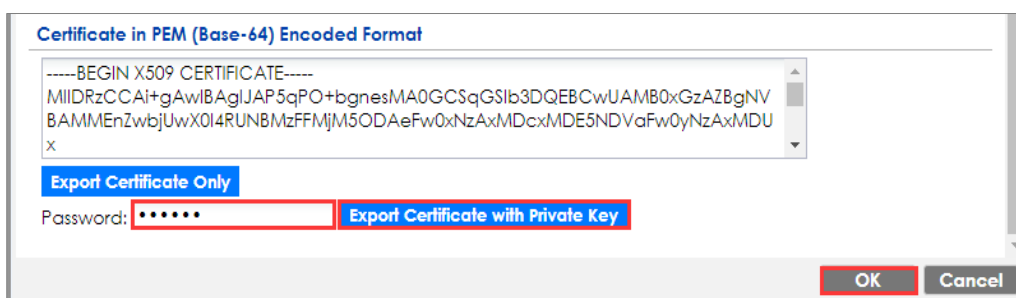
Go to ZyWALL/USG **CONFIGURATION > Object > Certificate**, select the certificate (default in this example) and click **Edit**.

CONFIGURATION > Object > Certificate > default

| My Certificates Setting | | | | | | |
|-----------------------------------|---------|------|-----------------------|-----------------------|-------------------------|-------------------------|
| Add Edit Remove Object References | | | | | | |
| # | Name ▲ | Type | Subject | Issuer | Valid From | Valid To |
| 1 | default | SELF | CN=vpn50_b8ECA31E2398 | CN=vpn50_b8ECA31E2398 | 2017-01-07 10:19:45 GMT | 2027-01-05 10:19:45 GMT |

Export default certificate from ZyWALL/USG with Private Key (zyx123 in this example)

CONFIGURATION > Object > Certificate > default > Edit > Export Certificate with Private Key



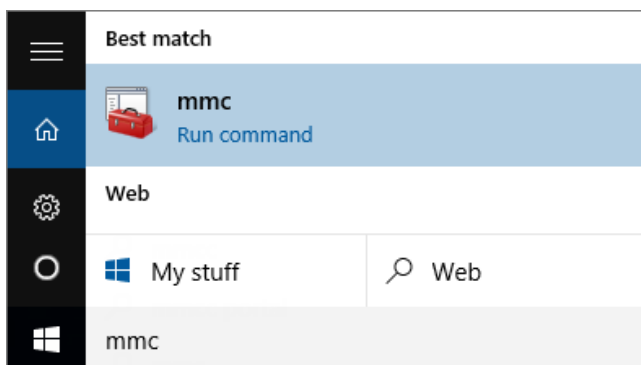
Save **default** certificate as *.p12 file to Windows 10 computer.



default.p12

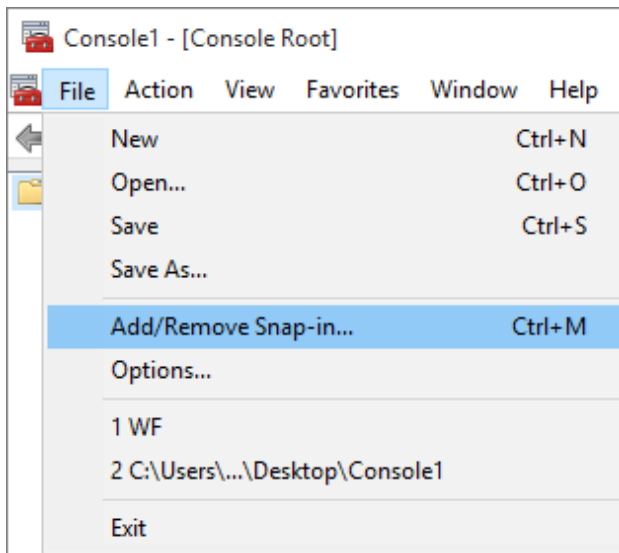
In Windows 10 Operating System, go to **Start Menu > Search Box**. Type **mmc** and press **Enter**.

Start Menu > Search Box > mmc



In the mmc console window, click **File > Add/Remove Snap-in...**

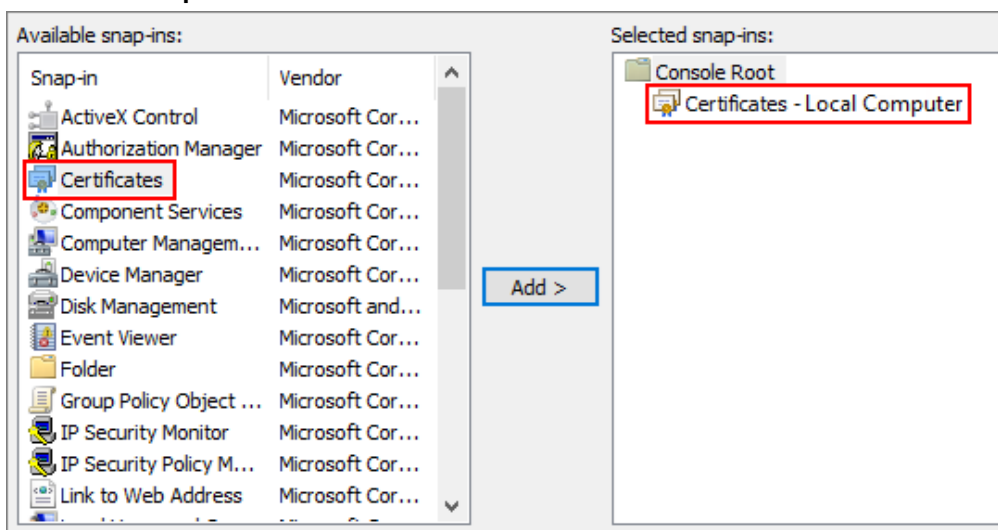
File > Add/Remove Snap-in...



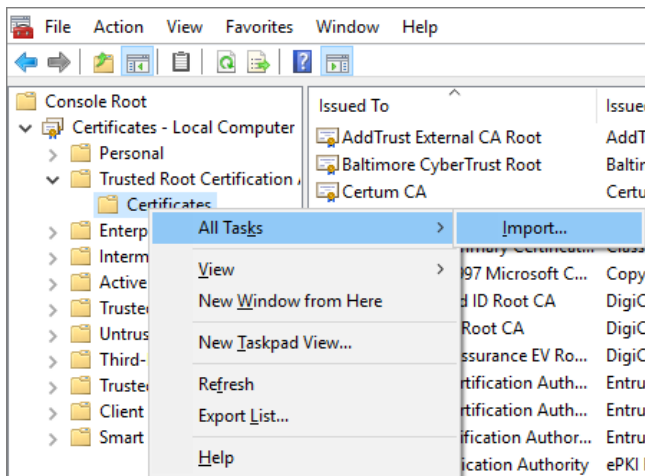
In the **Available snap-ins**, select **Certificates** click **Add**. Then, click **Finished**.

Press **OK** to close the Snap-ins window.

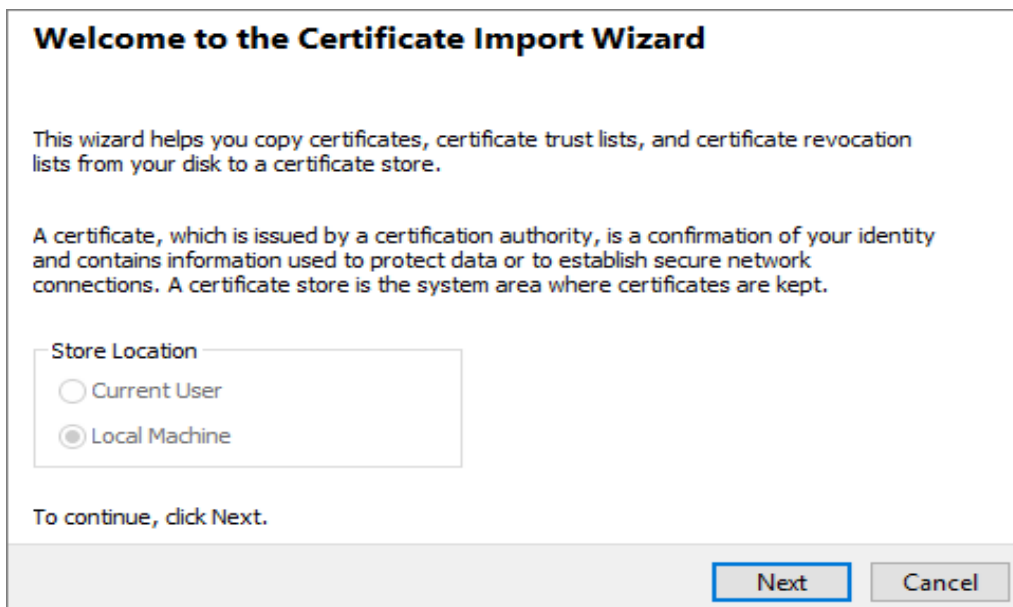
Available snap-ins > Certificates > Add



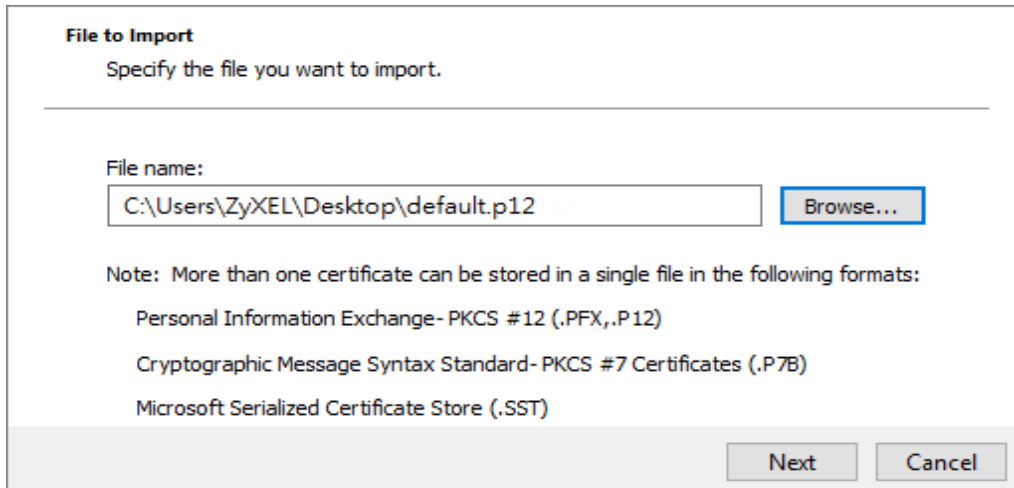
In the mmc console window, go to **Certificates (Local Computer) > Trusted Root Certification Authorities**, right click **Certificate > All Tasks > Import...**



Click **Next**.



Click **Browse...**, and locate the .p12 file you downloaded earlier. Then, click **Next**.



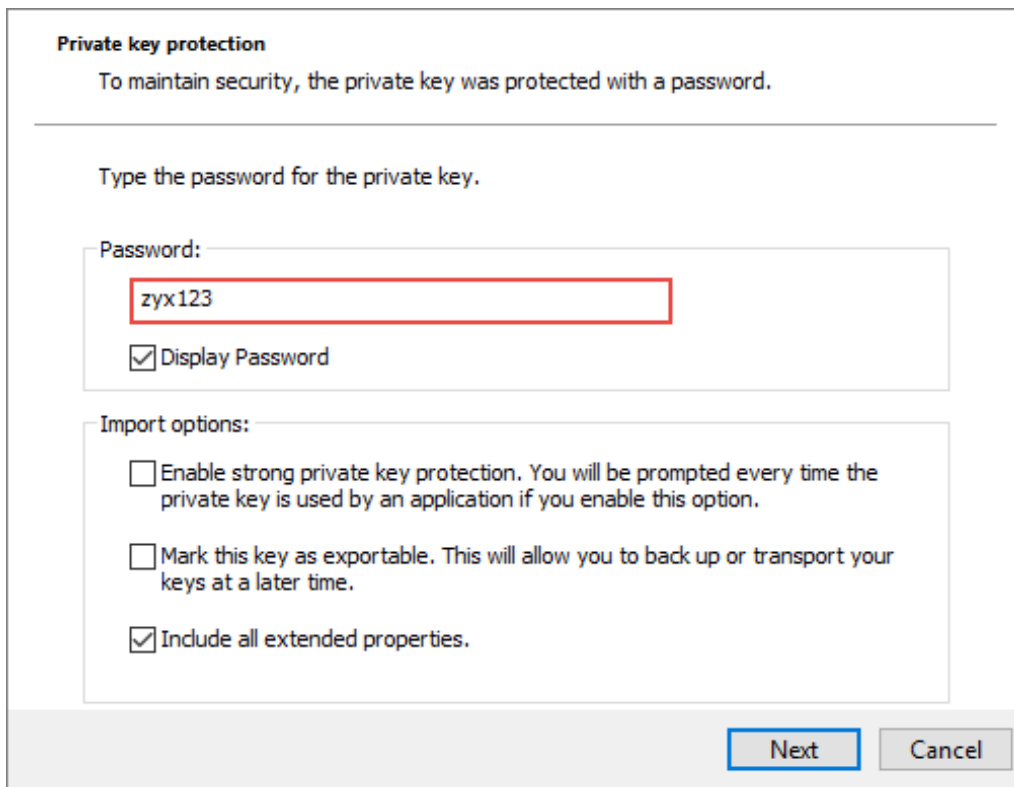
File to Import
Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

- Personal Information Exchange- PKCS #12 (.PFX,.P12)
- Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
- Microsoft Serialized Certificate Store (.SST)

Type **zyx123** in the **Password** field and click **Next**.



Private key protection
To maintain security, the private key was protected with a password.

Type the password for the private key.

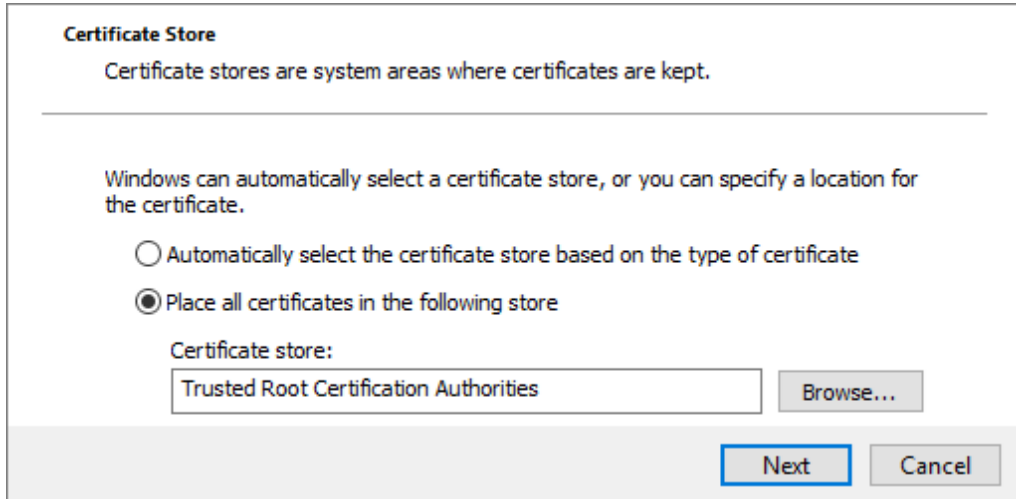
Password:

☒ Display Password


Import options:

- ☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
- ☐ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
- ☒ Include all extended properties.

Select **Place all certificates in the following store** and then click **Browse** and find **Trusted Root Certification Authorities**. Click **Next**, then click **Finish**.



The image shows a Windows 'Certificate Store' dialog box. At the top, it says 'Certificate Store' and 'Certificate stores are system areas where certificates are kept.' Below this, it states 'Windows can automatically select a certificate store, or you can specify a location for the certificate.' There are two radio button options: 'Automatically select the certificate store based on the type of certificate' (which is unselected) and 'Place all certificates in the following store' (which is selected). Under the selected option, there is a text box labeled 'Certificate store:' containing the text 'Trusted Root Certification Authorities'. To the right of the text box is a 'Browse...' button. At the bottom right of the dialog are 'Next' and 'Cancel' buttons. The 'Next' button is highlighted with a blue border.

 Note: Each ZyWALL/USG device has its own self-signed certificate by factory default. When you reset to default configuration file, the original self-signed certificate is erased, and a new self-signed certificate will be created when the ZyWALL/USG boots the next time.

Set Up the L2TP VPN Tunnel on the Windows 10

To configure L2TP VPN in Windows 10 operating system, go to **Start > Settings > Network & Internet > VPN > Add a VPN Connection** and configure as follows.

VPN Provider set to **Windows (built-in)**.

Configure **Connection name** for you to identify the VPN configuration.

Set **Server** name or address to be the ZyWALL/USG's WAN IP address (172.124.163.150 in this example).

Select **VPN type** to **Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)**.

Enter **User name** and **Password** which the same as **Allowed User** created in ZyWALL/USG (L2TP_Remote_Users/zyx168 in this example).

Add a VPN connection

VPN provider

Windows (built-in) ▾

Connection name

ZyXEL_L2TP_VPN

Server name or address

172.124.163.150

VPN type

Layer 2 Tunneling Protocol with IPsec (L2TP/I ▾

Type of sign-in info

User name and password ▾

User name (optional)

L2TP_Remote_Users

Password (optional)

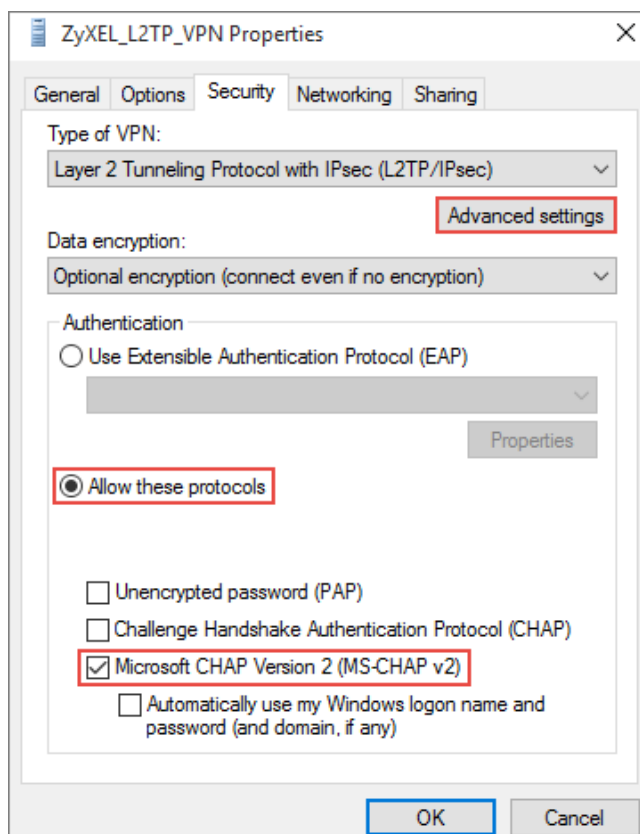
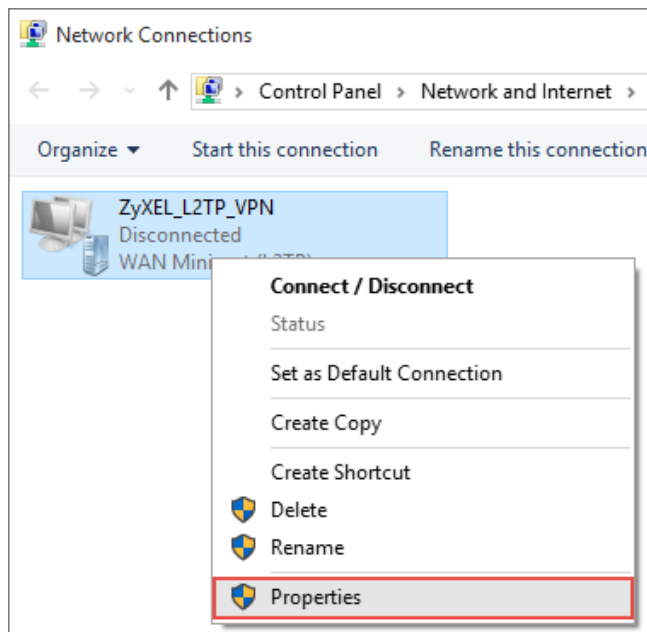
•••••

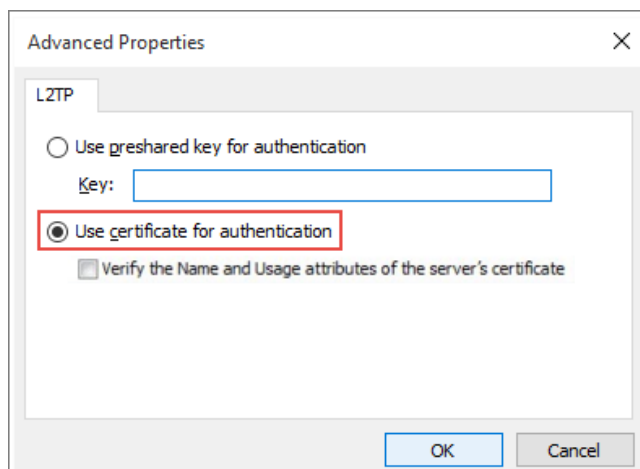
☒ Remember my sign-in info

Save

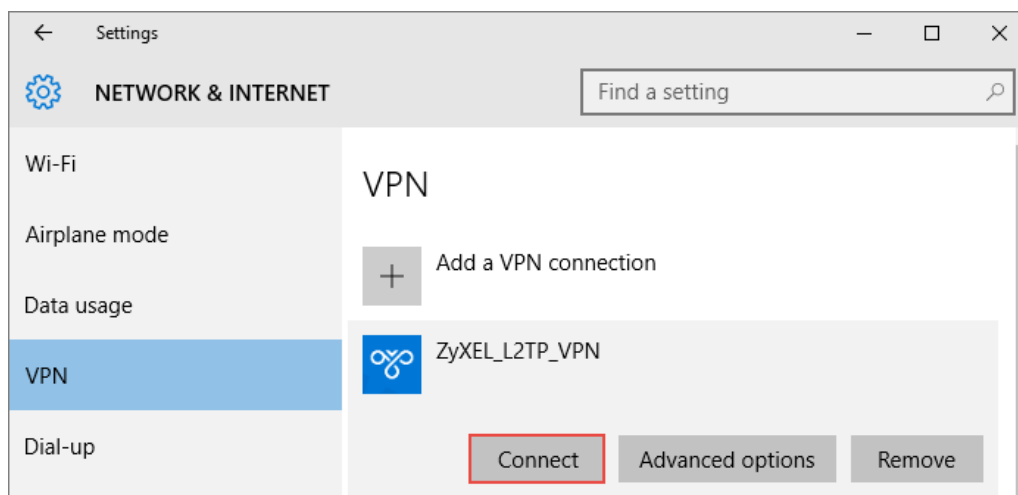
Cancel

Go to **Control Panel > Network and Internet > Network Connections** and right click **Properties**. Continue to **Security > Advanced settings** and select **Use Certificate for authentication**.





Go to **Network & Internet Settings** window, click **Connect**.



Test the L2TP over IPSec VPN Tunnel

Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, the **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

| IPv4 Configuration | | | | |
|--|---|--------------|--------------|-------------------------------------|
| Add Edit Remove Activate Inactivate Connect Disconnect Object References | | | | |
| # | Status | Name | VPN Gateway | Policy |
| 1 |  | WIZ_L2TP_VPN | WIZ_L2TP_VPN | WIZ_L2TP_VPN_LOCAL/ |

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic. Click **Connectivity Check** to verify the result of ICMP Connectivity.

Hub_HQ > MONITOR > VPN Monitor > IPSec > WIZ_L2TP_VPN

IPSec

Current IPSec Security Associations

Name:

Policy:

Disconnect

Connectivity Check

| # | S... | S... | Name | Policy | My Address | Secure Gate... | Up time | Timeout | Inbound(Bytes) | Outbound(B... |
|---|------|------|--------------|----------------------------|--------------|-----------------|---------|---------|------------------|----------------|
| 1 | N/A | N/A | WIZ_L2TP_VPN | 10.214.30.64<>10.214.30.69 | 10.214.30.64 | D: 10.214.30.69 | 56 | 3564 | 201(33810 byt... | 23(1363 bytes) |

Page 1 of 1

Show 50 Items

Displaying 1 - 1 of 1


Connectivity Check

Connectivity Check

IP Address: 192.168.100.10

OK Cancel

Result



ICMP Connectivity Check PASS on WIZ_L2TP_VPN

OK

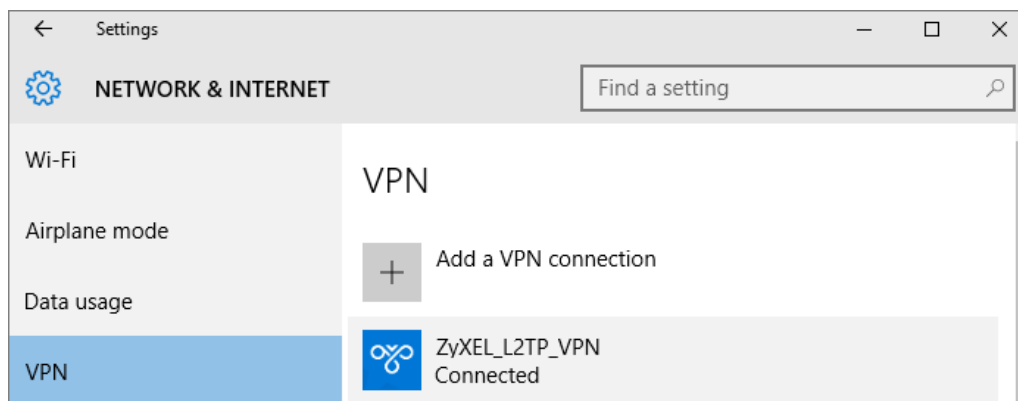
Go to ZyWALL/USG **MONITOR > VPN Monitor > L2TP over IPSec** and verify the **Current L2TP Session**.

MONITOR > VPN Monitor > L2TP over IPSec > L2TP_Remote_Users

| Current L2TP Session | | | | |
|---|-------------------|----------|----------------|--------------|
| Disconnect Refresh | | | | |
| # | User Name | Hostname | Assigned IP | Public IP |
| 1 | L2TP_Remote_Users | ellen-PC | 192.168.100.10 | 10.214.30.69 |
| Page 1 of 1 Show 50 items Displaying 1 - 1 of 1 | | | | |

Go to Window 10 operating system **Start > Settings > Network & Internet > VPN** and show **Connected** status.

Menu > Settings > VPN > ZyXEL_L2TP



What Could Go Wrong?

If you see [alert] log message such as below, please check ZyWALL/USG L2TP Allowed User or User/Group Settings. Windows 10 users must use the same Username and Password as configured in ZyWALL/USG to establish the L2TP VPN.

| # | ▼ | Priority | Category | Message | Note |
|----|---|----------|-----------------|---|----------|
| 13 | | alert | L2TP Over IPSec | User L2TP_Remote_Users has been denied from L2TP service.(Incorrect Username or Password) | L2TP_LOG |

If you see [info] or [error] log message such as below, please check ZyWALL/USG Phase 1 Settings. Windows 10 operating system users must use the same Pre-Shared Key as configured in ZyWALL/USG to establish the IKE SA.

| # | ▼ | Priority | Category | Message | Note |
|----|---|----------|----------|--|---------|
| 2 | | info | IKE | ISAKMP SA [WIZ_L2TP_VPN] is disconnected | IKE_LOG |
| 3 | | info | IKE | The cookie pair is : 0xd103273f03f379a0 / 0x05efd54196dc6cd6 | IKE_LOG |
| 10 | | info | IKE | Send:[NOTIFY:INVALID_PAYLOAD_TYPE] | IKE_LOG |
| 11 | | info | IKE | Invalid payload type in encrypted payload chain, possibly because of different pre-shared keys | IKE_LOG |

If you see that Phase 1 IKE SA process has completed but still get [info] log message as below, please check ZyWALL/USG Phase 2 Settings. ZyWALL/USG unit must set correct **Local Policy** to establish the IKE SA.

| Priority | Category | Message | Note |
|----------|----------|--|---------|
| info | IKE | Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN] | IKE_LOG |
| info | IKE | [SA] : No proposal chosen | IKE_LOG |
| info | IKE | [ID] : Tunnel [WIZ_L2TP_VPN] Phase 2 Local policy mismatch | IKE_LOG |

Ensure that the L2TP Address Pool does not conflict with any existing LAN1, LAN2, DMZ, or WLAN zones, even if they are not in use.

If you cannot access devices in the local network, verify that the devices in the local network set the USG's IP as their default gateway to utilize the L2TP tunnel.

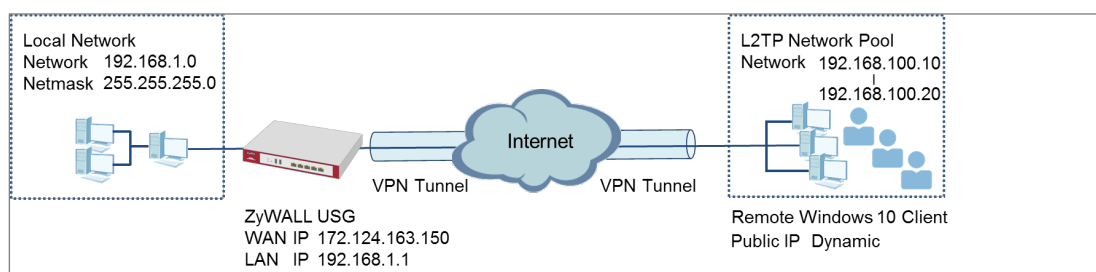
Make sure the ZyWALL/USG units' security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.


Verify that the Zone is set correctly in the VPN Connection rule. This should be set to IPSec_VPN Zone so that security policies are applied properly.

How to Import ZyWALL/USG Certificate for L2TP over IPsec in IOS mobile phone

This is an example of using the L2TP VPN and VPN client software included in Android mobile phone operating systems. When the VPN tunnel is configured, users can securely access the network behind the ZyWALL/USG and allow traffic from L2TP clients to go to the Internet from an iOS mobile phone.

ZyWALL/USG L2TP VPN with Remote iOS Mobile Phone Client Example

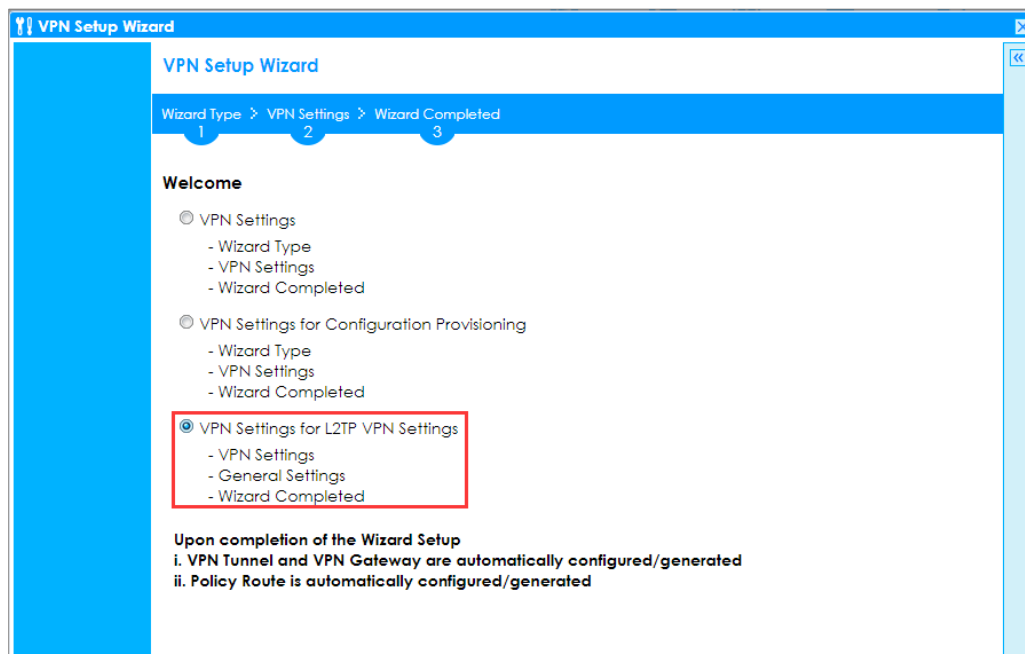


 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: 4.25) and iOS (Version: 10.0.10240)

Set Up the L2TP VPN Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings for L2TP VPN Settings** wizard to create a **L2TP VPN** rule that can be used with the iOS mobile phone clients. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



Then, configure the **Rule Name** and set **My Address** to be the **wan1** interface which is connected to the Internet. Type a secure **Pre-Shared Key** (8-32 characters).

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings

Assign the L2TP users' IP address range from 192.168.100.10 to 192.168.100.20 for use in the L2TP VPN tunnel and select **Allow L2TP traffic Through WAN** to allow traffic from L2TP clients to go to the Internet. Click **OK**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (L2TP VPN Settings)

VPN Setup Wizard

VPN Settings > General Settings > Wizard Completed

1 2 3

L2TP VPN Settings

IP Address Pool: RANGE ⓘ

Starting IP Address: 192.168.100.10

End IP Address: 192.168.100.20

First DNS Server (Optional):

Second DNS Server (Optional):

☒ Allow L2TP traffic Through WAN

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (Summary)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Express Settings

Summary

Rule Name: WIZ_L2TP_VPN

Secure Gateway: Any

Pre-Shared Key: xyz12345

My Address (interface): wan1

IP Address Pool: RANGE, 192.168.10.10 - 192.168.10.20

Now the rule is configured on the ZyWALL/USG. The rule settings appear in the **VPN > L2TP VPN** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings > Wizard Completed

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Summary

Rule Name: WIZ_L2TP_VPN

Secure Gateway: Any

Pre-Shared Key: xyz12345

My Address (interface): wan1

IP Address Pool: RANGE, 192.168.10.10 - 192.168.10.20

Go to **CONFIGURATION > VPN > VPN Gateway > WIZ_L2TP_VPN**, change **Authentication** method to be **Certificate** and select the certificate which ZyWALL/USG uses to identify itself to the Android mobile phone.

CONFIGURATION > VPN > VPN Gateway > WIZ_L2TP_VPN > Authentication > Certificate

Authentication

☐ Pre-Shared Key

☐ unmasked

☒ Certificate

☐ User Based PSK

default

(See [My Certificates](#))

admin

i

Go to **CONFIGURATION > VPN > L2TP VPN > Create new Object > User** to add **User Name** and **Password** (4-24 characters). Then, set **Allowed User** to the newly created object (L2TP_Remote_Users/zyx168 in this example).

CONFIGURATION > VPN > L2TP VPN > Create new Object > User

L2TP VPN

Show Advanced Settings Create new Object

User

Address

Reshooting

General Settings

☒ Enable L2TP Over IPSec

VPN Connection: WIZ_L2TP_VPN

IP Address Pool: WIZ_L2TP_VPN_IP_ RANGE, 192.168.100.10-192.168.100.20

Authentication Method: default local

Advance

Allowed User: any

Keep Alive Timer: 60 (1-180 seconds)

First DNS Server (Optional): Custom Defined

Second DNS Server (Optional): Custom Defined

First WINS Server (Optional):

Second WINS Server (Optional):

Add A User

User Configuration

User Name : L2TP_Remote_Users

User Type: user

Password:

Retype:

Description: Local User

Authentication Timeout Settings
 ☒ Use Default Settings
 ☐ Use Manual Settings

Lease Time: 1440 minutes

Reauthentication Time: 1440 minutes

OK

Cancel

L2TP VPN

Show Advanced Settings Create new Object

Configuration Walkthrough

Troubleshooting

General Settings

☒ Enable L2TP Over IPSec

VPN Connection: WIZ_L2TP_VPN

IP Address Pool: WIZ_L2TP_VPN_IP_ RANGE, 192.168.100.10-192.168.100.20

Authentication Method: default local

Advance

Allowed User: any

Keep Alive Timer: 60 (1-180 seconds)

First DNS Server (Optional): Custom Defined

Second DNS Server (Optional): Custom Defined

First WINS Server (Optional):

Second WINS Server (Optional):

any

any

=== Object ===

ad-users

admin

ldap-users

radius-users

ua-users

L2TP_Remote_Users

Export a Certificate from ZyWALL/USG and Import it to iOS Mobile Phone

Go to ZyWALL/USG **CONFIGURATION > Object > Certificate**, select the certificate (**default** in this example) and click **Edit**.

CONFIGURATION > Object > Certificate > default

| My Certificates Setting | | | | | | |
|---|---------|------|-----------------------|-----------------------|-------------------------|-------------------------|
| Add Edit Remove Object References | | | | | | |
| # | Name | Type | Subject | Issuer | Valid From | Valid To |
| 1 | default | SELF | CN=vpn50_B8ECA31E2398 | CN=vpn50_B8ECA31E2398 | 2017-01-07 10:19:45 GMT | 2027-01-05 10:19:45 GMT |
| Page 1 of 1 Show 50 items Displaying 1 - 1 of 1 | | | | | | |

Export default certificate from ZyWALL/USG with Private Key (zyx123 in this example)

CONFIGURATION > Object > Certificate > default > Edit > Export Certificate with Private Key

Certificate in PEM (Base-64) Encoded Format

```
-----BEGIN X509 CERTIFICATE-----
MIIDRzCCAItgAwIBAgIJAP5qPO+bgnesMA0GCSqGSIb3DQEBCwUAMB0xGzAZBgNV
BAMMEnZwbjUwX0I4RUNBMzFFMjM5ODAEFw0xNzAxMDcxMDE5NDVaFw0yNzAxMDU
x
```

Password:

Save **default** certificate as ***.p12** file to Android mobile phone computer.



default.p12

Set Up the L2TP VPN Tunnel on the iOS Mobile Device

- 1 To configure L2TP VPN in iOS operating system, go to **Start > Settings > Network & Internet > VPN > Add a VPN Connection** and configure as follows.
- 2 VPN Provider set to Windows (built-in).
- 3 Configure **Connection name** for you to identify the VPN configuration.

- 4 Set **Server** name or address to be the ZyWALL/USG's WAN IP address (172.124.163.150 in this example).
- 5 Select VPN type to Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec).
- 6 Enter **User name** and **Password** which the same as **Allowed User** created in ZyWALL/USG (L2TP_Remote_Users/zyx168 in this example).

Add a VPN connection

VPN provider
Windows (built-in) ▾

Connection name
ZyXEL_L2TP_VPN

Server name or address
172.124.163.150

VPN type
Layer 2 Tunneling Protocol with IPsec (L2TP/I ▾

Type of sign-in info
User name and password ▾

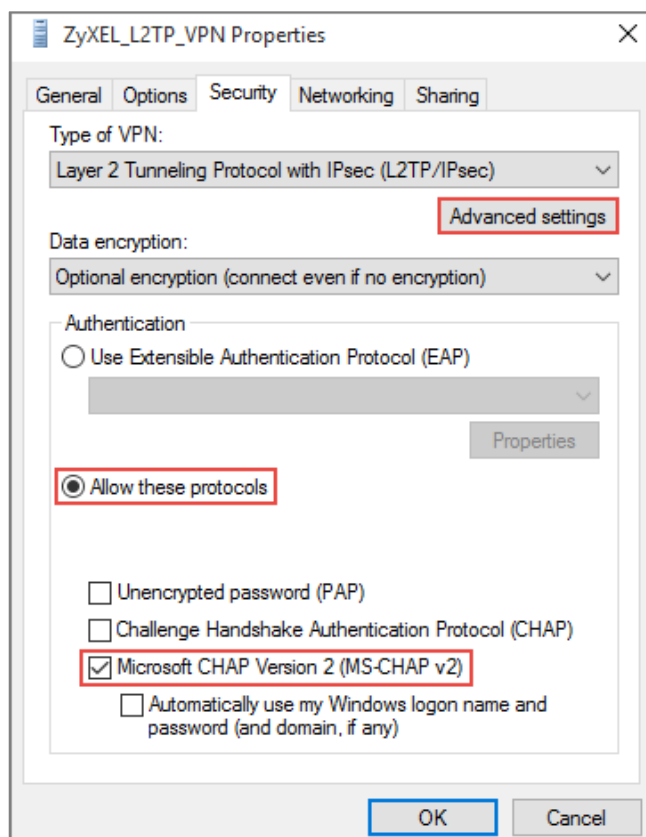
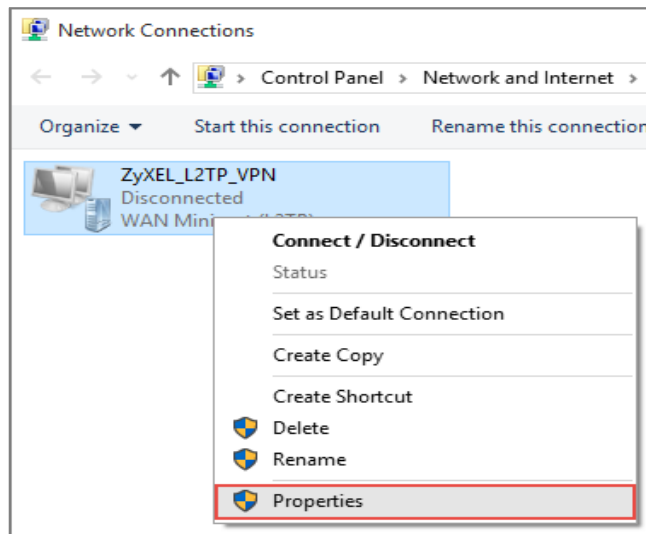
User name (optional)
L2TP_Remote_Users

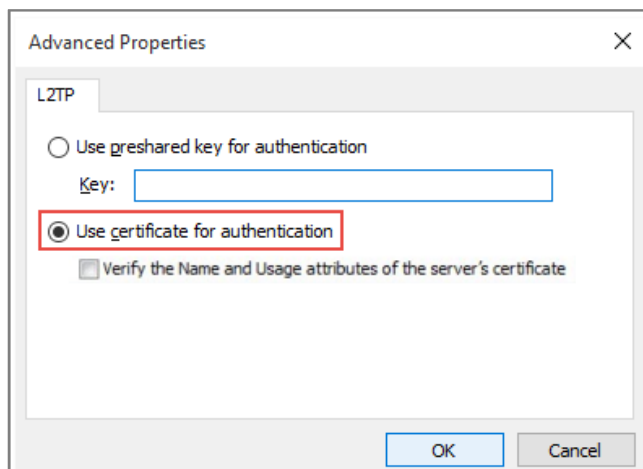
Password (optional)
•••••

☒ Remember my sign-in info

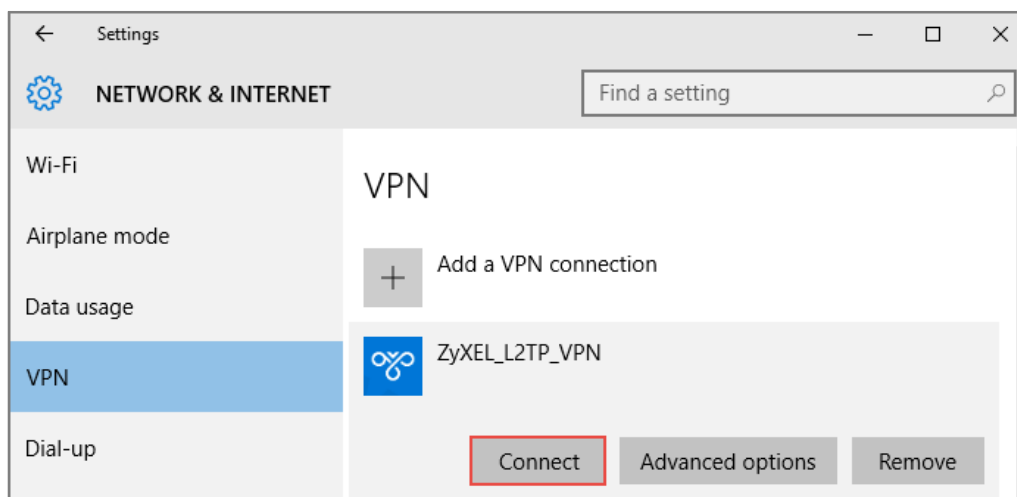
Save Cancel

- 7 Go to Control Panel > Network and Internet > Network Connections and right click Properties. Continue to Security > Advanced settings and select Use Certificate for authentication.






- 8 Go to Network & Internet Settings window, click Connect.



Test the L2TP over IPSec VPN Tunnel

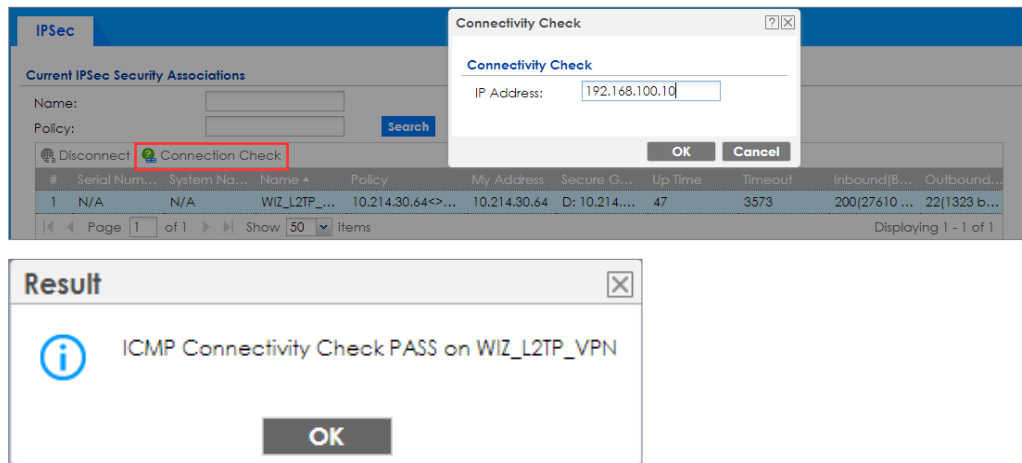
1. Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, the **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

| IPv4 Configuration | | | | |
|--|---|--------------|--------------|-------------------------------------|
| Add Edit Remove Activate Inactivate Connect Disconnect Object References | | | | |
| # | Status | Name | VPN Gateway | Policy |
| 1 |  | WIZ_L2TP_VPN | WIZ_L2TP_VPN | WIZ_L2TP_VPN_LOCAL/ |
| Page 1 of 1 Show 50 items Displaying 1 - 1 of 1 | | | | |

- Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic. Click **Connectivity Check** to verify the result of ICMP Connectivity.

Hub_HQ > MONITOR > VPN Monitor > IPSec > WIZ_L2TP_VPN



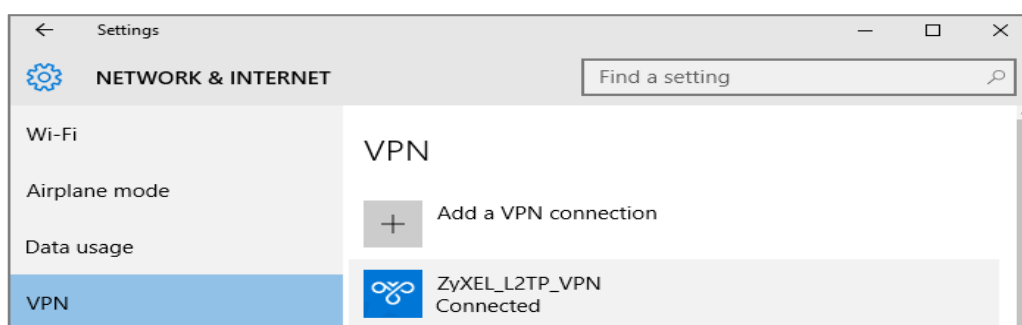
- Go to ZyWALL/USG **MONITOR > VPN Monitor > L2TP over IPSec** and verify the **Current L2TP Session**.

MONITOR > VPN Monitor > L2TP over IPSec > L2TP_Remote_Users

| Current L2TP Session | | | | |
|----------------------|-------------------|----------|----------------|--------------|
| Disconnect Refresh | | | | |
| # | User Name | Hostname | Assigned IP | Public IP |
| 1 | L2TP_Remote_Users | ellen-PC | 192.168.100.10 | 10.214.30.69 |

- Go to iOS operating system **Start > Settings > Network & Internet > VPN** and show **Connected** status.

Menu > Settings > VPN > ZyXEL_L2TP



What Could Go Wrong?

1. If you see [alert] log message such as below, please check ZyWALL/USG L2TP Allowed User or User/Group Settings. iOS users must use the same Username and Password as configured in ZyWALL/USG to establish the L2TP VPN.

| # | Ti... | Priority | Category | Message | Note |
|---|-------|----------|-----------------|---|----------|
| 1 | 2... | info | IKE | ISAKMP SA [WIZ_L2TP_VPN] is disconnected | IKE_LOG |
| 2 | 2... | info | IKE | Send:[HASH][DEL] [count=6] | IKE_LOG |
| 3 | 2... | info | IKE | Tunnel [WIZ_L2TP_VPN:WIZ_L2TP_VPN:0xa8aad2b4] is disconnected | IKE_LOG |
| 4 | 2... | alert | L2TP Over IPSec | User L2TP_Remote_Users has been denied from L2TP service.(Incorrect Username or Password) | L2TP_LOG |

2. If you see [info] or [error] log message such as below, please check ZyWALL/USG Phase 1 Settings. iOS users must use the same Pre-Shared Key as configured in ZyWALL/USG to establish the IKE SA.

| Priority | Category | Message | Note |
|----------|----------|--|---------|
| info | IKE | Send:[NOTIFY:INVALID_PAYLOAD_TYPE] | IKE_LOG |
| info | IKE | Invalid payload type in encrypted payload chain, possibly because of different pre-shared keys | IKE_LOG |

3. If you see that Phase 1 IKE SA process has completed but still get [info] log message as below, please check ZyWALL/USG Phase 2 Settings. ZyWALL/USG unit must set correct **Local Policy** to establish the IKE SA.

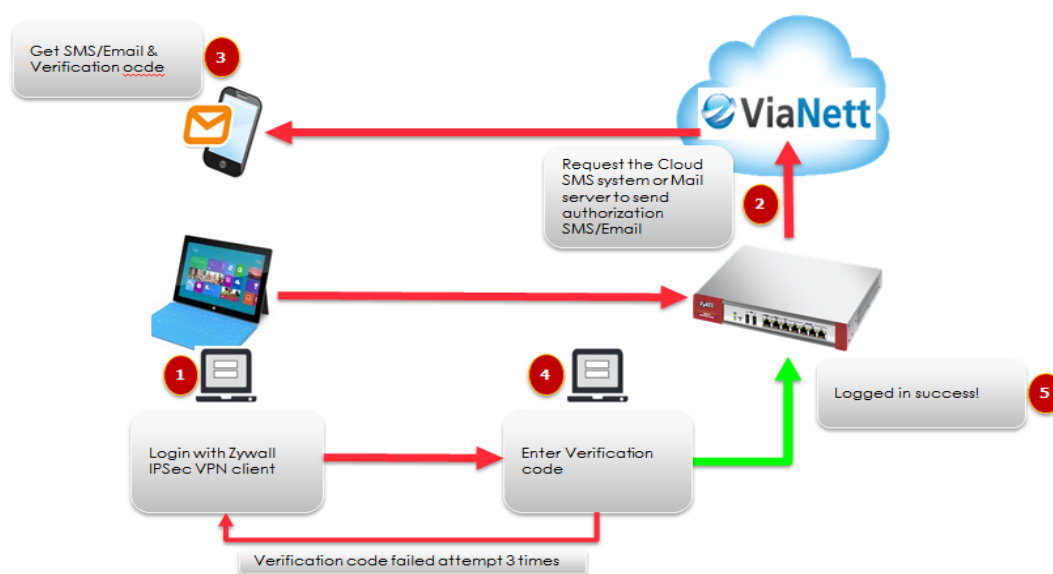
| Priority | Category | Message | Note |
|----------|----------|--|---------|
| info | IKE | ISAKMP SA [WIZ_L2TP_VPN] is disconnected | IKE_LOG |
| info | IKE | Received delete notification | IKE_LOG |
| info | IKE | Recv:[HASH][DEL] | IKE_LOG |
| info | IKE | Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN] | IKE_LOG |
| info | IKE | [SA] : No proposal chosen | IKE_LOG |
| info | IKE | [ID] : Tunnel [WIZ_L2TP_VPN] Phase 2 Local policy mismatch | IKE_LOG |

4. Ensure that the L2TP Address Pool does not conflict with any existing LAN1, LAN2, DMZ, or WLAN zones, even if they are not in use.
5. If you cannot access devices in the local network, verify that the devices in the local network set the USG's IP as their default gateway to utilize the L2TP tunnel.

6. Make sure the ZyWALL/USG units' security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.
7. Verify that the Zone is set correctly in the VPN Connection rule. This should be set to IPSec_VPN Zone so that security policies are applied properly.

How to Configure 2 factor for VPN connection?

This example shows how to use two-factor authentication to have double-layer security to access a secured network behind the Zyxel Device via a VPN tunnel between a ZyWALL/USG and a ZyWALL IPSec VPN Client. The first layer is the VPN client user name / password and the second layer is an authorized SMS (via mobile phone number) or email address.



Walkthrough

1. Set up the ZyWALL/USG IPSec VPN Tunnel on USG
2. Set up the ZyWALL IPSec VPN Client on windows client.
3. Set up notification for email and SMS message sending.
4. Enable 2 factor authentications for VPN service.

Set up the ZyWALL/USG IPSec VPN Tunnel

In the ZyWALL/USG, go to **CONFIGURATION > Quick Setup > VPN Setup Wizard**, use the **VPN Settings for Configuration Provisioning** wizard to create a VPN rule that can be used with the ZyWALL IPSec VPN Client. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
1 2 3

Welcome

- ☐ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☒ **VPN Settings for Configuration Provisioning**
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
1 2 3

Please select the type of VPN policy you wish to setup.

Type of VPN policy

- ☒ **Express**
- ☐ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings-1

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Scenario

Rule Name:

WIZ_VPN_PROVISIONING

Application Scenario:

Remote Access (Server Role)

Type a secure **Pre-Shared Key** (8-32 characters). Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings-2

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Configuration

Secure Gateway:

Any

Pre-Shared Key:

zyx12345

Local Policy (IP/Mask)

192.168.1.33

/

255.255.255.0

Remote Policy (IP/Mask):

Any

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings-3

VPN Setup Wizard

[Wizard Type](#) > **VPN Settings** > [Wizard Completed](#)

1

2

3

Express Settings

Summary

| | |
|--------------------------|-----------------------------|
| Rule Name: | WIZ_VPN_PROVISIONING |
| Secure Gateway: | Any |
| Pre-Shared Key: | zyx12345 |
| Local Policy (IP/Mask): | 192.168.1.0 / 255.255.255.0 |
| Remote Policy (IP/Mask): | Any |

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed

VPN Setup Wizard

[Wizard Type](#) > [VPN Settings](#) > **Wizard Completed**

1

2

3

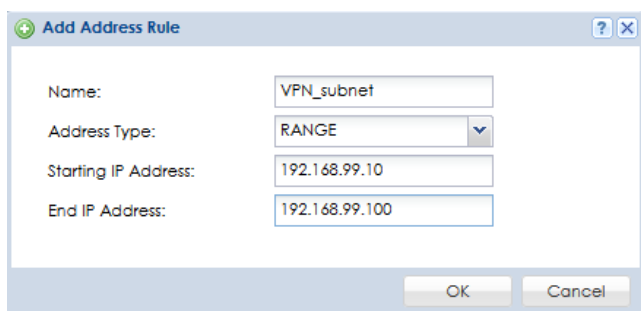
Express Settings

Congratulations. The VPN Access wizard is completed

Summary

| | |
|--------------------------|-----------------------------|
| Rule Name: | WIZ_VPN_PROVISIONING |
| Secure Gateway: | Any |
| Pre-Shared Key: | zyx12345 |
| Local Policy (IP/Mask): | 192.168.1.0 / 255.255.255.0 |
| Remote Policy (IP/Mask): | Any |

Go to **CONFIGURATION > VPN > IPSec VPN > VPN connection**. Enable **Mode config** for IPSec VPN client connection, create address object

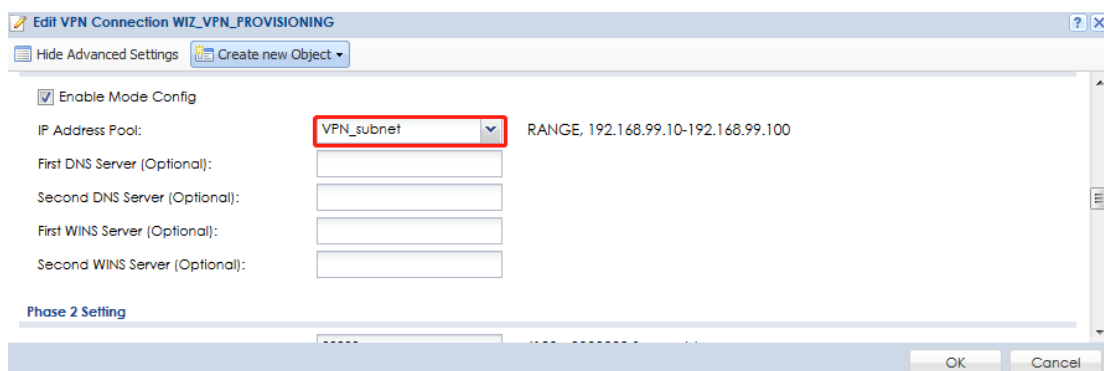


The 'Add Address Rule' dialog box contains the following fields:

- Name: VPN_subnet
- Address Type: RANGE
- Starting IP Address: 192.168.99.10
- End IP Address: 192.168.99.100

Buttons: OK, Cancel

Select the address object for mode config VPN IP address Pool.



The 'Edit VPN Connection WIZ_VPN_PROVISIONING' dialog box shows the following settings:

- ☒ Enable Mode Config
- IP Address Pool: VPN_subnet (highlighted with a red box) RANGE, 192.168.99.10-192.168.99.100
- First DNS Server (Optional):
- Second DNS Server (Optional):
- First WINS Server (Optional):
- Second WINS Server (Optional):

Section: Phase 2 Setting

Buttons: OK, Cancel

Go to **CONFIGURATION > Object > User/Group > Add A User** and create a user account for the ZyWALL IPSec VPN Client user. Type one or more valid email addresses and valid mobile telephone number for this user so that messages can be sent to this user for 2 factor authentication.

CONFIGURATION > Object > User/Group > Add A User

Go to **CONFIGURATION > VPN > IPsec VPN > Gateway**, enable X-Auth for VPN client authentication.

Go to **CONFIGURATION > VPN > IPsec VPN > Configuration Provisioning**. In the **General Settings** section, select the **Enable Configuration Provisioning**. Then, go to

the **Configuration** section and click **Add** to bind a configured **VPN Connection** to **Allowed User**. Click **Activate** and **Apply** to save the configuration.

CONFIGURATION > VPN > IPSec VPN > Configuration Provisioning

General Settings

☒ Enable Configuration Provisioning

Authentication

Client Authentication Method: default

Configuration

Add Edit Remove Activate Inactivate Move

| # | Status | Priority | Type | VPN Connection | Allowed User |
|---|--------|----------|------|----------------------|---------------|
| 1 | | 1 | 4in4 | WIZ_VPN_PROVISIONING | Remote_Client |

Page 1 of 1 | Show 50 items | Displaying 1 - 1 of 1

Apply Reset

Set up the ZyWALL IPSec VPN Client

Download **ZyWALL IPSec VPN Client** software from ZyXEL Download Library:

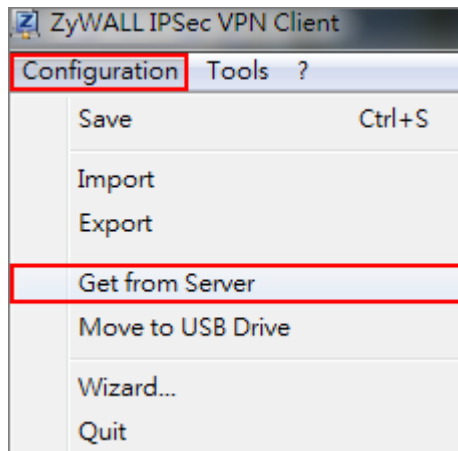
http://www.zyxel.com/support/download_landing.shtml

Search by Model Number

ZyWALL IPSec VPN Client

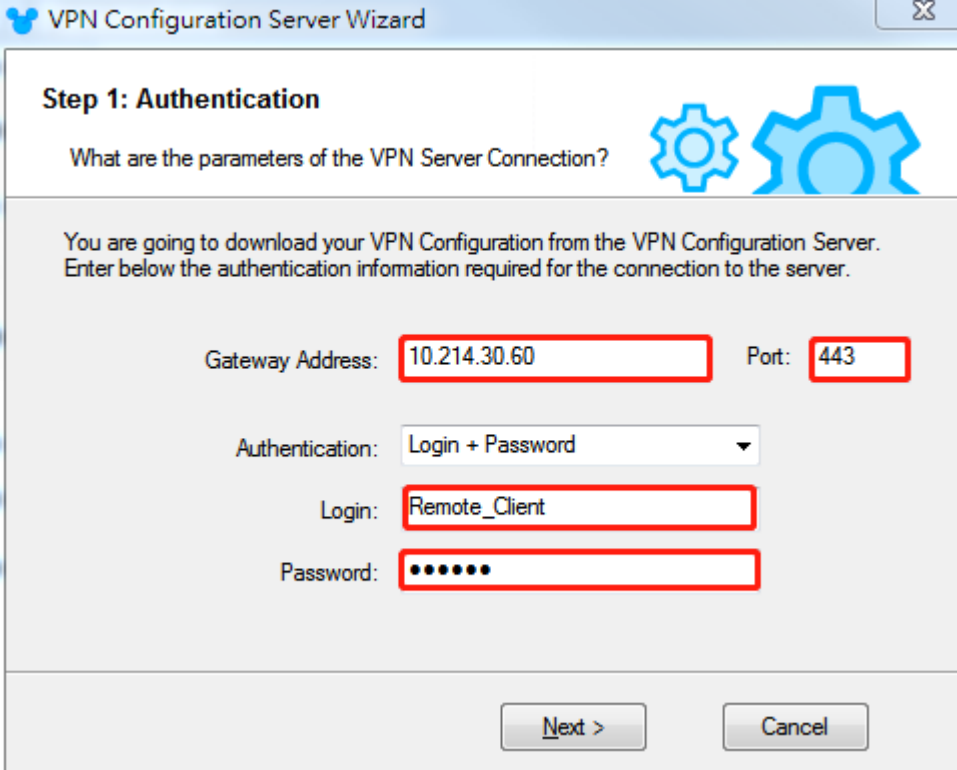
Open ZyWALL IPSec VPN Client, select **CONFIGURATION > Get from Server**.

CONFIGURATION > Get from Server



Enter the WAN IP address or URL for the ZyWALL/USG in the **Gateway Address**. If you changed the default HTTPS **Port** on the ZyWALL/USG, and then enter the new one here. Enter the **Login** user name and **Password** exactly as configured on the ZyWALL or external authentication server. Click **Next**, you will see it's processing VPN configuration from the server.

CONFIGURATION > Get from Server > Step 1: Authentication



VPN Configuration Server Wizard

Step 1: Authentication

What are the parameters of the VPN Server Connection?

You are going to download your VPN Configuration from the VPN Configuration Server.
Enter below the authentication information required for the connection to the server.

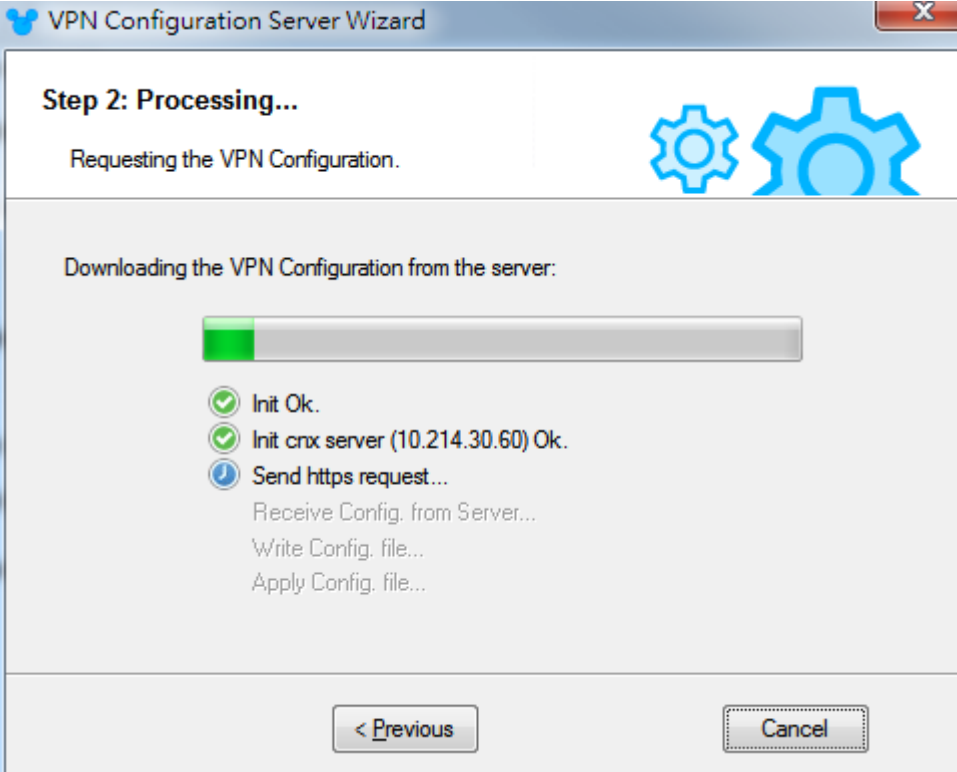
Gateway Address: Port:

Authentication:

Login:

Password:

CONFIGURATION > Get from Server > Step 2: Processing



VPN Configuration Server Wizard

Step 2: Processing...

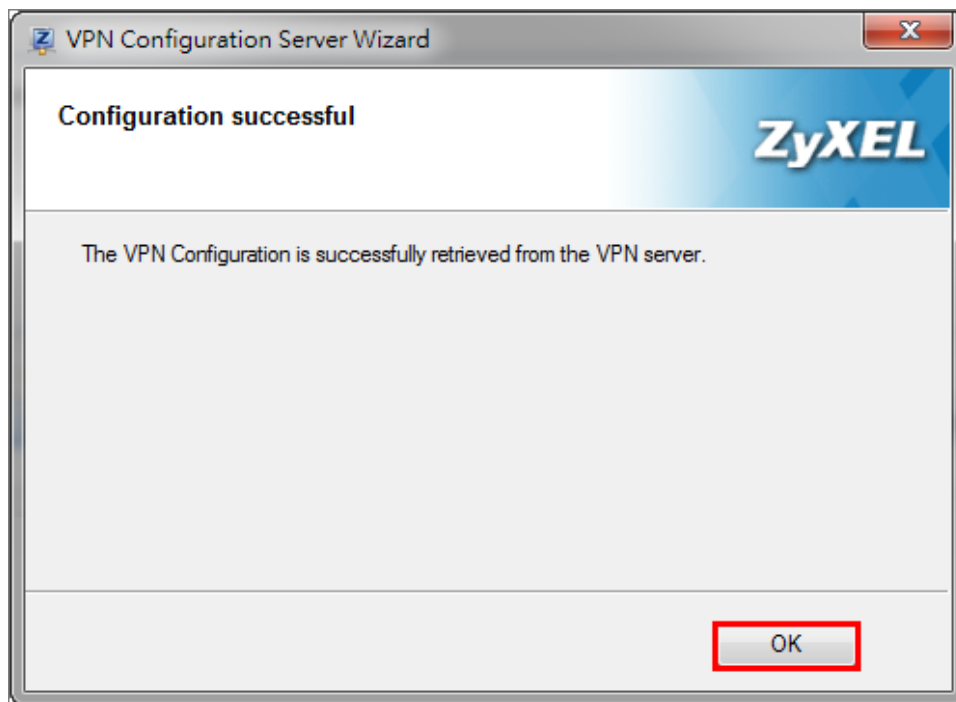
Requesting the VPN Configuration.

Downloading the VPN Configuration from the server:

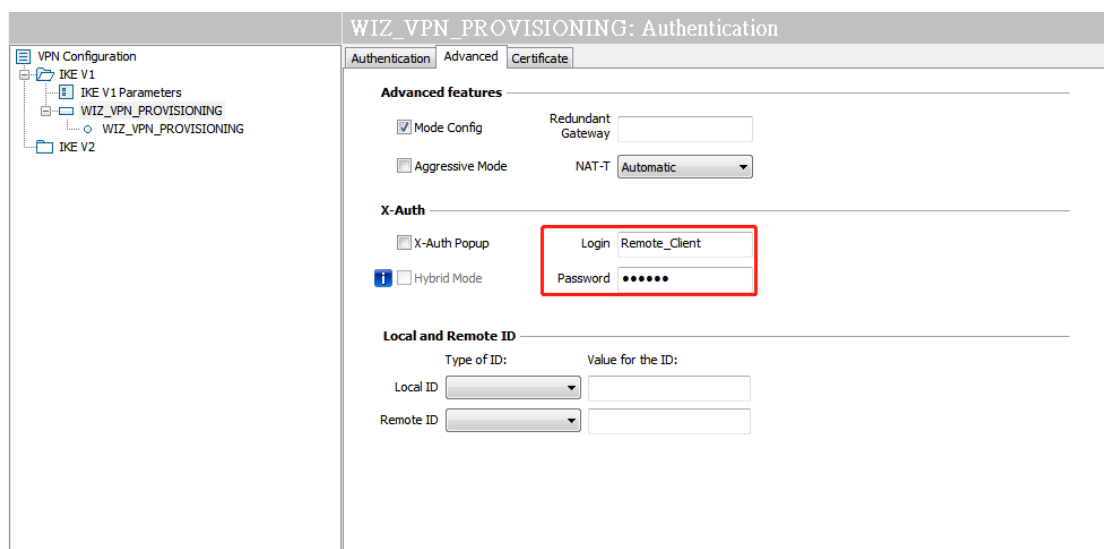
- ☒ Init Ok.
- ☒ Init cnx server (10.214.30.60) Ok.
- ☐ Send https request...
 - Receive Config. from Server...
 - Write Config. file...
 - Apply Config. file...

Then, you will see the **Configuration successful** page, click **OK** to exit the wizard.

CONFIGURATION > Get from Server > Configuration successful



VPN CONFIGURATION > IKE V1 > WIZ_VPN_PROVISIONING > Advanced, type Login account and password for authentication.



Set up notification for 2 factor authentication

In the ZyWALL/USG, go to **CONFIGURATION > System > Notification > Mail Server**

1. Type the name or IP address of the SMTP server.
2. Enter the service port for SMTP.
3. Type the e-mail address from which the outgoing e-mail is delivered.
4. Select this check box if it is necessary to provide a user name and password to the SMTP server.
5. Click **“Apply”** button to save your changes to the Zyxel Device.

The screenshot shows the 'Mail Server' configuration page in the ZyXel web interface. The 'General Settings' tab is selected. The following fields are highlighted with red boxes:

- Mail Server:** smtp.pchome.com.tw (Outgoing SMTP Server Name or IP Address)
- Mail Subject:** ☐ Append system name ☐ Append date time
- Mail Server Port:** 25
- Mail From:** cooldia@pchome.com.tw (Email Address)
- SMTP Authentication:** ☒
- User Name:** cooldia
- Password:** [masked with dots]
- Retype to Confirm:** [masked with dots]

The **Schedule** section at the bottom shows 'Time For Sending Report' set to 0 (hours) and 0 (minutes).

Go to 2nd tab **CONFIGURATION > System > Notification > SMS**, in this scenario, we will use email and SMS for 2 factor authentication.

1. Select the check box “Enable SMS” to turn on the SMS service.
2. Enter the default country code for the mobile phone number to which you want to send SMS messages.
3. Enter the user name and password for your ViaNett account.
4. Click **“Apply”** button to save your changes to the Zyxel Device.

The screenshot shows the ZyXEL web interface for SMS configuration. The 'SMS' tab is active. In the 'General Settings' section, the 'Enable SMS' checkbox is checked. Below it, the 'Default country code for phone number' is set to '886' (1-4 digit). The 'Purchase SMS Voucher from Zyxel reseller' section contains a link to zyxel.vianett.com. The 'ViaNett Configuration' section has three fields: 'User Name' (pd000245), 'Password' (masked with dots), and 'Retype to Confirm' (masked with dots). These three fields are enclosed in a red rectangular box.

Set up authentication for 2 factor VPN connection

In the ZyWALL/USG, go to **CONFIGURATION > Object > Auth.Method > Two-factor Authentication**.

1. Select the check box **"Enable"** to enable 2 factor authentications.
2. Enter the maximum time (in minutes) that the user must click or tap the authorization link in the SMS or email in order to get authorization for the VPN connection.
3. Select which kinds of VPN tunnels require Two-Factor Authentication. in this scenario, we enable 2 factor authentication on IPSec VPN Access
4. This list displays the names of the users and user groups that can be selected for two-factor authentication.
5. Use this section to configure how to send an SMS or email for authorization.
We select both methods in this scenario.
6. Configure the link that the user will receive in the SMS or email. The user must be able to access the link.
7. You can either create a default message in the text box or upload a message file (Use Multilingual file) from your computer.
8. Click **"Apply"** button to save your changes to the Zyxel Device.

General Settings

☒ **Enable**

Valid Time: (1-15 minutes)

Two-factor Authentication for Services:

☐ SSL VPN Access ☒ **IPSec VPN Access** ☐ L2TP/IPSec VPN Access

User/Group

Selectable User/Group Objects

admin
ldap-users
radius-users
ad-users
test

Selected User/Group Objects

any

Delivery Settings

Deliver Authorize Link Method: ☒ **SMS** ☒ **Email**

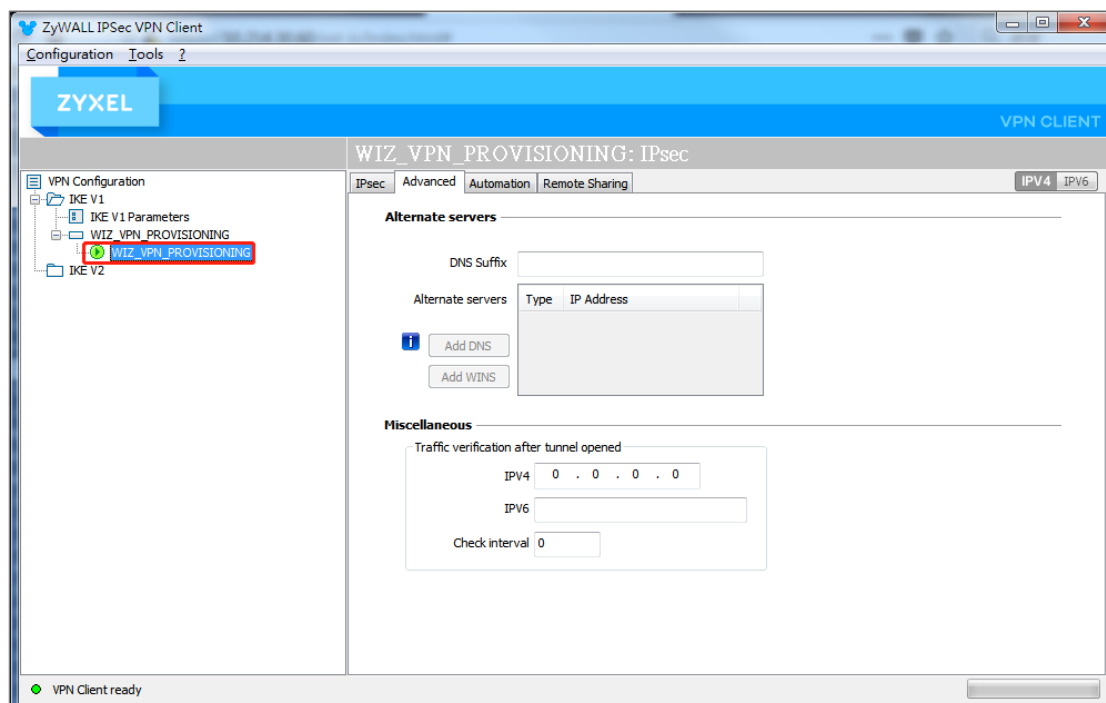
Authorize Link URL Address: (Domain Name or IP Address) i

Message: ☒ Use Default Message ☐ Use Multilingual file

<users>. You have initiated a VPN connection to a secured network behind the <hosts>. Please click or tap the following link within <time> minutes to get authorization for the VPN connection. <url>

Test the Result

Go to **VPN Configuration > IKEv1**, right click the **WIZ_VPN_PROVISIONING** and select **Open tunnel**. You will see the **Tunnel opened** on ZyWALL IPSec VPN client



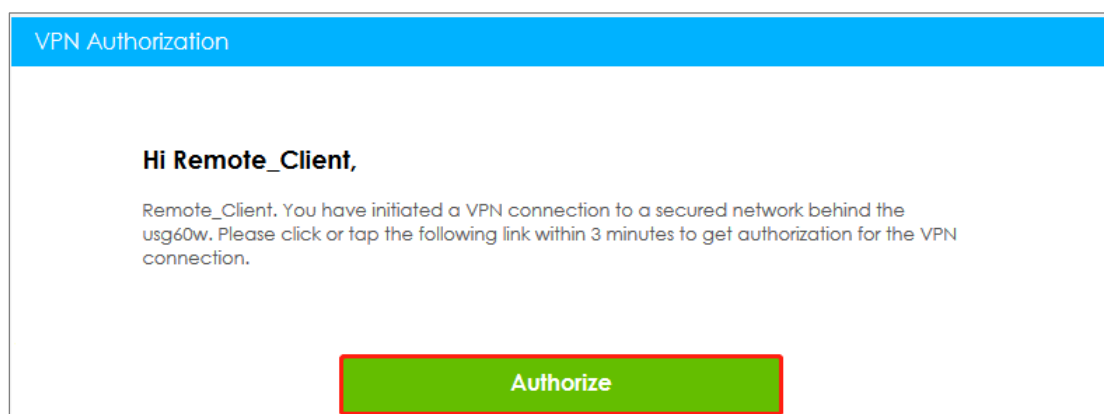
The VPN tunnel is created from the ZyWALL IPSec VPN client to the ZyWALL/USG, but we are still unable to access Intranet behind the ZyWALL/USG. The ZyWALL/USG send authorized link via phone number or email address in order to authenticate this user's

use of the VPN tunnel (factor 2). If user does not click the link, then the Zyxel Device terminates the VPN connection. The client should access the authorization link sent via SMS or email by the Cloud SMS system within a specified deadline (Valid Time). If the authorization is correct and received on time, then the client can have VPN access to the secured network. If the authorization deadline has expired, then the client will have to run the VPN client again. If authorization credentials are incorrect or if the SMS/email was not received, then the client must check with the network administrator.

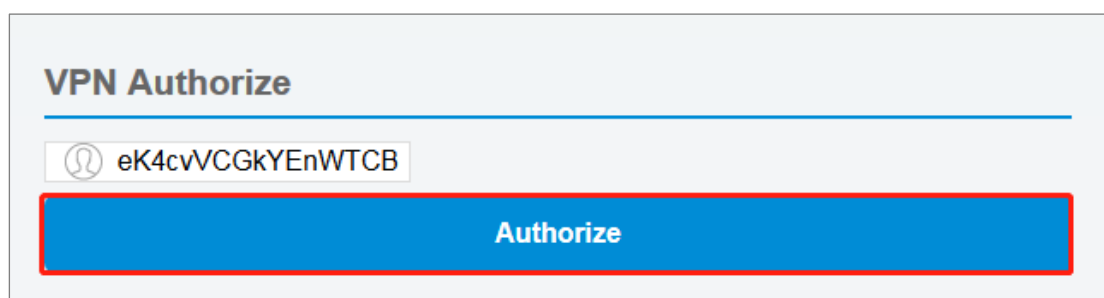
The following is authorized example by email and SMS

Authorized by email link

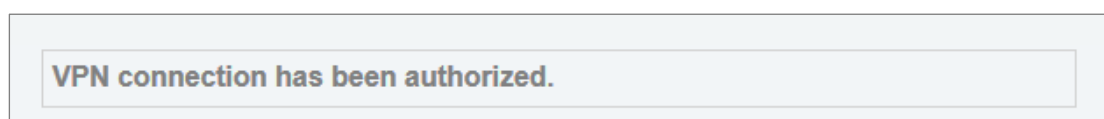
1. Received authorization mail with authorize link.



2. Click the "**Authorize**" to authorization.

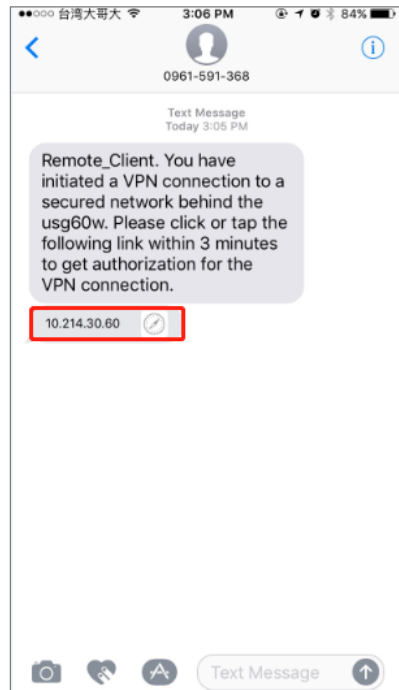


3. After we see "**VPN connection has been authorized**", we can access the secured network behind the ZyWALL/USG.

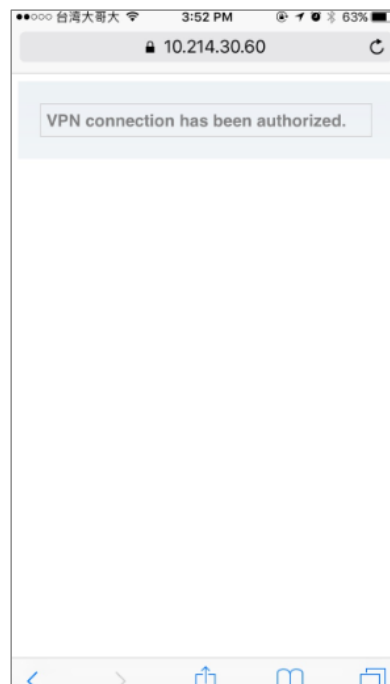
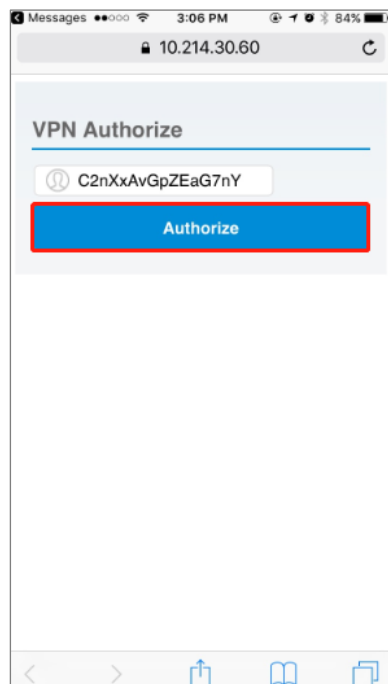


Authorized by SMS

1. Received authorization SMS with authorize link.



2. Click the SMS link to authorized, after we see "VPN connection has been authorized", we can access the secured network behind the ZyWALL/USG.



What could went wrong

If you see below log message "**Mail server authentication failed.**", please check "**CONFIGURATION > System > Notification > SMTP Server**", Make sure your password is correct for mail authentication

MONITOR > Log

| # | Time | Priority | Category | Message | Source | Destination | Note |
|---|----------------|----------|----------------|--|--------|-------------|----------------|
| 1 | 2018-07-27 ... | error | System | Mail server authentication failed. | | | |
| 2 | 2018-07-27 ... | info | Authenticat... | send E-mail to user: Remote_Client, email:coo*****t... | | | two-factor ... |

If you see below log message "**Cannot resolve mail server address smtp.pchome.com.t**" please check "**CONFIGURATION > System > Notification > SMTP Server**", Make sure your service IP/hostname is correct for mail authentication.

MONITOR > Log

| # | Time | Priority | Category | Message | Source | Destination | Note |
|---|----------------|----------|----------------|--|--------|-------------|----------------|
| 1 | 2018-07-27 ... | error | System | Cannot resolve mail server address smtp.pchome.com.t. | | | |
| 2 | 2018-07-27 ... | info | Authenticat... | send E-mail to user: Remote_Client, email:coo*****t... | | | two-factor ... |

If you are unable to received SMS for authorization, please check "**CONFIGURATION > System > Notification > SMS**", confirm the country code is correct for SMS message
CONFIGURATION > System > Notification > SMS

General Settings

☒ Enable SMS

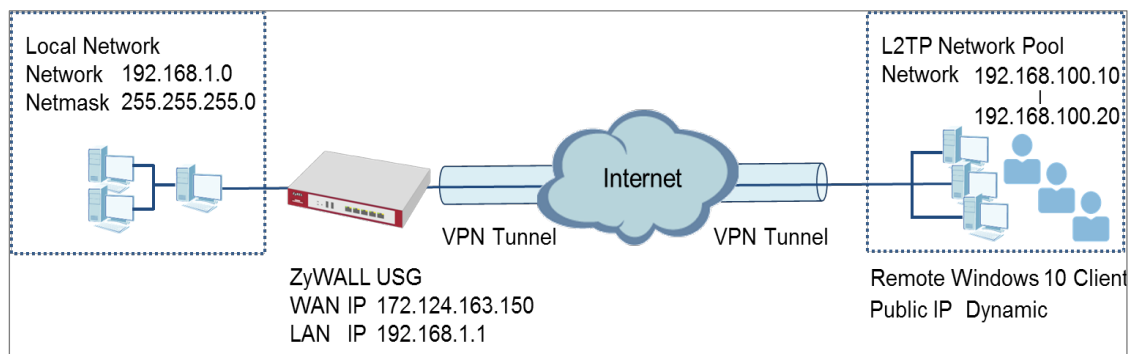
Default country code for phone number:
(1-4) digit

[Purchase SMS Voucher from Zyxel reseller](#)

How to Import ZyWALL/USG Certificate for L2TP over IPsec in Android mobile phone

This is an example of using the L2TP VPN and VPN client software included in Android mobile phone operating systems. When the VPN tunnel is configured, users can securely access the network behind the ZyWALL/USG and allow traffic from L2TP clients to go to the Internet from an Android mobile phone.

ZyWALL/USG L2TP VPN with Remote Android Mobile Phone Client Example

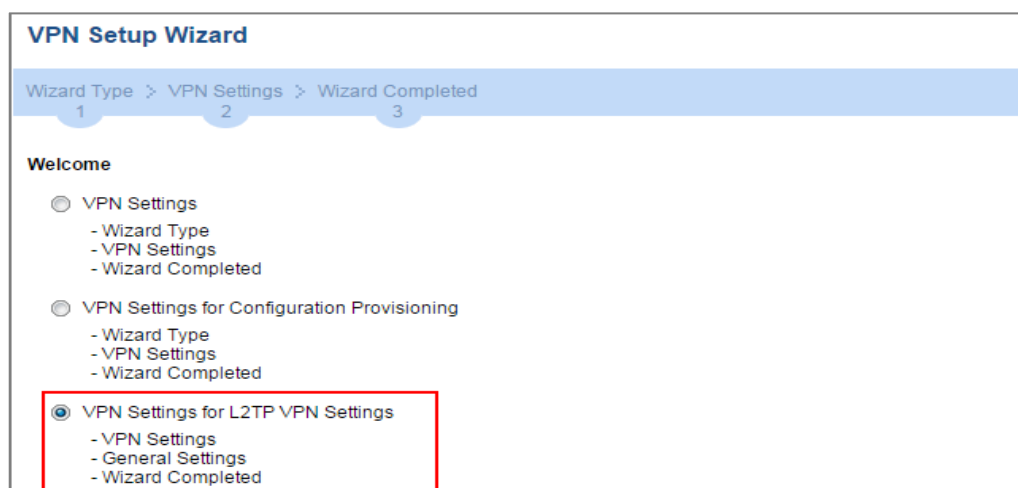


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: 4.25) and Android (Version: 10.0.10240)

Set Up the L2TP VPN Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings for L2TP VPN Settings** wizard to create a **L2TP VPN** rule that can be used with the Android mobile phone clients. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



Then, configure the **Rule Name** and set **My Address** to be the **wan1** interface which is connected to the Internet. Type a secure **Pre-Shared Key** (8-32 characters).

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings

VPN Setup Wizard

VPN Settings > General Settings > Wizard Completed

1

2

3

L2TP VPN Settings

Rule Name:

Phase 1 Setting

My Address (interface):

Authentication Method

Pre-Shared Key:

Assign the L2TP users' IP address range from 192.168.100.10 to 192.168.100.20 for use in the L2TP VPN tunnel and select **Allow L2TP traffic Through WAN** to allow traffic from L2TP clients to go to the Internet. Click **OK**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (L2TP VPN Settings)

VPN Setup Wizard

VPN Settings > General Settings > Wizard Completed

1

2

3

L2TP VPN Settings

IP Address Pool: ⓘ

Starting IP Address:

End IP Address:

First DNS Server (Optional):

Second DNS Server (Optional):

☒ Allow L2TP traffic Through WAN

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (Summary)

VPN Setup Wizard

Wizard Type

VPN Settings

Wizard Completed

1

2

3

Advanced Settings

Summary

| | |
|-------------------------|--|
| Rule Name: | WIZ_L2TP_VPN |
| Secure Gateway: | Any |
| Pre-Shared Key: | xyz12345 |
| My Address (interface): | wan1 |
| IP Address Pool: | RANGE, 192.168.100.10 - 192.168.100.20 |

Now the rule is configured on the ZyWALL/USG. The rule settings appear in the **VPN > L2TP VPN** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings > Wizard Completed

VPN Setup Wizard

Wizard Type

VPN Settings

Wizard Completed

1

2

3

L2TP VPN Settings

Congratulations. The VPN Access wizard is completed

Summary

| | |
|-------------------------|--|
| Rule Name: | WIZ_L2TP_VPN |
| My Address (interface): | wan1 |
| Pre-Shared Key: | xyz12345 |
| IP Address Pool: | RANGE, 192.168.100.10 - 192.168.100.20 |

Go to **CONFIGURATION > VPN > VPN Gateway > WIZ_L2TP_VPN**, change **Authentication** method to be **Certificate** and select the certificate which ZyWALL/USG uses to identify itself to the Android mobile phone.

CONFIGURATION > VPN > VPN Gateway > WIZ_L2TP_VPN > Authentication > Certificate

Authentication

☐ Pre-Shared Key

☐ unmasked

☒ Certificate default (See [My Certificates](#))

☐ User Based PSK L2TP_Remote_Users i

Go to **CONFIGURATION > VPN > L2TP VPN > Create new Object > User** to add **User Name** and **Password** (4-24 characters). Then, set **Allowed User** to the newly created object (L2TP_Remote_Users/zyx168 in this example).

CONFIGURATION > VPN > L2TP VPN > Create new Object > User

Add A User

User Configuration

User Name : L2TP_Remote_Users

User Type: User

Password:

Retype:

Description: Local User

OK Cancel

L2TP VPN

Show Advanced Settings Create new Object

User

Address

General Settings

☒ Enable L2TP Over IPSec

VPN Connection: WIZ_L2TP_VPN

IP Address Pool: WIZ_L2TP_VPN_IP_ADDRESS i RANGE, 192.168.100.10-192.168.100.20

Authentication Method: default local

Allowed User: any

Keep Alive Timer: 60 (1-180 seconds)

L2TP VPN

Show Advanced Settings Create new Object

General Settings

☒ Enable L2TP Over IPSec

VPN Connection: WIZ_L2TP_VPN

IP Address Pool: WIZ_L2TP_VPN_IP_ADDRESS RANGE, 192.168.100.10-192.168.100.20

Authentication Method: default

Allowed User: any

Keep Alive Timer: 60 (1-180 seconds)

local

any

=== Object ===

admin

ldap-users

radius-users

ad-users

L2TP_Remote_Users

Export a Certificate from ZyWALL/USG and Import it to Android Mobile Phone

Go to ZyWALL/USG **CONFIGURATION > Object > Certificate**, select the certificate (**default** in this example) and click **Edit**.

CONFIGURATION > Object > Certificate > default

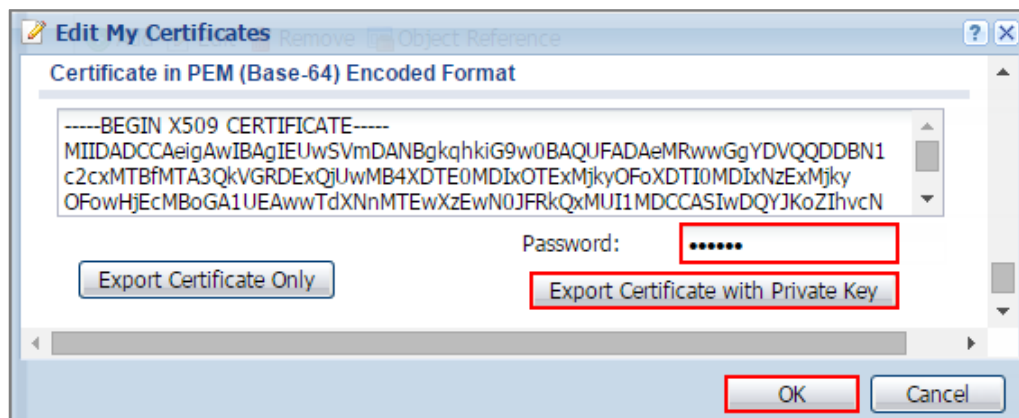
My Certificates Setting

Add Edit Remove Object Reference

| # | Name | Type | Subject | Issuer | Valid From | Valid To |
|---|---------|------|------------------------|------------------------|-------------------------|-------------------------|
| 1 | default | SELF | CN=usg110_107BEFD11B50 | CN=usg110_107BEFD11B50 | 2014-02-19 11:29:28 GMT | 2024-02-17 11:29:28 GMT |

Export default certificate from ZyWALL/USG with Private Key (zyx123 in this example)

CONFIGURATION > Object > Certificate > default > Edit > Export Certificate with Private Key



Save **default** certificate as ***.p12** file to Android mobile phone computer.



default.p12

Set Up the L2TP VPN Tunnel on the Android Mobile Device

- 1 To configure L2TP VPN in Android, go to Start > Settings > Network & Internet > VPN > Add a VPN Connection and configure as follows.
- 2 VPN Provider set to Windows (built-in).
- 3 Configure **Connection name** for you to identify the VPN configuration.
- 4 Set **Server** name or address to be the ZyWALL/USG's WAN IP address (172.124.163.150 in this example).

- 5 Select VPN type to Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec).
- 6 Enter **User name** and **Password** which the same as **Allowed User** created in ZyWALL/USG (L2TP_Remote_Users/zyx168 in this example).

Add a VPN connection

VPN provider

Windows (built-in) ▾

Connection name

ZyXEL_L2TP_VPN

Server name or address

172.124.163.150

VPN type

Layer 2 Tunneling Protocol with IPsec (L2TP/I ▾

Type of sign-in info

User name and password ▾

User name (optional)

L2TP_Remote_Users

Password (optional)

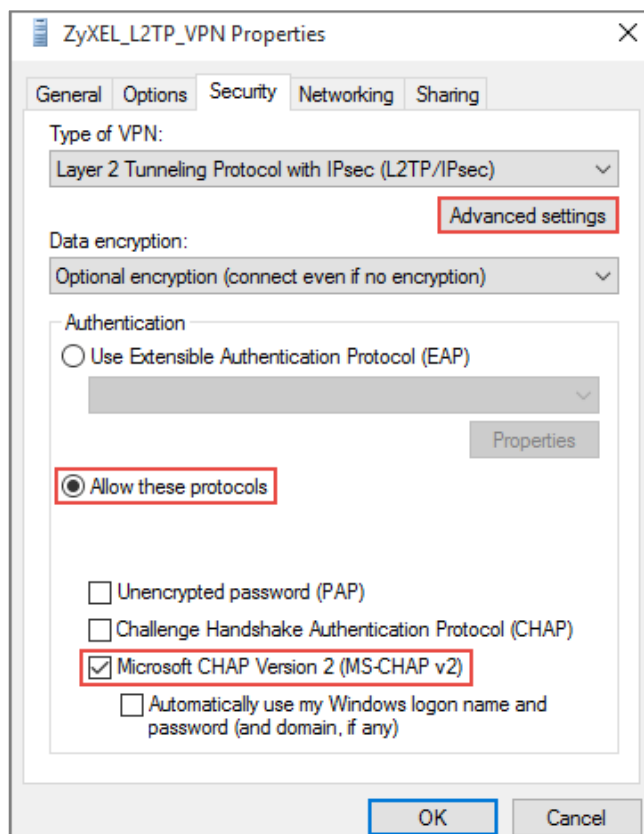
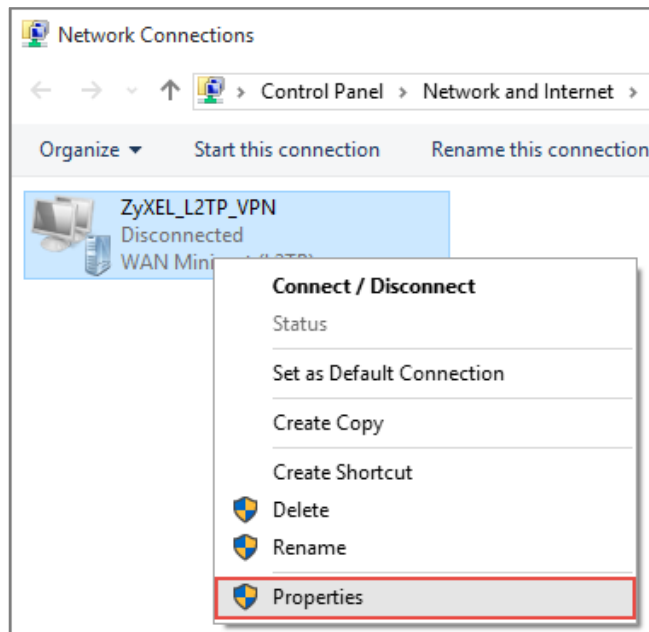
•••••

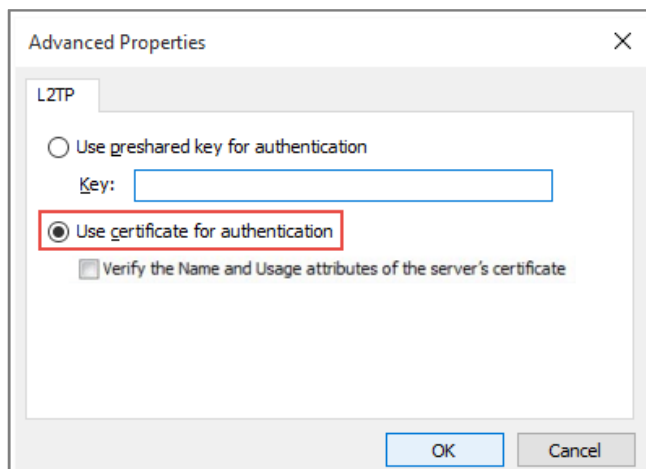
☒ Remember my sign-in info

Save

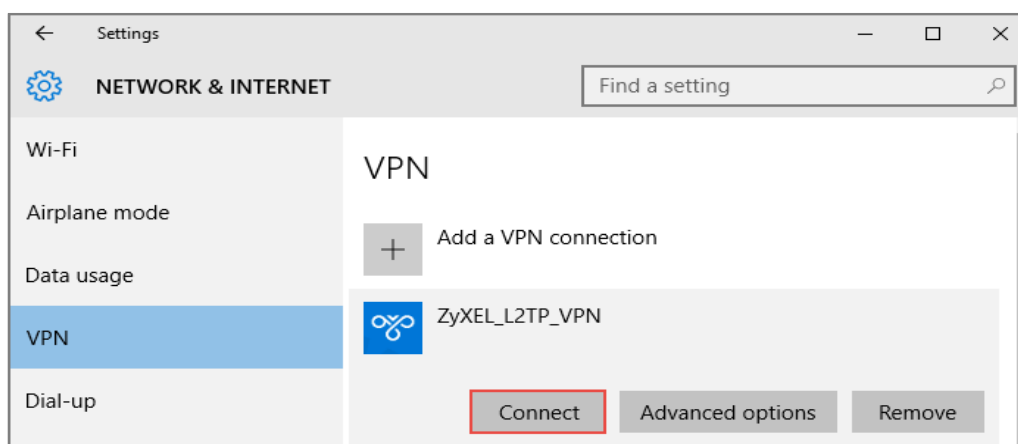
Cancel

Go to **Control Panel > Network and Internet > Network Connections** and right click **Properties**. Continue to **Security > Advanced settings** and select **Use Certificate for authentication**.





Go to **Network & Internet Settings** window, click **Connect**.



Test the L2TP over IPSec VPN Tunnel

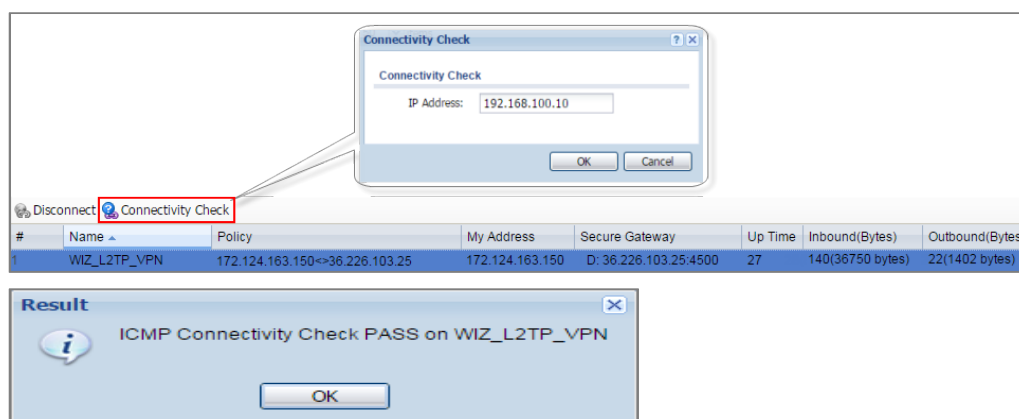
Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, the **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

| IPv4 Configuration | | | | |
|---|--------|--------------|--------------|-------------------------------------|
| Add Edit Remove Activate Inactivate Connect Disconnect Object Reference | | | | |
| # | Status | Name | VPN Gateway | Policy |
| 1 | | WIZ_L2TP_VPN | WIZ_L2TP_VPN | WIZ_L2TP_VPN_LOCAL/ |

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic. Click **Connectivity Check** to verify the result of ICMP Connectivity.

Hub_HQ > MONITOR > VPN Monitor > IPSec > WIZ_L2TP_VPN



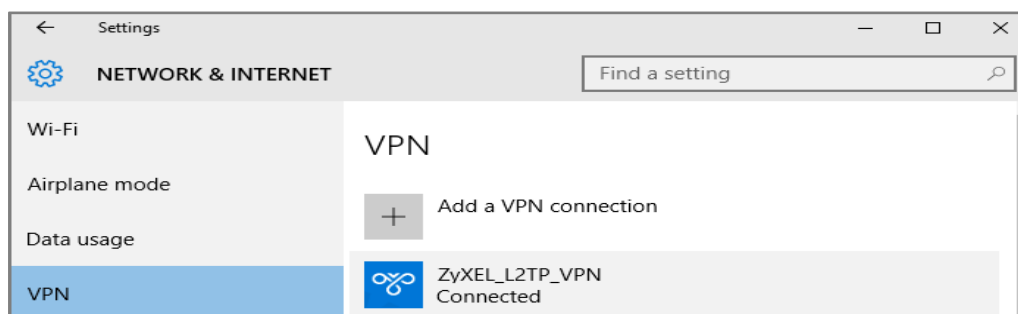
Go to ZyWALL/USG **MONITOR > VPN Monitor > L2TP over IPSec** and verify the **Current L2TP Session**.

MONITOR > VPN Monitor > L2TP over IPSec > L2TP_Remote_Users

| Current L2TP Session | | | | |
|---|-------------------|------------|----------------|---------------|
| <div> Disconnect Refresh </div> | | | | |
| # | User Name | Hostname | Assigned IP | Public IP |
| 1 | L2TP_Remote_Users | Windows_10 | 192.168.100.10 | 36.226.103.25 |

Go to Android **Start > Settings > Network & Internet > VPN** and show **Connected** status.

Menu > Settings > VPN > ZyXEL_L2TP



What Could Go Wrong?

- 7 If you see [alert] log message such as below, please check ZyWALL/USG L2TP Allowed User or User/Group Settings. Android users must use the same Username and Password as configured in ZyWALL/USG to establish the L2TP VPN.

| Priority | Category | Message | Note |
|----------|-----------------|---|----------|
| alert | L2TP Over IPSec | User L2TP_Remote_Users has been denied from L2TP service.(Incorrect Username or Password) | L2TP_LOG |

- 8 If you see [info] or [error] log message such as below, please check ZyWALL/USG Phase 1 Settings. Android users must use the same Pre-Shared Key as configured in ZyWALL/USG to establish the IKE SA.

| Priority | Category | Message | Note |
|----------|----------|--|---------|
| error | IPSec | SPI: 0x0 (0) SEQ: 0x0 (0) No rule found. Dropping TCP packet | IPSec |
| info | IKE | Send:[NOTIFY:INVALID_PAYLOAD_TYPE] | IKE_LOG |
| info | IKE | Invalid payload type in encrypted payload chain, possibly because of different pre-shared keys | IKE_LOG |
| Priority | Category | Message | Note |
| info | IKE | [SA] : No proposal chosen | IKE_LOG |
| info | IKE | [ID] : Tunnel [WIZ_L2TP_VPN] Phase 1 Remote ID mismatch | IKE_LOG |

- 9 If you see that Phase 1 IKE SA process has completed but still get [info] log message as below, please check ZyWALL/USG Phase 2 Settings. ZyWALL/USG unit must set correct **Local Policy** to establish the IKE SA.

| Priority | Category | Message | Note |
|----------|----------|--|---------|
| info | IKE | [ID] : Tunnel [WIZ_L2TP_VPN] Phase 2 Local policy mismatch | IKE_LOG |
| Priority | Category | Message | Note |
| info | IKE | Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN] | IKE_LOG |
| info | IKE | [SA] : No proposal chosen | IKE_LOG |
| info | IKE | [SA] : Tunnel [WIZ_L2TP_VPN] Phase 2 proposal mismatch | IKE_LOG |

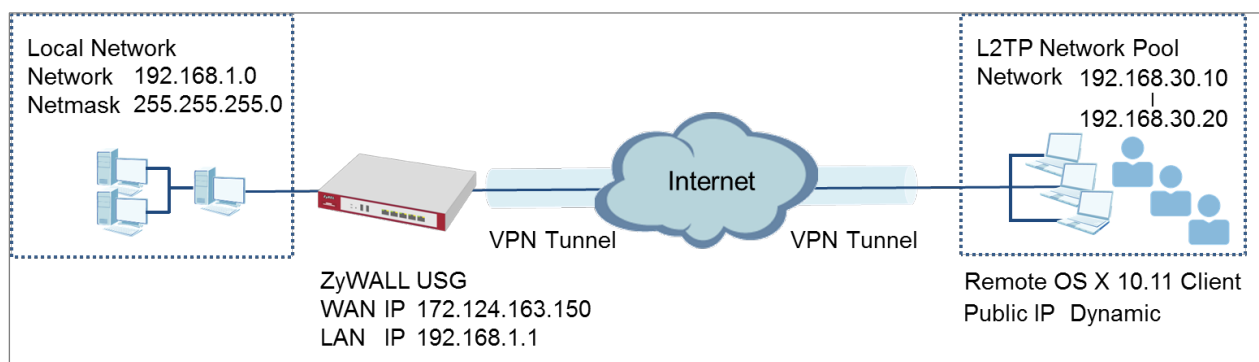
- 10 Ensure that the L2TP Address Pool does not conflict with any existing LAN1, LAN2, DMZ, or WLAN zones, even if they are not in use.


- 11** If you cannot access devices in the local network, verify that the devices in the local network set the USG's IP as their default gateway to utilize the L2TP tunnel.
- 12** Make sure the ZyWALL/USG units' security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.
- 13** Verify that the Zone is set correctly in the VPN Connection rule. This should be set to IPSec_VPN Zone so that security policies are applied properly.

How to Configure the L2TP VPN with Apple MAC OS X 10.11 Operating System

This is an example of using the L2TP VPN and VPN client software included in Apple MAC OS X 10.11 El Capitan operating systems. When the VPN tunnel is configured, users can securely access the network behind the ZyWALL/USG and allow traffic from L2TP clients to go to the Internet from an Apple computer.

ZyWALL/USG L2TP VPN with Apple MAC OS X 10.11 El Capitan



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25) and Apple MAC (Version: OS X10.11 El Capitan).

Set Up the L2TP VPN Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings for L2TP VPN Settings** wizard to create a **L2TP VPN** rule that can be used with the MAC OS X clients. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Welcome

☐ VPN Settings

- Wizard Type
- VPN Settings
- Wizard Completed

☐ VPN Settings for Configuration Provisioning

- Wizard Type
- VPN Settings
- Wizard Completed

☒ VPN Settings for L2TP VPN Settings

- VPN Settings
- General Settings
- Wizard Completed

Then, configure the **Rule Name** and set **My Address** to be the **wan1** interface which is connected to the Internet. Type a secure **Pre-Shared Key** (8-32 characters).

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings

VPN Setup Wizard

VPN Settings > General Settings > Wizard Completed

123

L2TP VPN Settings

Rule Name:

WIZ_L2TP_VPN

Phase 1 Setting

My Address (Interface):

ge1

Authentication Method

Pre-Shared Key:

xyz12345

Configure the L2TP users' IP address range from 192.168.30.10 to 192.168.30.20 for use in the L2TP VPN tunnel and check **Allow L2TP traffic Through WAN**. Click **OK**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings

VPN Setup Wizard

VPN Settings > General Settings > Wizard Completed

123

L2TP VPN Settings

IP Address Pool: RANGE ⓘ

Starting IP Address: 192.168.30.10

End IP Address: 192.168.30.20

First DNS Server (Optional):

Second DNS Server (Optional):

☒ Allow L2TP traffic Through WAN

Continue to the next page to review your **Summary** and click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings > Summary

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Summary

Rule Name: WIZ_L2TP_VPN

Secure Gateway: Any

Pre-Shared Key: xyz12345

My Address (interface): ge1

IP Address Pool: RANGE, 192.168.30.10 - 192.168.30.20

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings > Summary > Wizard Completed

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

L2TP VPN Settings

Congratulations. The VPN Access wizard is completed

Summary

| | |
|-------------------------|--------------------------------------|
| Rule Name: | WIZ_L2TP_VPN2 |
| My Address (interface): | ge1 |
| Pre-Shared Key: | xyz12345 |
| IP Address Pool: | RANGE, 192.168.30.10 - 192.168.30.20 |

Go to **CONFIGURATION > VPN > L2TP VPN > Create new Object > User** to add **User Name** and **Password** (4-24 characters). Then, set **Allowed User** to the newly created object (L2TP_Remote_Users/zyx168 in this example).

CONFIGURATION > VPN > L2TP VPN > Create new Object > User

L2TP VPN

Show Advanced Settings

Create new Object▼

User

Address

Reshooting

General Settings

Config Walkth

☒ Enable L2TP Over IPSec

VPN Connection:

WIZ_L2TP_VPN

IP Address Pool:

WIZ_L2TP_VPN_IP_A

RANGE, 192.168.30.10-192.168.30.20 ⓘ

Authentication Method:

default

local

☒ Advance

Allowed User:

any

Keep Alive Timer:

60

(1-180 seconds)

+ Add A User

?

×

User Configuration

User Name :

L2TP_Remote_Users

User Type:

user

Password:

.....

Retype:

.....

Description:

Local User

Authentication Timeout Settings

☒ Use Default Settings
 ☐ Use Manual Settings

Lease Time:

1440

minutes

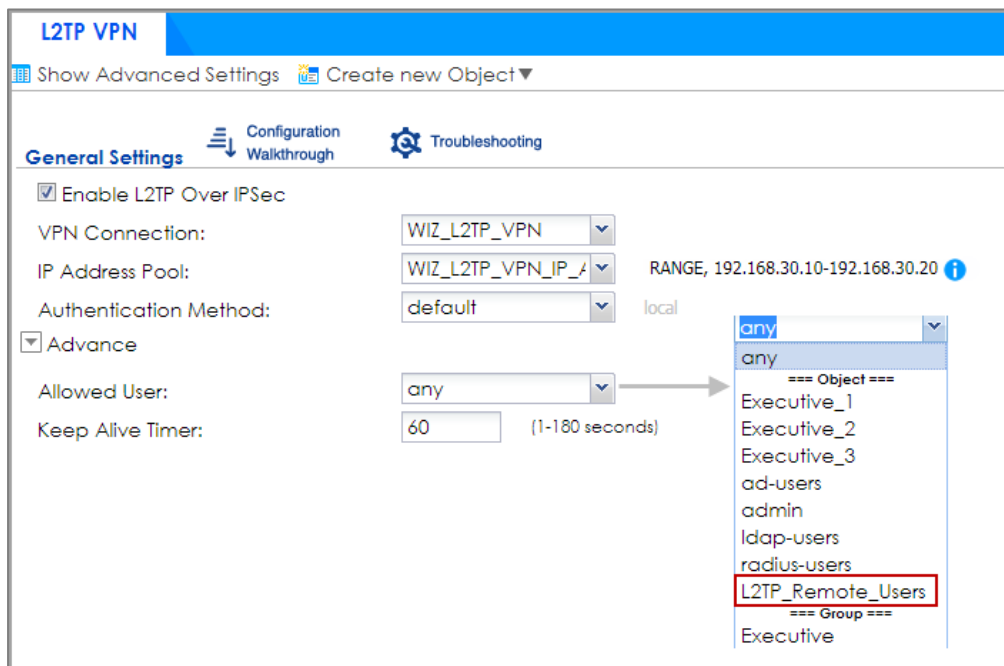
Reauthentication Time:

1440

minutes

OK

Cancel



Set Up the L2TP VPN Tunnel on the Apple MAC OS X 10.11 El Capitan Operating System

To configure L2TP VPN in OS X 10.11 operation system, go to **System Preferences...**
> Network, click the "+" button at the bottom left of the connections to add a new connection and configure as follows.

Set the **Interface** to be **VPN**, select **VPN Type** to be **L2TP over IPSec**.

Configure **Service Name** for you to identify the VPN configuration. Click **Create**.

Select the interface and enter a name for the new service.

Interface:

VPN Type:

Service Name:

Configure **Server Address** to be the ZyWALL/USG's WAN IP address (172.124.163.150 in this example). Enter **Account Name** which should be the same as **Allowed User** created in ZyWALL/USG (L2TP_Remote_Users in this example). Then, click **Authentication Settings....**

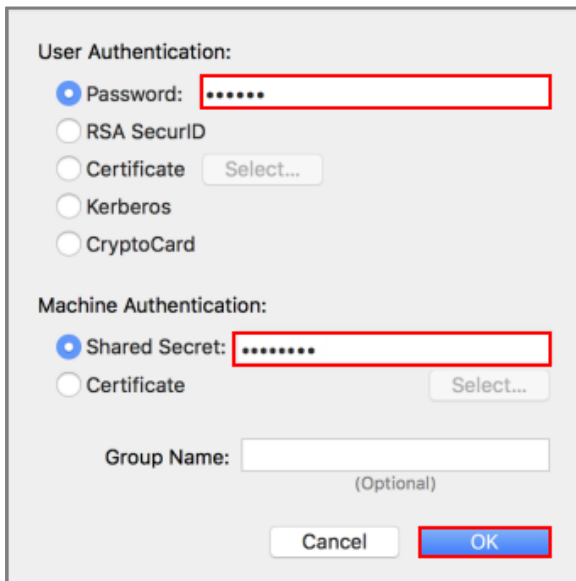
Configuration:

Server Address:

Account Name:

In the **User Authentication** section, enter **Password** which should be the same as **Allowed User** created in ZyWALL/USG (zyx123 in this example).

In the **Machine Authentication** section, enter **Shared Secret** to be the pre-shared key of the IPSec VPN gateway the ZyWALL/USG uses for L2TP VPN over IPSec (zyx12345 in this example). Click **OK**.



User Authentication:

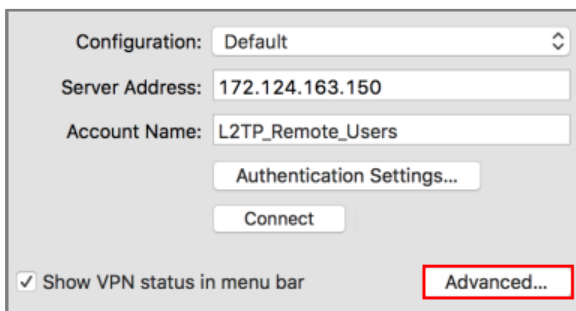
- ☒ Password:
- ☐ RSA SecurID
- ☐ Certificate
- ☐ Kerberos
- ☐ CryptoCard

Machine Authentication:

- ☒ Shared Secret:
- ☐ Certificate

Group Name:
(Optional)

Go back to **Configuration** and click **Advanced....** Select **Send all traffic over VPN connection** to allow the L2TP/IPSec VPN traffic between ZyWALL/USG and MAC OS X system.

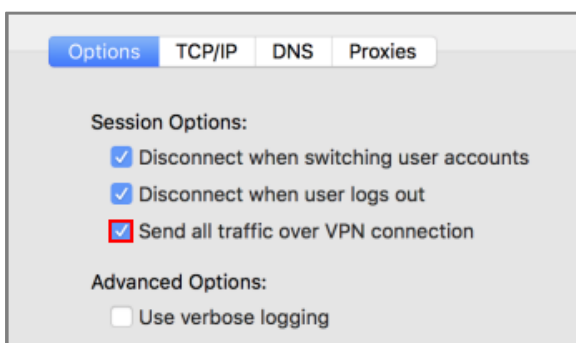


Configuration:

Server Address:

Account Name:

☒ Show VPN status in menu bar



Options TCP/IP DNS Proxies

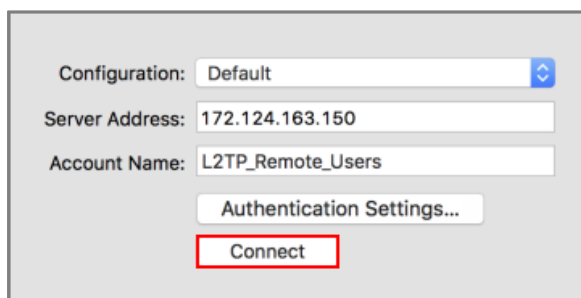
Session Options:

- ☒ Disconnect when switching user accounts
- ☒ Disconnect when user logs out
- ☒ Send all traffic over VPN connection

Advanced Options:

- ☐ Use verbose logging

Go back to **Configuration** and click **Connect**.



Configuration: Default

Server Address: 172.124.163.150

Account Name: L2TP_Remote_Users

Authentication Settings...

Connect

Test the L2TP over IPSec VPN Tunnel

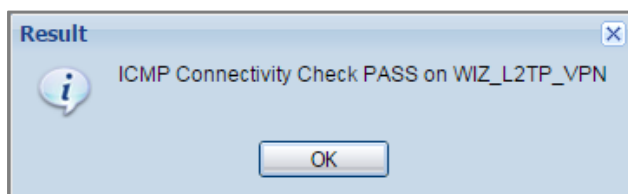
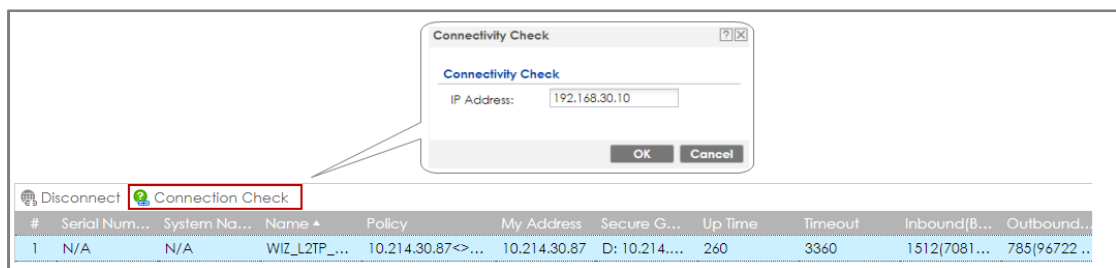
Go to ZyWALL/USG **CONFIGURATION** > **VPN** > **IPSec VPN** > **VPN Connection**, the **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

| # | Status | Name | VPN Gateway | Policy |
|---|--------|--------------------|--------------------|---|
| 1 | | VPN_to_VPC | VPN_to_VPC | VPN_to_VPC_LOCAL/VPN_to_V... |
| 2 | | VPN_to_Azure | VPN_to_Azure | VPN_to_Azure_LOCAL/VPN_to_... |
| 3 | | Hub_HQ_to_Branch_A | Hub_HQ_to_Branch_A | VPN_to_VPC_LOCAL/Spoke_Bra... |
| 4 | | Hub_HQ_to_Branch_B | Hub_HQ_to_Branch_B | Hub_HQ/Spoke_Branch_B_LOCAL |
| 5 | | Spoke_Branch_A | Spoke_Branch_A | Spoke_Branch_A_LOCAL/Hub_HQ |
| 6 | | Spoke_Branch_B | Spoke_Branch_B | Spoke_Branch_B_LOCAL/Hub_HQ |
| 7 | | WIZ_VPN_Branch | WIZ_VPN_Branch | WIZ_VPN_Branch_LOCAL/WIZ_V... |
| 8 | | WIZ_L2TP_VPN | WIZ_L2TP_VPN | WIZ_L2TP_VPN_LOCAL/ |

Go to ZyWALL/USG **MONITOR** > **VPN Monitor** > **IPSec** and verify the tunnel **Up Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic. Click **Connectivity Check** to verify the result of ICMP Connectivity.

MONITOR > VPN Monitor > IPSec > WIZ_L2TP_VPN



功能有問題無法截圖, connectivity check fail

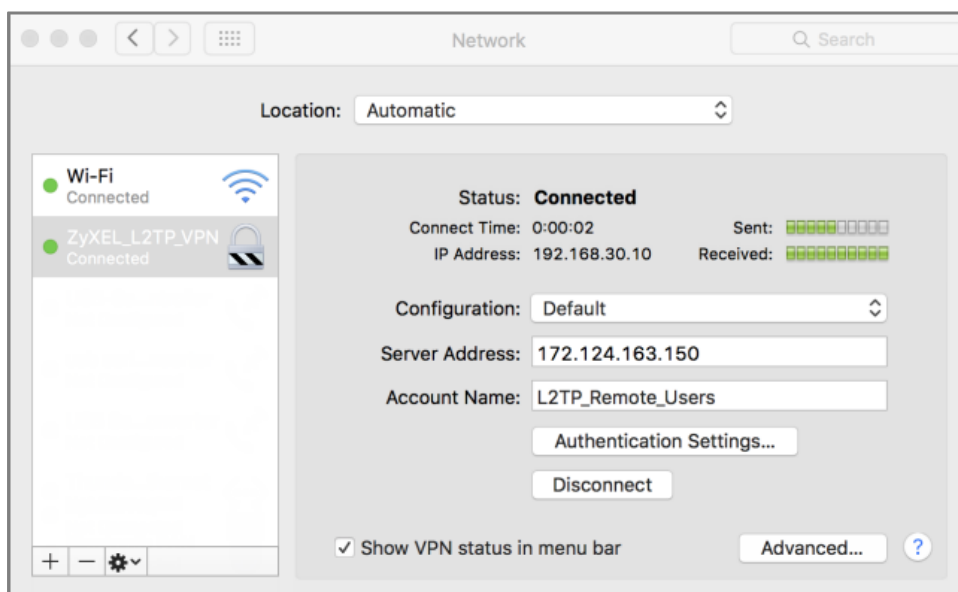
Go to ZyWALL/USG **MONITOR > VPN Monitor > L2TP over IPSec** and verify the **Current L2TP Session**.

MONITOR > VPN Monitor > L2TP over IPSec > L2TP_Remote_Users

| Current L2TP Session | | | | |
|---|-------------------|----------------|---------------|---------------|
| <div> Disconnect Refresh </div> | | | | |
| # | User Name | Hostname | Assigned IP | Public IP |
| 1 | L2TP_Remote_Users | Apple_MAC_OS_X | 192.168.30.10 | 36.226.103.25 |

Go to MAC OS X **System Preferences... > Network** and show **Connected** status, **Connect Time** and assigned **IP Address**.

System Preferences... > Network



What Could Go Wrong?

If you see [alert] log message such as below, please check ZyWALL/USG L2TP **Allowed User** or **User/Group Settings**. Apple MAC OS X El Capitan operating system users must use the same **Username** and **Password** as configured in ZyWALL/USG to establish the L2TP VPN.

| # | Time | Priority | Category | Message | Note |
|---|------------|----------|------------------|---|----------|
| 6 | 2017-06... | alert | L2TP Over IPS... | User L2TP_Remote_Users has been denied from L2TP service.(Incorrect Username or Password) | L2TP_LOG |

If you see [info] or [error] log message such as below, please check ZyWALL/USG Phase 1 Settings. Apple MAC OS X El Capitan operating system users must use the same **Pre-Shared Key** as configured in ZyWALL/USG to establish the IKE SA.

| Priority | Category | Message | Note |
|----------|----------|--|---------|
| info | IKE | Send:[NOTIFY:INVALID_PAYLOAD_TYPE] | IKE_LOG |
| info | IKE | Invalid payload type in encrypted payload chain, possibly because of different pre-shared keys | IKE_LOG |

| Priority | Category | Message | Note |
|----------|----------|---|---------|
| info | IKE | [SA] : No proposal chosen | IKE_LOG |
| info | IKE | [ID] : Tunnel [WIZ_L2TP_VPN] Phase 1 Peer ID mismatch | IKE_LOG |

If you see that Phase 1 IKE SA process has completed but still get [info] log message as below, please check ZyWALL/USG Phase 2 Settings. ZyWALL/USG unit must set correct **Local Policy** to establish the IKE SA.

| Priority | Category | Message | Note |
|----------|----------|--|---------|
| info | IKE | Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN] | IKE_LOG |
| info | IKE | [SA] : No proposal chosen | IKE_LOG |
| info | IKE | [ID] : Tunnel [WIZ_L2TP_VPN] Phase 2 Local policy mismatch | IKE_LOG |
| info | IKE | Recv:[HASH][SA][NONCE][ID][ID] | IKE_LOG |
| info | IKE | Phase 1 IKE SA process done | IKE_LOG |

| Priority | Category | Message | Note |
|----------|----------|--|---------|
| info | IKE | Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN] | IKE_LOG |
| info | IKE | [SA] : No proposal chosen | IKE_LOG |
| info | IKE | [SA] : Tunnel [WIZ_L2TP_VPN] Phase 2 proposal mismatch | IKE_LOG |
| info | IKE | Recv:[HASH][SA][NONCE][ID][ID] | IKE_LOG |
| info | IKE | Phase 1 IKE SA process done | IKE_LOG |

Ensure that the L2TP Address Pool does not conflict with any existing LAN1, LAN2, DMZ, or WLAN zones, even if they are not in use.

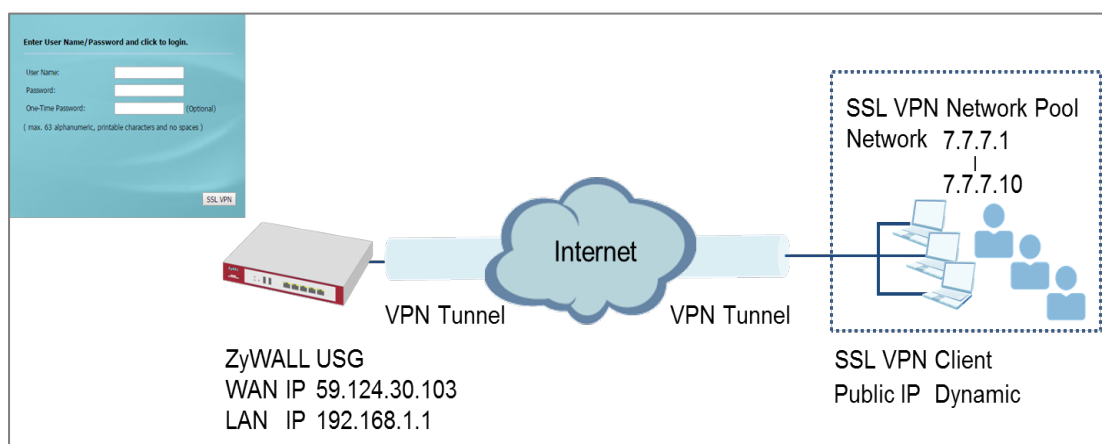
If you cannot access devices in the local network, verify that the devices in the local network set the USG's IP as their default gateway to utilize the L2TP tunnel.

Make sure the ZyWALL/USG units' security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

Verify that the Zone is set correctly in the Zone object. This should be set to IPSec_VPN Zone so that security policies are applied properly.

How to configure if I want user can only see SSL VPN Login button in web portal login page

This example shows how to strict portal access for SSL VPN clients. The example instructs how to allow end users to only see the SSL VPN Login button in the web portal login screen and the administrator can only manage the device from LAN.



ZyWALL/USG only see SSL VPN Login button in web portal login page

Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG60 (Firmware Version: ZLD 4.25).

Set Up the DNS Service

In this scenario, you need to have a DNS host to fulfill the requirement. In this example, go to <https://www.noip.com/> to register an account and create a DNS host. The following mapping IP address is the public IP of the ZyWALL/USG's WAN IP address.

Set Up the ZyWALL/USG SSL VPN Setting

In the ZyWALL/USG, go to **CONFIGURATION > VPN > SSL VPN > Global Setting > SSL VPN Login Domain Name** and type in the DNS domain name.

CONFIGURATION > VPN > SSL VPN > Global Setting > SSL VPN Login Domain Name

| | | |
|----------------------------------|---|------------|
| Global Settings | | |
| Network Extension Local IP: | <input type="text" value="192.168.200.1"/> | |
| SSL VPN Login Domain Name | | |
| SSL VPN Login Domain Name 1 | <input type="text" value="zyxetestssl.ddns.net"/> | (Optional) |
| SSL VPN Login Domain Name 2 | <input type="text"/> | (Optional) |
| Message | | |
| Login Message: | <input type="text" value="Welcome to SSL VPN"/> | |
| Logout Message: | <input type="text" value="Goodbye to SSL VPN"/> | |

Use SSL VPN, you need to allow users to access the **HTTPS** service. Go to **CONFIGURATION > Security Policy > Policy Control**. Make sure the security policy allows **HTTPS** traffic from the **WAN** interface to the **ZyWALL** (the example shows the default settings).

CONFIGURATION > Security Policy > Policy Control

General Settings

☒ Enable Policy Control

IPv4 Configuration

☐ Allow Asymmetrical Route

+ Add Edit Remove Activate Inactivate Move Clone

| Pri... | St... | Name | From | To | IPv4 Sour... | IPv4 Des... | Service | User | Schedule | A... | Log | UTM Profile |
|--------|-------|------------------|-----------|-------------|--------------|-------------|---------|------|----------|--------|-----|-------------|
| 1 | | LAN1_Outgoing | LAN1 | any (Exc... | any | any | any | any | none | all... | no | |
| 2 | | LAN2_Outgoing | LAN2 | any (Exc... | any | any | any | any | none | all... | no | |
| 3 | | DMZ_to_WAN | DMZ | any (Exc... | any | any | any | any | none | all... | no | |
| 4 | | IPSec_VPN_Ou... | IPSec_... | any (Exc... | any | any | any | any | none | all... | no | |
| 5 | | SSL_VPN_Outg... | SSL_VPN | any (Exc... | any | any | any | any | none | all... | no | |
| 6 | | TUNNEL_Outgo... | TUNNEL | any (Exc... | any | any | any | any | none | all... | no | |
| 7 | | LAN1_to_Device | LAN1 | ZyWALL | any | any | any | any | none | all... | no | |
| 8 | | LAN2_to_Device | LAN2 | ZyWALL | any | any | any | any | none | all... | no | |
| 9 | | DMZ_to_Device | DMZ | ZyWALL | any | any | Default | any | none | all... | no | |
| 10 | | WAN_to_Device | WAN | ZyWALL | any | any | Default | any | none | all... | no | |
| 11 | | IPSec_VPN_to_... | IPSec_... | ZyWALL | any | any | any | any | none | all... | no | |

Apply Reset

Default_Allow_WAN_To_ZyWALL
Description: System Default Allow From WAN To ZyWALL
Members: AH ESP HTTPS IKE NAT GRE VRRP

Set Up the ZyWALL/USG System Setting

Go to **CONFIGURATION > System > WWW > Admin Service Control > Add Admin**

ACL Rule 1. Set the address access action as **Deny** for **ALL** address in **WAN**.

CONFIGURATION > System > WWW > Admin Service Control > Add Admin ACL Rule 1

+ [HTTPS] Add Admin ACL Rule1

Create new Object ▼

Address Object: ALL

Zone: WAN

Action: Deny

OK Cancel

HTTPS

☒ Enable

Server Port: 443

☐ Authenticate Client Certificates (See Trusted CAs)

Server Certificate: default

☒ Redirect HTTP to HTTPS

Admin Service Control

+ Add Edit Remove Move

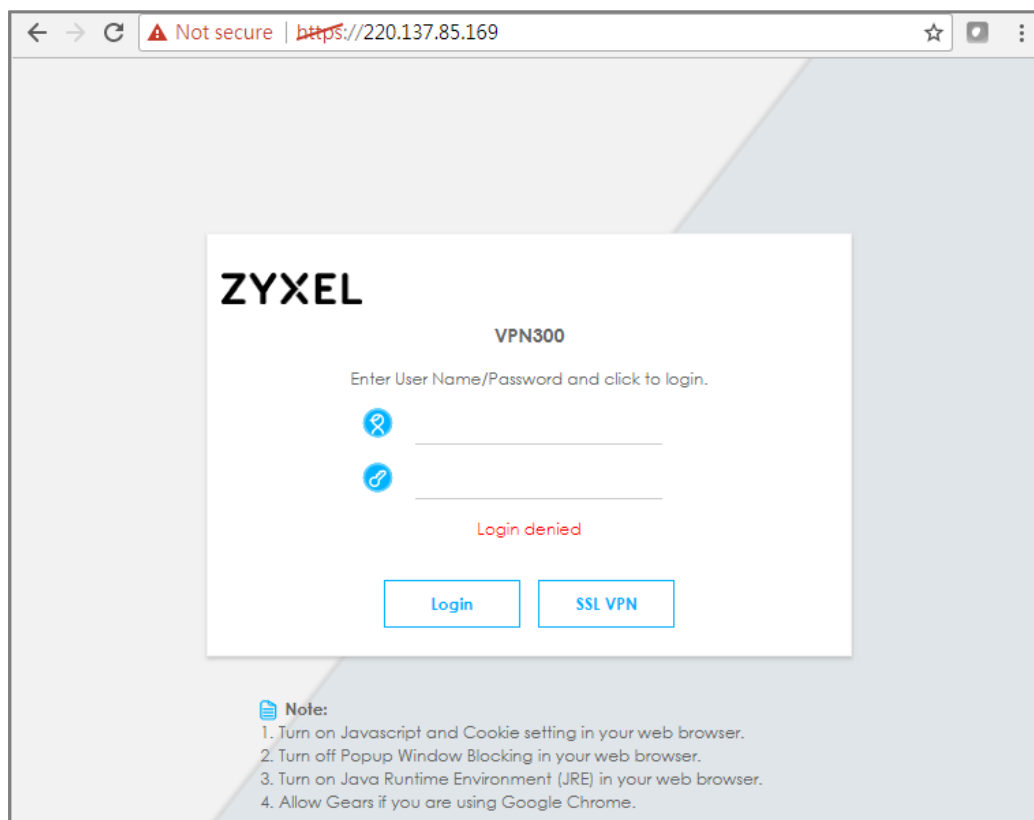
| # | Zone | Address | Action |
|---|------|---------|--------|
| 1 | WAN | ALL | deny |
| - | ALL | ALL | accept |

Page 1 of 1 Show 50 items Displaying 1 - 2 of 2

Test the SSL VPN

Type in the URL (<https://sslvpnzyxelttest.ddns.net>) and you will only see the **SSL VPN Login** button in the web portal screen.

Type in the URL (<https://sslvpnzyxelttest.ddns.net>)



Login to the device via the WAN interface with the administrator's user name and password. The screen will show **Login denied**.


Login to the device via the WAN interface


← → ↻ ⚠ Not secure | <https://220.137.85.169> ☆ 📺 ⋮

ZYXEL

VPN300

Enter User Name/Password and click to login.





Login denied

LoginSSL VPN

Note:

1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.
4. Allow Gears if you are using Google Chrome.

Login to the device via the LAN interface with the administrator's user name and password. The management portal will be displayed.

Login to the device via the LAN interface

ZYXEL VPN300

Enter User Name/Password and click to login.

Username:

Password:

[Login](#) [SSL VPN](#)

Note:

1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.
4. Allow Gears if you are using Google Chrome.

ZYXEL VPN300

Logout Help About Site Map Object Reference CU

General VPN

CPU Usage: 12 %

Memory Usage: 21 %

Flash Usage: 9 %

USB Storage Usage: 0/0 MB

Active Sessions: 61/2000000

DHCP Table: 2 Host(s)

Device HA: 000 Switch Counter

Virtual Device

ZYXEL VPN300 VPN Firewall

USB: 1 2 LINK ACT

P1 P2 P3 P4 10 / 100 / 1000 P5 P6 P7 P8

Device Information

| | |
|---------------------------------------|---|
| System Name | Boot Status |
| VPN300 | OK |
| Serial Number | Firmware Version |
| S172L15290016 | V4.30(ABFC.0)b1s1 / 2017-06-09 21:43:11 |
| MAC Address Range | Firmware Upgrade License |
| BB:EC:A3:A9:C0:0B ~ BB:EC:A3:A9:C0:12 | Not Licensed |
| System Uptime | Current Date/Time |
| 02:57:33 | 2017-07-07 / 06:23:43 UTC+00:00 |

Tx/Rx Statics Port Selection: P1

Go to **MONITOR > Log**. You can see that the admin login has been denied access from the WAN interface but it is allowed from the LAN interface.

MONITOR > Log

Logs

Category:

User

Email Log Now

Refresh

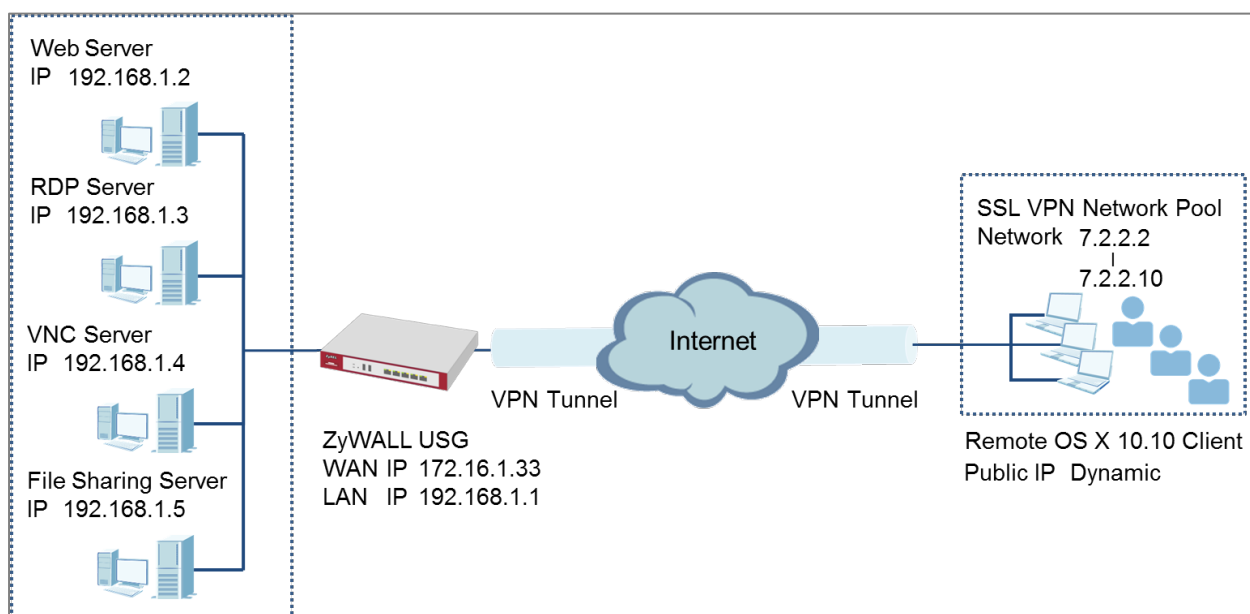
Clear Log


| Priority | C... | Message | Source | Destination | Note |
|----------|------|--|-------------------|------------------|----------------|
| notice | User | Administrator admin(MAC=00:16:36:2B:B4:2F) from http/https has logged out Device | 192.168.1.34 | 192.168.1.1 | Account: admin |
| notice | User | Administrator admin(MAC=00:16:36:2B:B4:2F) from http/https has logged in Device | 192.168.1.34 | 192.168.1.1 | Account: admin |
| notice | User | User admin has been denied access from HTTPS | 10.214.30.55:5... | 10.214.30.90:443 | Account: admin |

How to Deploy SSL VPN with Apple Mac OS X 10.10 Operating System

This is an example of using the ZyWALL/USG SSL VPN client software in Apple MAC OS X 10.10 Yosemite operating systems for secure connections to the network behind the ZyWALL/USG. When the VPN tunnel is configured, users can securely access the network from a Mac OS X 10.11 Yosemite computer.

ZyWALL/USG SSL VPN with Apple MAC OS X 10.10 Yosemite

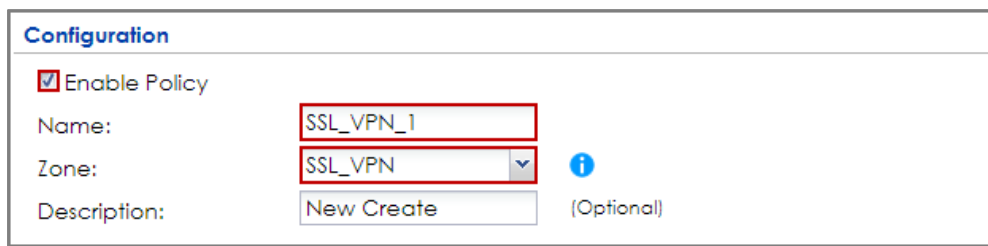


 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG110 (Firmware Version: ZLD 4.25) and Apple MAC (Version: OS X10.10 Yosemite).

Set Up the SSL VPN Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > VPN > SSL VPN > Access Privilege** to add an **Access Policy**. Configure a **Name** for you to identify the SSL VPN configuration.

CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > Configuration



Configuration

☒ Enable Policy

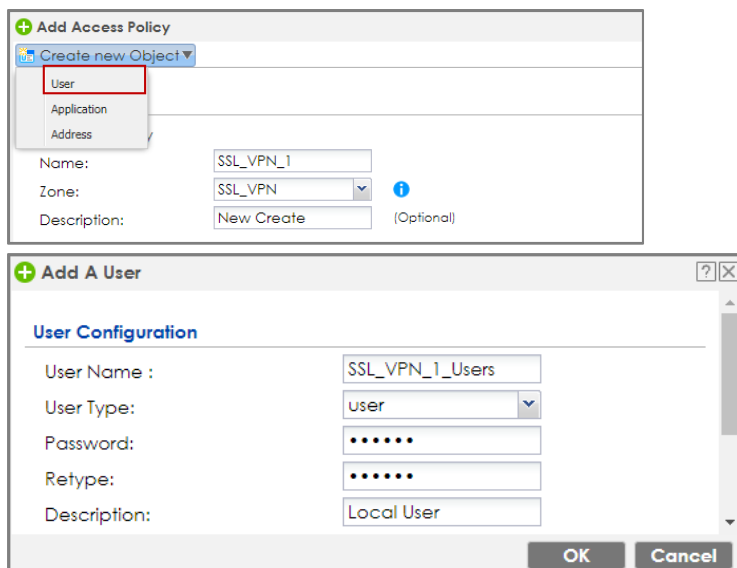
Name:

Zone:

Description: (Optional)

Go to **Create new Object > User** to add **User Name** (SSL_VPN_1_Users in this example) and **Password** (4-24 characters, zyx168 in this example), click **OK**.

CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > Create new Object > User



Add Access Policy

Create new Object

User

Application

Address

Name:

Zone:

Description: (Optional)

Add A User

User Configuration

User Name :

User Type:

Password:

Retype:

Description:

OK Cancel

Go to **Create new Object > Application** to add servers you allow **SSL_VPN_1_Users** to access, click **OK**.

CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > Create new Object > Application

The image displays four instances of the 'Add SSL Application' dialog box, each showing a different configuration for a new application object.

- Top Left:** 'Web Application' type, 'Web Server' server type, Name: 'Internal_Server', URL: 'http://192.168.1.2'. 'Web Page Encryption' is checked.
- Top Right:** 'Web Application' type, 'RDP' server type, Name: 'RDP', Server Address(es): '192.168.1.3' (User Defined).
- Bottom Left:** 'File Sharing' type, Name: 'File_Share', Shared Path: '\\192.168.1.5\\Internal'.
- Bottom Right:** 'Web Application' type, 'VNC' server type, Name: 'VNC', Server Address(es): '192.168.1.4' (User Defined).

Go to **Create new Object > Address** to add the IP address pool for **SSL_VPN_1_Users**.

CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > Create new Object > Address

The image shows two related configuration windows.

- Left Window (Edit Access Policy):** The 'Create new Object' dropdown is open, and 'Address' is selected. The 'Name' field contains 'SSL_VPN_1', 'Zone' is 'SSL_VPN', and 'Description' is 'New Create'.
- Right Window (Add Address Rule):** 'Name' is 'SSL_VPN_POOL', 'Address Type' is 'RANGE', 'Starting IP Address' is '7.2.2.2', and 'End IP Address' is '7.2.2.10'.

Then, move the just created address object to **Selected User/Group Objects**.

Similarly, in **SSL Application List (Optional)** move the servers you want available to SSL users to **Selected Appellation Objects**.

CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > User/Group & SSL Application

User/Group

Selectable User/Group Objects

billing-users

ua-users

trial-users

L2TP_Remote_Users

SSL_VPN_1_Users

→

←

Selected User/Group Objects

SSL Application List (Optional)

Selectable Application Objects

Internal_Server

RDP

VNC

File_Share

→

←

Selected Application Objects

Scroll down to **Network Extension (Optional)** to select **Enable Network Extension** to allow SSL VPN users to access the resources behind the ZyWALL/USG local network.

Select network(s) name in the **Selectable Address Objects** list and click the right arrow button to add to the **Selected Address Objects** list. You can select more than one network.

CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > Network Extension (Optional)

Network Extension (Optional)

☒ Enable Network Extension (Full Tunnel Mode)

☐ Force all client traffic to enter SSL VPN tunnel ⓘ

☐ NetBIOS broadcast over SSL VPN Tunnel

Assign IP Pool: SSL_VPN_POOL ⓘ RANGE 7.2.2.2-7.2.2.10

DNS Server 1: none

DNS Server 2: none

WINS Server 1: none

WINS Server 2: none

Network List

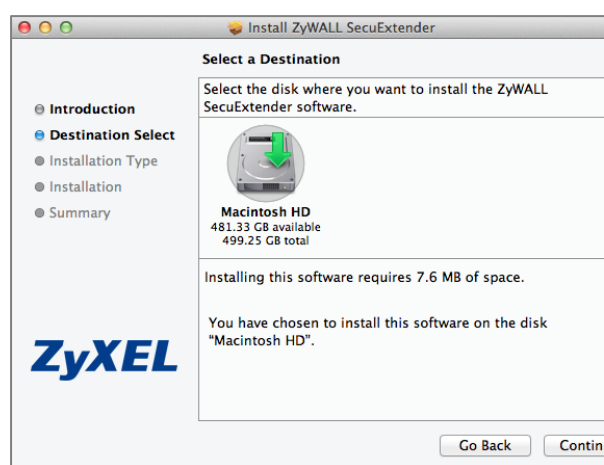
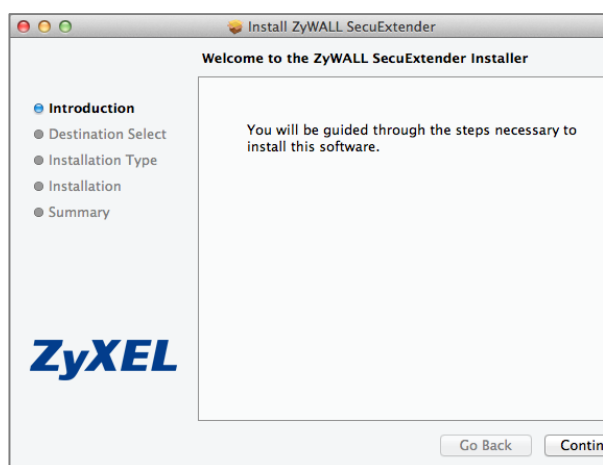
Selectable Address Objects

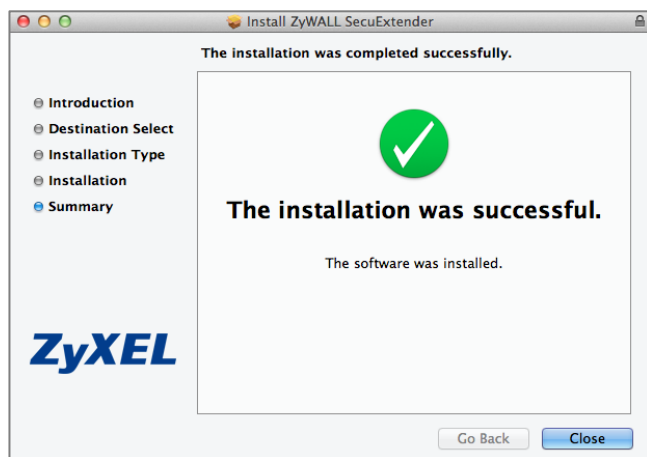
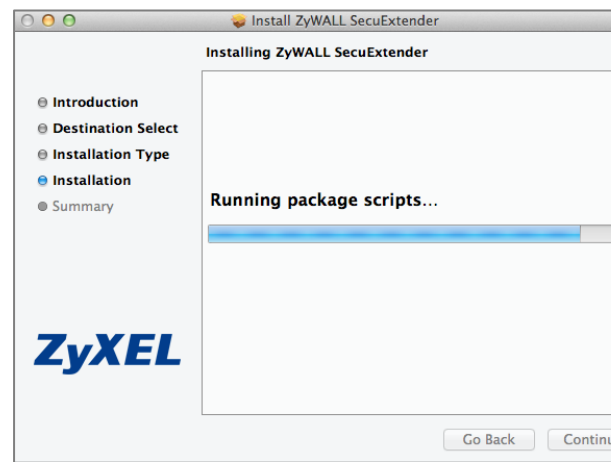
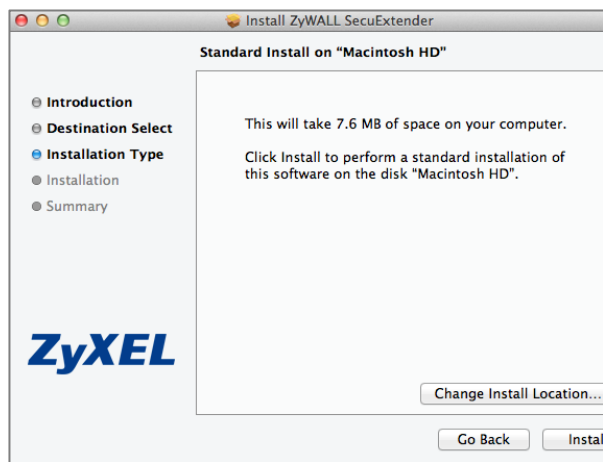
- DMZ_SUBNET
- IP6to4-Relay
- LAN1_SUBNET**
- LAN2_SUBNET
- RFC1918_1

Selected Address Objects

Set Up the SSL VPN Tunnel on the Apple MAC OS X 10.10 Operating System

Download SSL VPN Client software: **ZyWALL SecuExtender** for MAC from the ZyXEL Global Website and double-click on the downloaded file to install it.





Go to **ZyWALL SecuExtender > Preferences**, click the "+" button at the bottom left to add a new SSL VPN connection.



Configure the **Connection Name** for you to identify the SSL VPN configuration.
Then, set the **Remote Server Address** to be the WAN IP of ZyWALL/USG (172.16.1.33 in this example). Click **Save**.



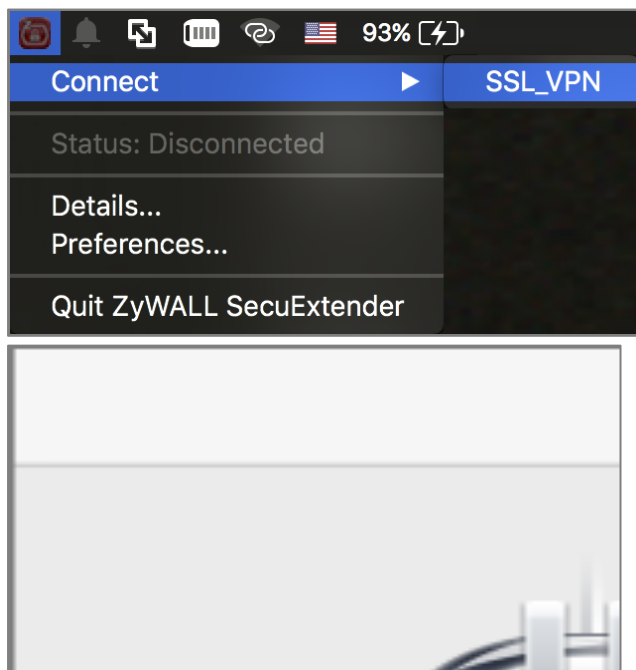
Here are two methods to initiate SSL VPN connections:

From ZyWALL SecuExtender

From a Web Browser

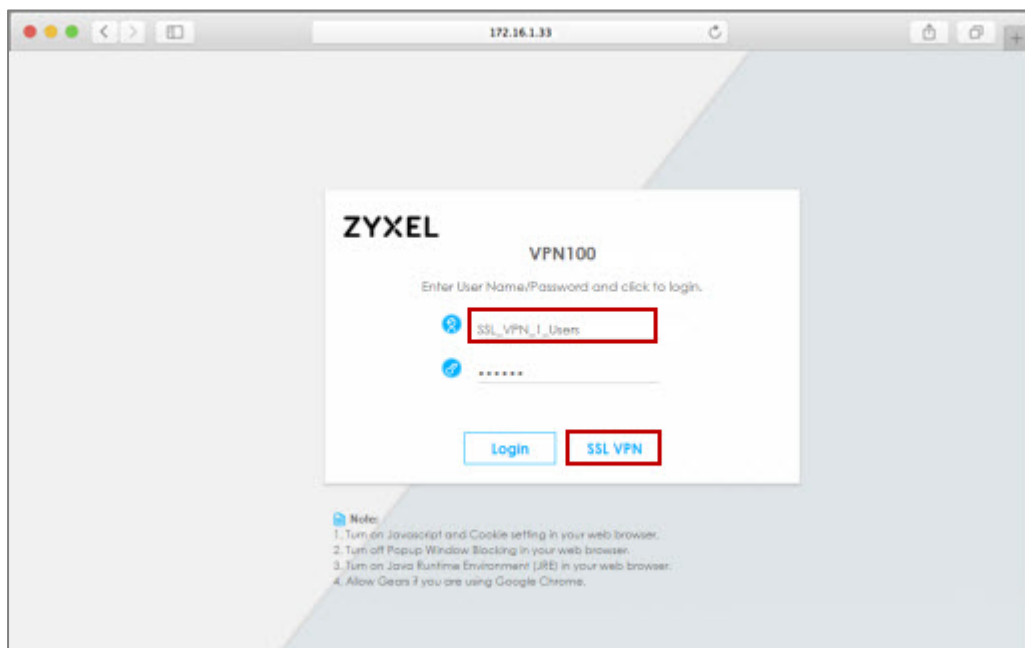
From ZyWALL SecuExtender

Go to **ZyWALL SecuExtender > Connect > SSL_VPN**, to display the username and password dialog box. Set **Username** and **Password** to be the same as your ZyWALL/USG SSL VPN **Selected User/Group** name and password (SSL_VPN_1_Users/zyx168 in this example).



From a Web Browser

Type ZyWALL/USG's WAN IP into the browser, to display the login screen. Enter **User Name** and **Password** to be the same as your ZyWALL/USG SSL VPN **Selected User/Group** name and password (SSL_VPN_1_Users/zyx168 in this example). Click **SSL VPN**.



Test the SSL VPN Tunnel

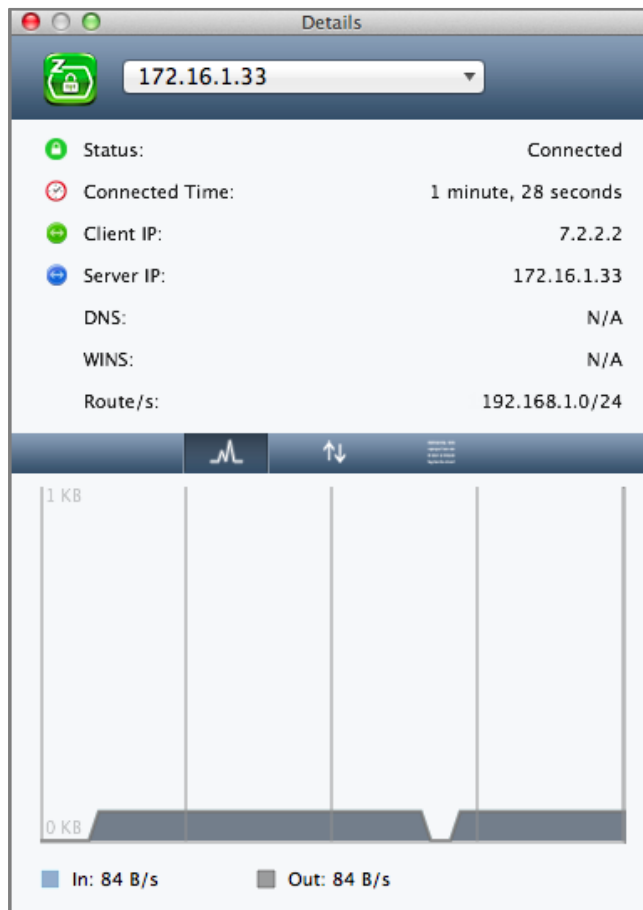
Go to ZyWALL/USG **MONITOR** > **VPN Monitor** > **SSL** and verify the tunnel **Login Address**, **Connected Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic.

MONITOR > **VPN Monitor** > **SSL** > **SSL_VPN_1_Users**

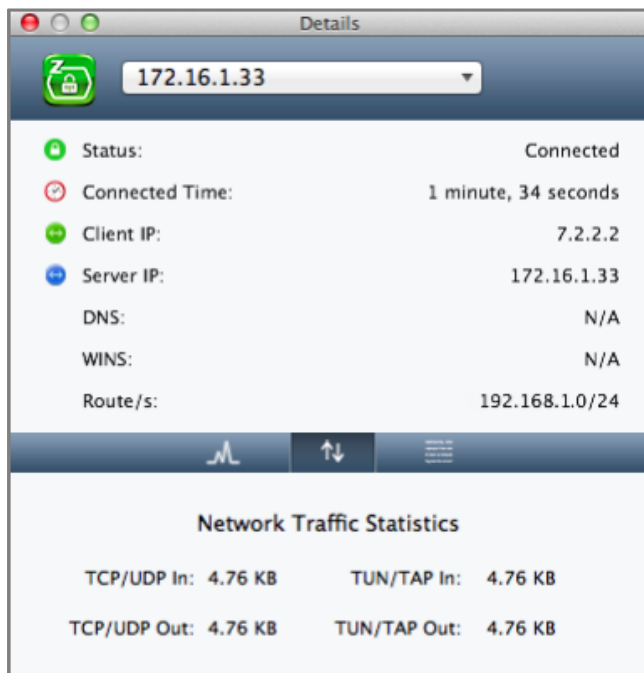
| Current SSL VPN Connection | | | | | | |
|--|-----------------|-------------------|---------------|----------------|----------------|-----------------|
| Disconnect Refresh | | | | | | |
| # | User | Access | Login Address | Connected Time | Inbound(Bytes) | Outbound(Bytes) |
| 1 | SSL_VPN_1_Users | Network-Extension | 10.214.30.104 | 00:01:39 | 9390 | 503 |

Go to **ZyWALL SecuExtender** > **Details** and check **Traffic Graph**, **Network Traffic Statics** and **Log Details**.

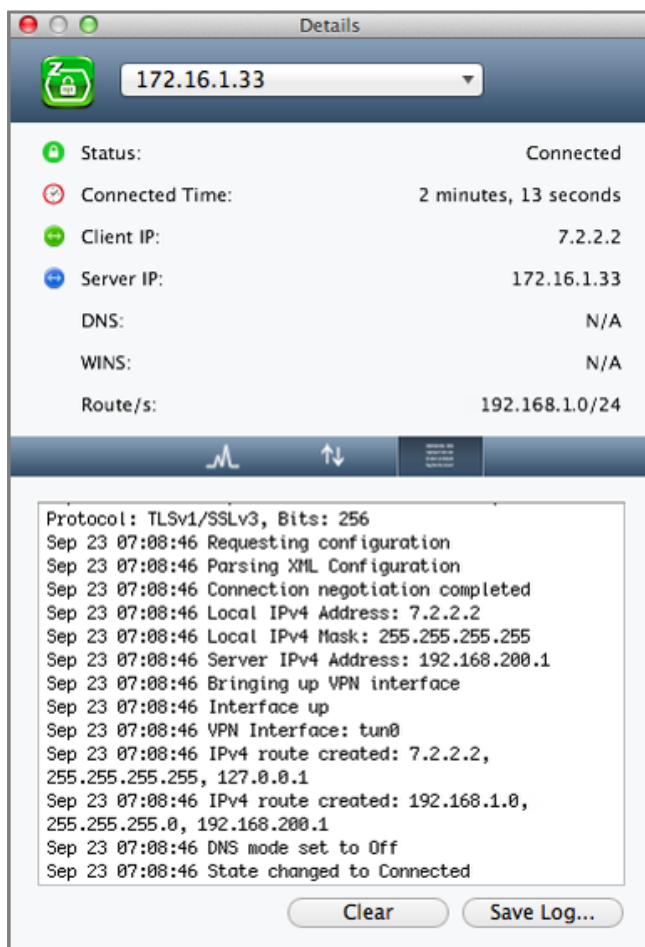
ZyWALL SecuExtender > Details > Traffic Graph



ZyWALL SecuExtender > Details > Network Traffic Statics



ZyWALL SecuExtender > Details > Log Details



What Could Go Wrong?

If you see [notice] or [alert] log message such as below, please check ZyWALL/USG SSL **Selected User/Group Objects** settings. MAC OS X 10.10 Yosemite users must use the same **Username** and **Password** as configured in ZyWALL/USG to establish the SSL VPN tunnel.

| Priority | Category | Message | Note |
|----------|----------|--|-----------------------|
| notice | SSL VPN | Failed login attempt to SSLVPN from http/https (incorrect password or inexistent username) | Account: SSL_VPN_1... |
| alert | User | Failed login attempt to Device from http/https (incorrect password or inexistent username) | Account: SSL_VPN_1... |

If you uploaded a logo to show in the SSL VPN user screens but it does not display properly, check that the logo graphic is in GIF, JPG, or PNG format. The graphic should use a resolution of 103 x 29 pixels to avoid distortion when displayed. The ZyWALL/USG automatically resizes a graphic of a different resolution to 103 x 29 pixels. The file size must be 100 kilobytes or less. Transparent background is recommended.

If users can log into the SSL VPN but cannot see some of the resource links check the SSL application object's configuration.

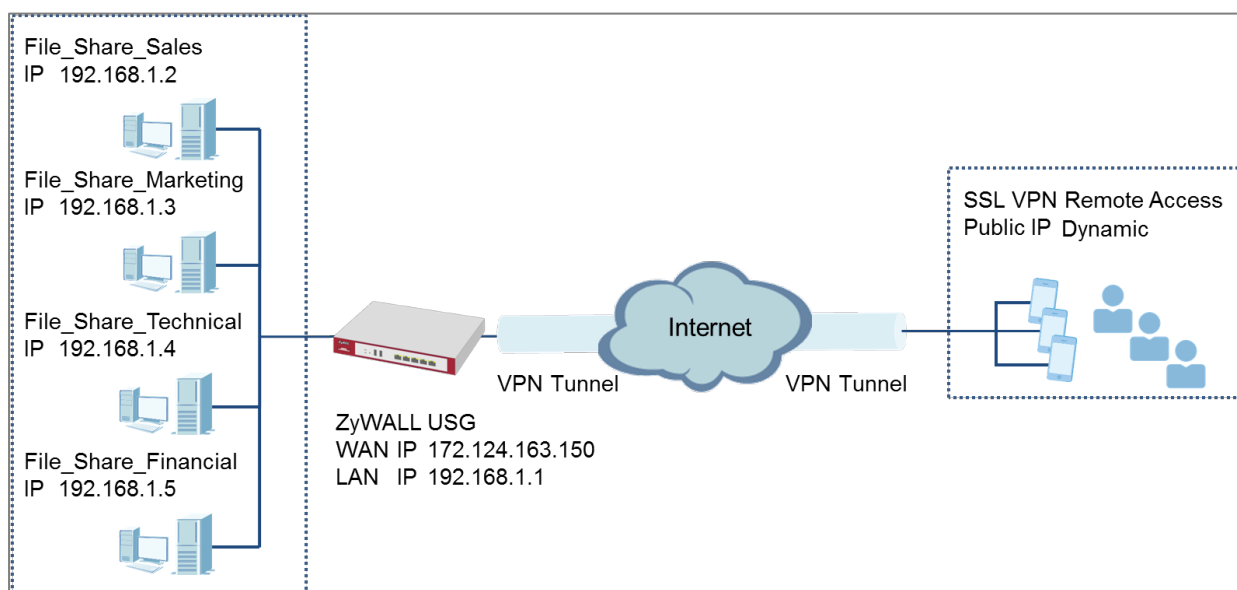
If the ZyWALL/USG redirects the user to the user aware screen, check whether the user account is included in an SSL VPN access policy or not.


Changing the HTTP/HTTPS configuration disconnects SSL VPN network extension sessions. Users need to re-connect if this happens.

How To Configure SSL VPN for Remote Access Mobile Devices

This is an example of using the ZyWALL/USG SSL VPN for remote access mobile devices to securely connect to the File Sharing Server behind the ZyWALL/USG.

ZyWALL/USG SSL VPN for Secure External Access to Network Resources




 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG1900 (Firmware Version: ZLD 4.25).

Set Up the SSL VPN Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > VPN > SSL VPN > Access Privilege** to add an **Access Policy**. Configure a **Name** for you to identify the SSL VPN configuration.

CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > Configuration

| Configuration | |
|---|---|
| <input checked="" type="checkbox"/> Enable Policy | |
| Name: | SSL_VPN_1 |
| Zone: | SSL_VPN  |
| Description: | New Create (Optional) |

Go to **Create new Object > User** to add **User Name** (SSL_VPN_1_Users in this example) and **Password** (4-24 characters, zyx168 in this example), click **OK**.

CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > Create new Object > User

+

Add Access Policy

Create new Object ▼

User

Application

Address

Name:

SSL_VPN_1

Zone:

SSL_VPN ▼

i

(Optional)

Description:

New Create

+

Add A User

?

✕

User Configuration

User Name :

SSL_VPN_1_Users

User Type:

user ▼

Password:

•••••

Retype:

•••••

Description:

Local User

OK

Cancel

Go to **Create new Object > Application** to add servers that you will allow **SSL_VPN_1_Users** to access. Click **OK**.

CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > Create new Object > Application

The image displays four instances of the 'Add SSL Application' dialog box, each showing a different configuration for a File Sharing application. Each dialog has a title bar with a green plus icon and a close button. Below the title bar is a 'Create new Object' button. The 'Object' section contains a 'Type' dropdown set to 'File Sharing'. The 'File Sharing' section contains 'Name' and 'Shared Path' text boxes. The configurations are as follows:

| Dialog | Name | Shared Path |
|--------------|----------------------|-------------------------|
| Top Left | File_Share_Sales | \\192.168.1.2\Sales |
| Top Right | File_Share_Marketing | \\192.168.1.3\Marketing |
| Bottom Left | File_Share_Technical | \\192.168.1.4\Technical |
| Bottom Right | File_Share_Financial | \\192.168.1.5\Financial |

Then, move the just created address object to **Selected User/Group Objects**.

Similarly, in **SSL Application List (Optional)** move the servers you want available to SSL users to **Selected Application Objects**.

CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > User/Group & SSL Application

This section contains four identical screenshots of the 'Add SSL Application' dialog box, identical to the ones in the previous section. Each dialog shows a 'File Sharing' application with a unique name and shared path. The configurations are as follows:

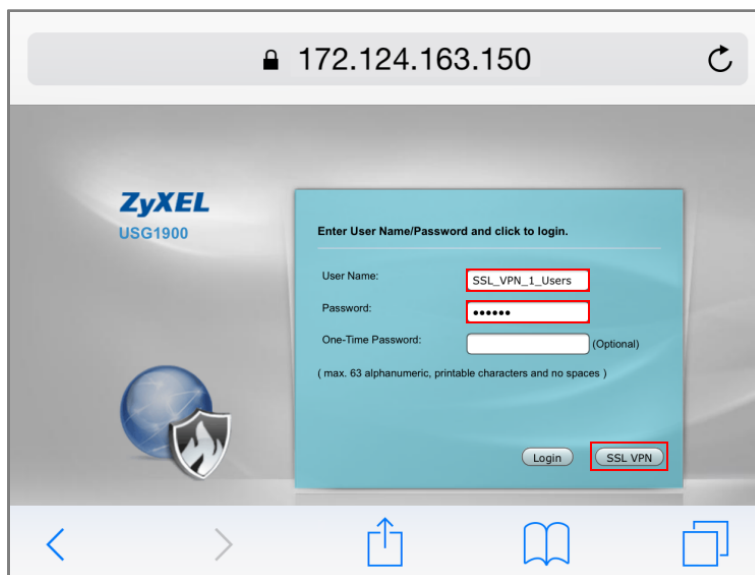
| Dialog | Name | Shared Path |
|--------------|----------------------|-------------------------|
| Top Left | File_Share_Sales | \\192.168.1.2\Sales |
| Top Right | File_Share_Marketing | \\192.168.1.3\Marketing |
| Bottom Left | File_Share_Technical | \\192.168.1.4\Technical |
| Bottom Right | File_Share_Financial | \\192.168.1.5\Financial |

Test the SSL VPN Tunnel

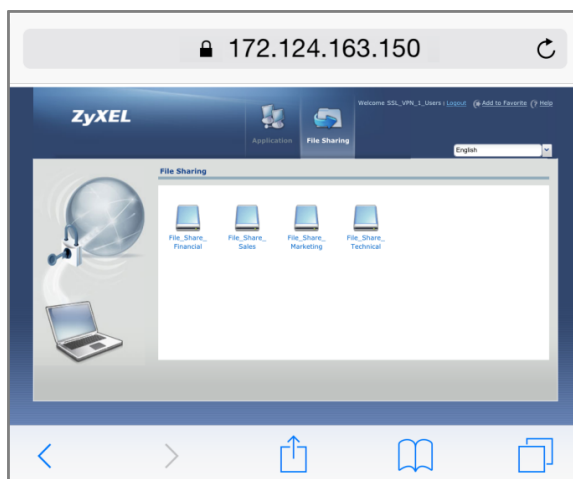
Type the ZyWALL/USG's WAN IP into the browser, then the login screen appears.

Enter **User Name** and **Password** to be the same as your ZyWALL/USG **SSL VPN**

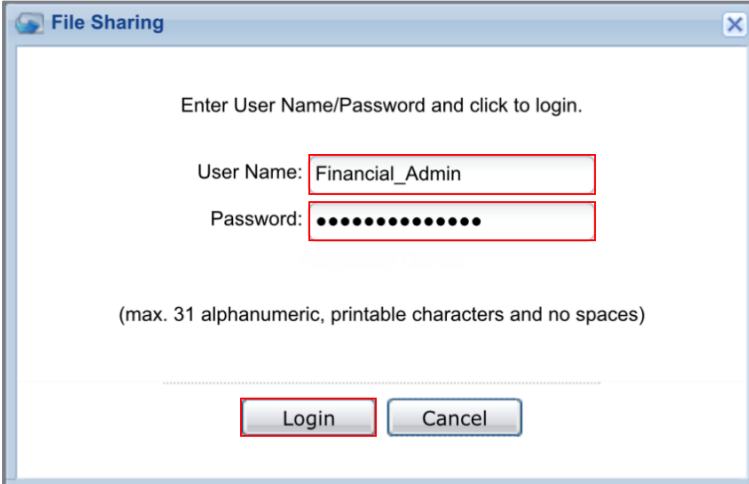
Selected User/Group name and password (SSL_VPN_1_Users/zyx168 in this example). Click **SSL VPN**.



The **File Sharing** server appears.



Click the **File Sharing** folder you want to access, enter **User Name/ Password** of your **File Sharing** server and click **Login**.



File Sharing

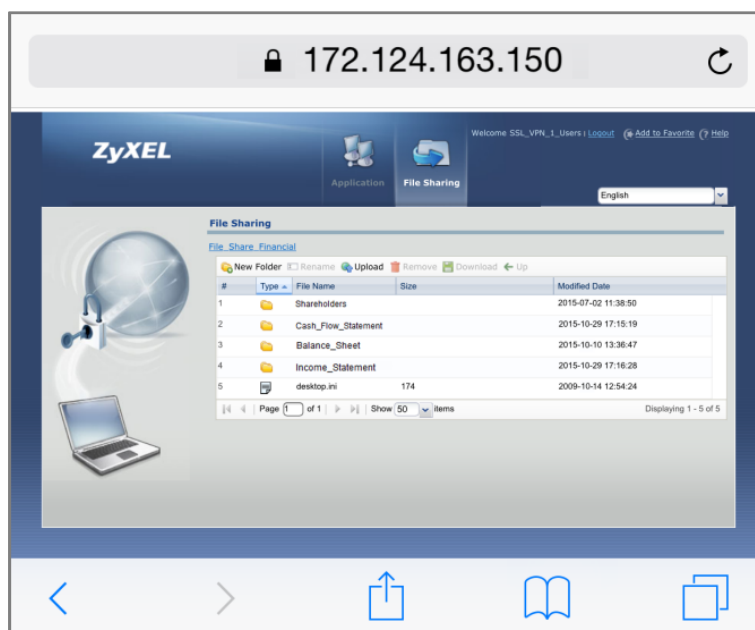
Enter User Name/Password and click to login.

User Name:

Password:

(max. 31 alphanumeric, printable characters and no spaces)

Now you can securely access the files.



What Could Go Wrong?

If you see [notice] or [alert] log message such as below, please check ZyWALL/USG SSL **Selected User/Group Objects** settings. Windows 10 users must use the same **Username** and **Password** as configured in ZyWALL/USG to establish the SSL VPN tunnel.

| Priority | Category | Message | Note |
|----------|----------|--|-----------------------|
| notice | SSL VPN | Failed login attempt to SSLVPN from http/https (incorrect password or inexistent username) | Account: SSL_VPN_1... |
| alert | User | Failed login attempt to Device from http/https (incorrect password or inexistent username) | Account: SSL_VPN_1... |

If you uploaded a logo to show in the SSL VPN user screens but it does not display properly, check that the logo graphic is in GIF, JPG, or PNG format. The graphic should use a resolution of 103 x 29 pixels to avoid distortion when displayed. The ZyWALL/USG automatically resizes a graphic of a different resolution to 103 x 29 pixels. The file size must be 100 kilobytes or less. Transparent background is recommended.

If users can log into the SSL VPN but cannot see some of the resource links check the SSL application object's configuration.

If the ZyWALL/USG redirects the user to the user aware screen, check whether the user account is included in an SSL VPN access policy or not.

Changing the HTTP/HTTPS configuration disconnects SSL VPN network extension sessions. Users need to re-connect if this happens.

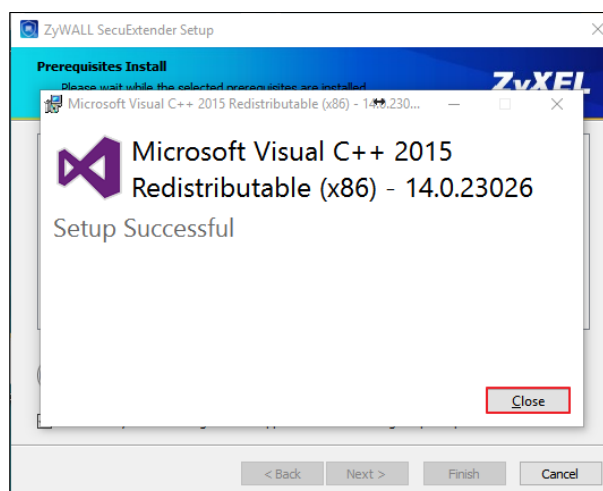
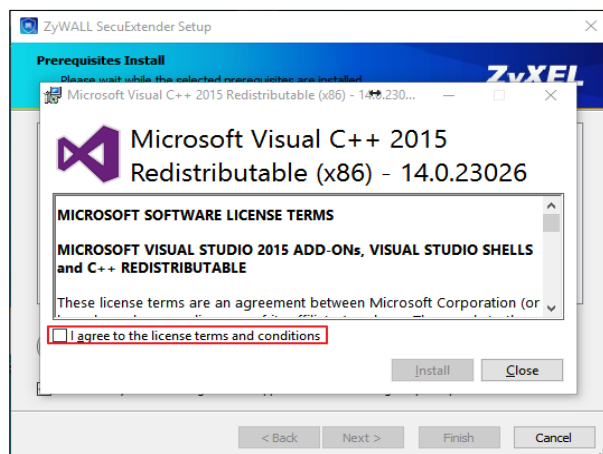
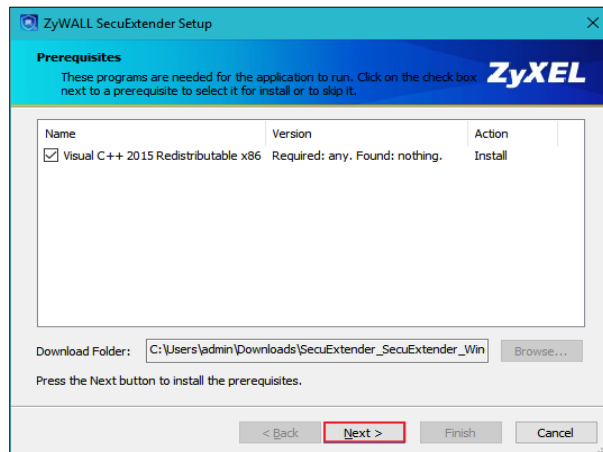
How to Configure an SSL VPN Tunnel (with SecuExtender version 4.0.0.1) on the Windows 10 Operating System

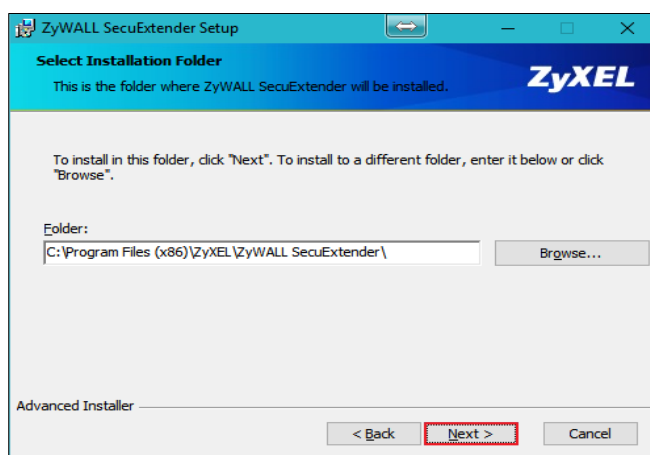
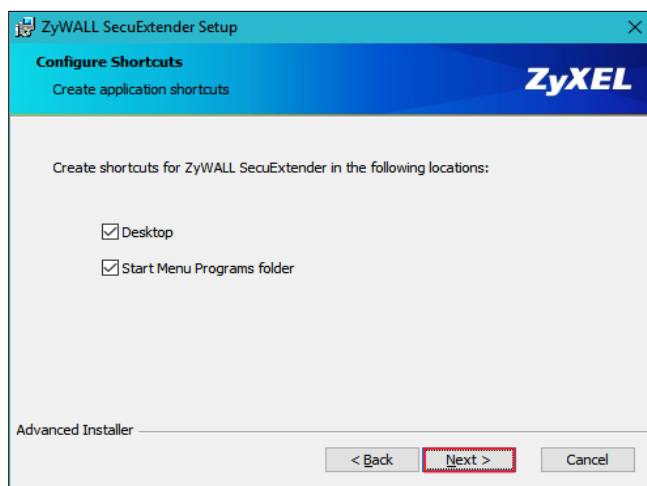
Set up the SSL VPN Tunnel with Windows 10

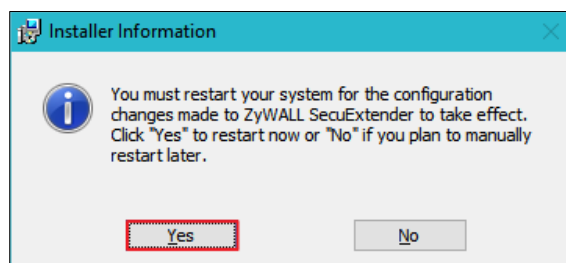
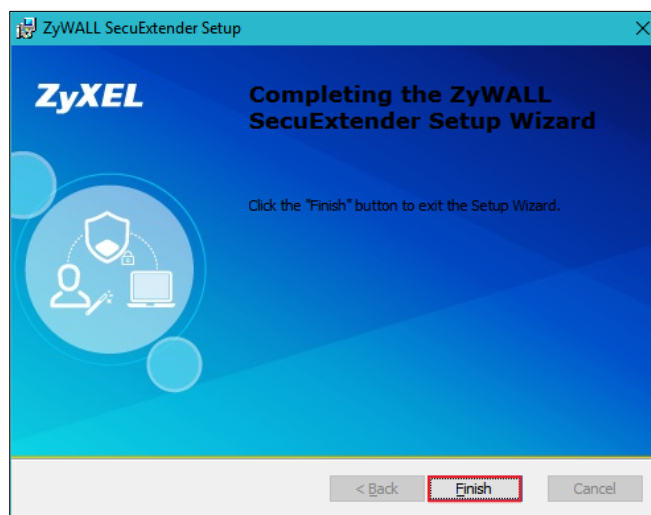
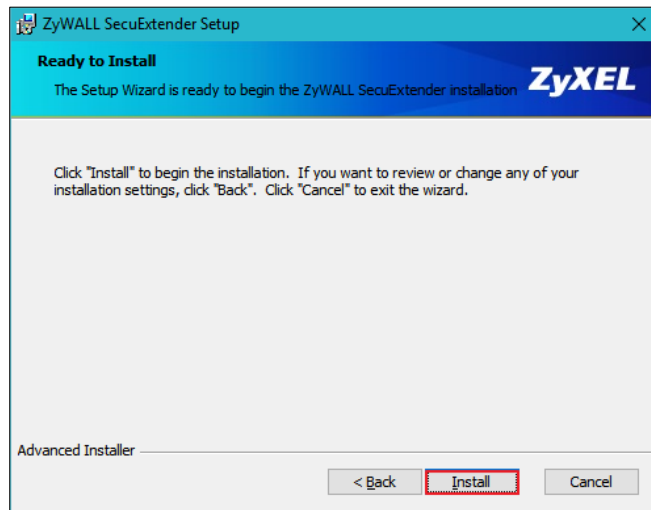
Please download SecuExtender version 4.0.0.1 from the download library of ZyXEL's official website.

| Model | Material | Version | OS | Checksum | Release Date | Release Note | Download |
|-------------------------|----------|------------------------------------|--|----------|--------------|--------------|----------|
| ZyWALL IPSec VPN Client | Software | ZyWALLIPSecVPNClient3.7204.6113 | Windows 7 32bit/ Windows 7 64bit/ Windows 8 32bit/ Windows 8 64bit/ Windows 10 32bit/ Windows 10 64bit | | May 24, 2017 | | |
| SecuExtender | Software | SecuExtender_MacOSX115 | Mac 10X/ MAC 10.8/ MAC 10.9/ MAC 10.10 | | Mar 15, 2017 | | |
| SecuExtender | Software | SecuExtender_Windows4.0.2.0 | Windows XP/ Windows 7 32bit/ Windows 7 64bit/ Windows 8 32bit/ Windows 8 64bit/ Windows 10 32bit/ Windows 10 64bit | | Jan 18, 2017 | | |

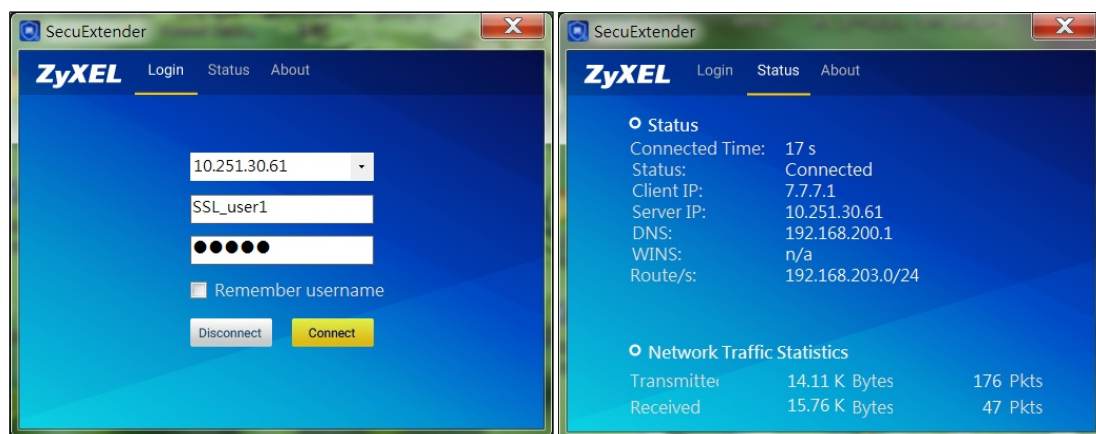
Before you start installing the SecuExtender, it is required to install the "Visual C++ 2015 Redistributable" package first. Click **Next**, select **I agree to the license terms and conditions**, and click **Install** to complete the Visual C++ 2015 Redistributable installation. After that, the setup wizard appears. Please note that the users need to reboot their systems after the SecuExtender installation is completed.







Double-click the shortcut icon on your desktop. It is the same as the SSL VPN standalone software on MAC OS X. Enter the server's IP or domain name, user name, and password to connect to the server. The example below shows that the client IP is **7.7.7.1** and you can also check the traffic statistic in the **Status** screen.



You can verify the connection status from the computer's taskbar icon.



When connected, the icon is blue.



When disconnected, the icon is red.

You can also use the USG monitor screen to check the login list of the users.

| Current User List | | | | | | |
|-------------------|-----------|---------------------|--------|----------------------|-------------------|-----------------|
| Force Logout | | | | | | |
| # | User ID | Reauth/Lease Time | Type | IP Address | MAC | User Info |
| 1 | SSL_user1 | 23:59:17 / 23:59:47 | SSLVPN | 10.251.30.56/7.7.7.1 | 3C:97:0E:30:0E:B8 | user(SSL_user1) |

What Can Go Wrong?

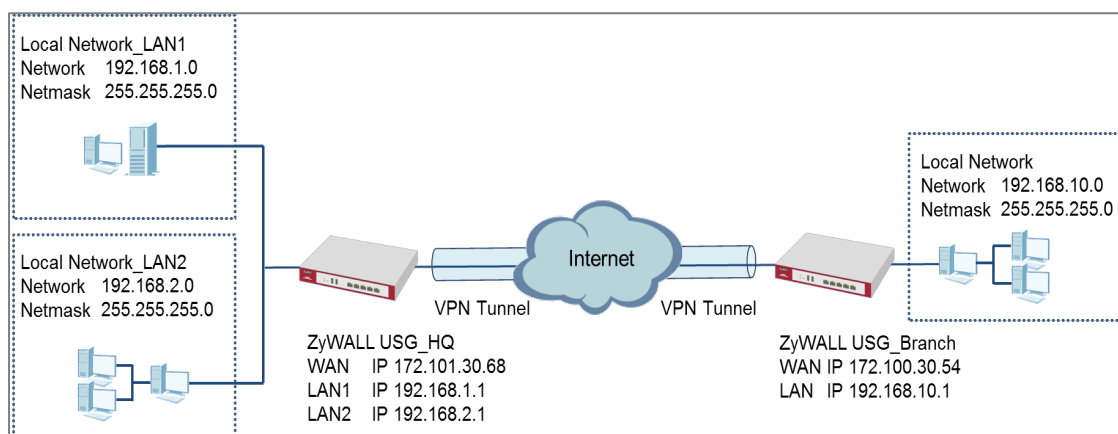
- 1 If you see a [notice] or [alert] log message such as shown below, please check the ZyWALL/USG SSL's **Selected User/Group Objects** settings. Windows 10 users must use the same **Username** and **Password** as configured in the ZyWALL/USG to establish the SSL VPN tunnel.

| Priority | Category | Message | Note |
|----------|----------|--|--------------------------|
| notice | SSL VPN | Failed login attempt to SSLVPN from http/https (incorrect password or inexistent username) | Account: SSL_VPN_1_Users |
| alert | User | Failed login attempt to Device from http/https (incorrect password or inexistent username) | Account: SSL_VPN_1_Users |


- 2 If you have uploaded a logo to show on the SSL VPN user screens but it does not display properly, check if the logo graphic is in GIF, JPG, or PNG format. The graphic should use a resolution of 103 x 29 pixels to avoid distortion when displayed. The ZyWALL/USG automatically resizes a graphic of a different resolution to 103 x 29 pixels. The file size must be 100 kilobytes or less. Transparent background is recommended.
- 3 If users can log into the SSL VPN but cannot see some of the resource links, check the SSL application object's configurations.
- 4 If the ZyWALL/USG redirects the user to the user aware screen, check whether the user account is included in an SSL VPN access policy or not.
- 5 If you have changed the HTTP/HTTPS configuration, the SSL VPN network extension sessions will be disconnected. The sessions need to be reconnected if this happens.

How to redirect multiple LAN interface traffic to the VPN tunnel

This example shows how to use the VPN Setup Wizard to create a site-to-site VPN with multiple LAN access to the VPN tunnel. The example instructs how to configure the VPN tunnel between each site and redirect multiple LAN interface traffic to the VPN tunnel. When the VPN tunnel is configured, multiple LAN subnets can be accessed securely.



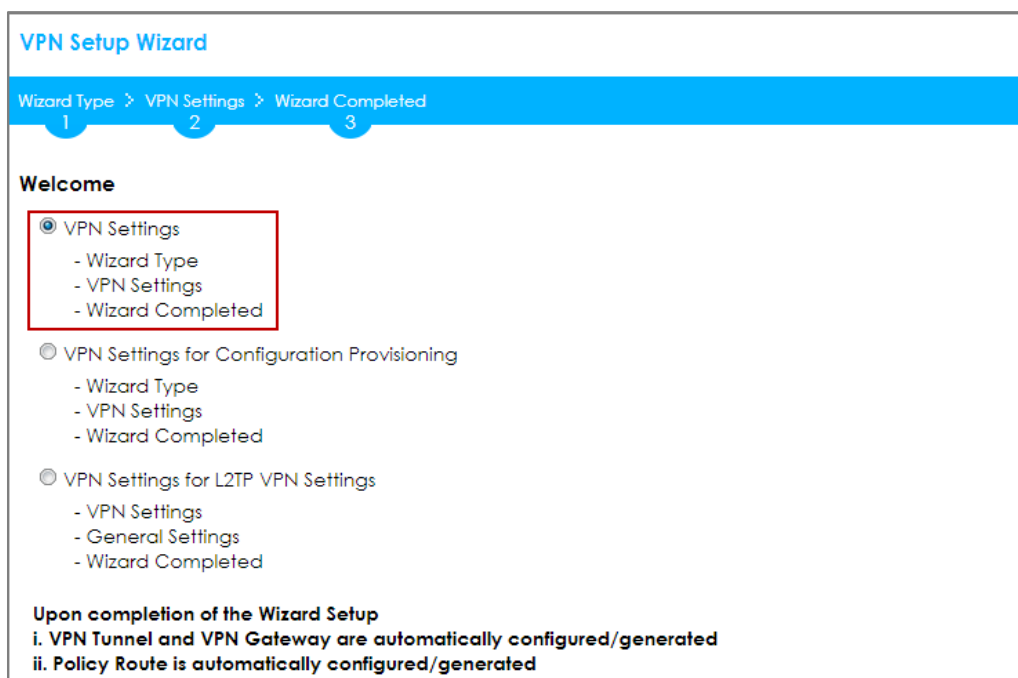
ZyWALL Site-to-site IPsec VPN with multiple LAN access

 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the ZyWALL/USG IPSec VPN Tunnel of Corporate Network (HQ)

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Welcome

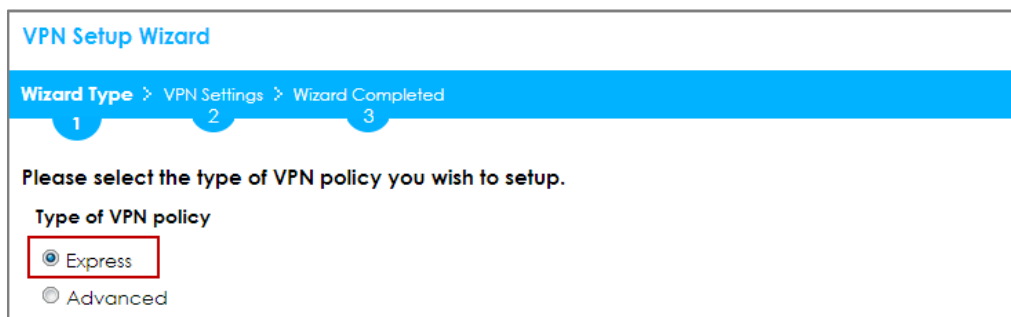
- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

Upon completion of the Wizard Setup

- i. VPN Tunnel and VPN Gateway are automatically configured/generated
- ii. Policy Route is automatically configured/generated

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Please select the type of VPN policy you wish to setup.

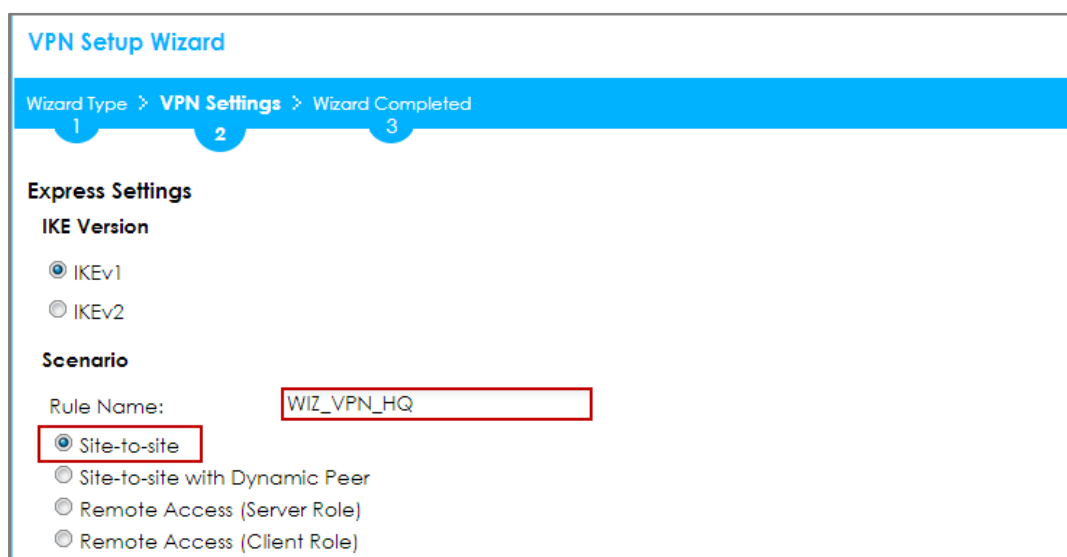
Type of VPN policy

☒ Express

☐ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name:

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

Configure **Secure Gateway** IP as the peer ZyWALL/USG's WAN IP address (in the example, 172.100.30.54). Type a secure **Pre-Shared Key** (8-32 characters).

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the peer ZyWALL/USG.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Configuration

Secure Gateway: 10.214.30.77 (IP or FQDN)

Pre-Shared Key: zyxel123

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Summary

Rule Name: WIZ_VPN_HQ

Secure Gateway: 10.214.30.77

Pre-Shared Key: zyxel123

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Express Settings

Congratulations. The VPN Access wizard is completed

Summary

| | |
|--------------------------|------------------------------|
| Rule Name: | WIZ_VPN_HQ |
| Secure Gateway: | 10.214.30.77 |
| Pre-Shared Key: | zyxel123 |
| Local Policy (IP/Mask): | 192.168.1.0 / 255.255.255.0 |
| Remote Policy (IP/Mask): | 192.168.10.0 / 255.255.255.0 |

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** and click **Show Advanced Settings**. Configure **Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPSec router.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type

Authentication

☒ Pre-Shared Key

.....

☐ unmasked

☐ Certificate

default
(See [My Certificates](#))

☐ User Based PSK

admin

☒ Advance

Local ID Type:
IPv4

Content:
0.0.0.0

Peer ID Type:
Any

Content:
10.214.30.77

Set Up the ZyWALL/USG IPSec VPN Tunnel of Corporate Network (Branch)

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

Upon completion of the Wizard Setup
 i. VPN Tunnel and VPN Gateway are automatically configured/generated
 ii. Policy Route is automatically configured/generated

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and to use a pre-shared key. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Please select the type of VPN policy you wish to setup.

Type of VPN policy

- ☒ Express
- ☐ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name: WIZ_VPN_Branch

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

Configure **Secure Gateway** IP as the peer ZyWALL/USG's WAN IP address (in the example, 172.101.30.68). Type a secure **Pre-Shared Key** (8-32 characters).

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the peer ZYWALL/USG.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Configuration

Secure Gateway: 10.214.30.106 (IP or FQDN)

Pre-Shared Key: zyxel123

Local Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Summary

Rule Name: WIZ_VPN_Branch

Secure Gateway: 10.214.30.106

Pre-Shared Key: zyxel123

Local Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Congratulations. The VPN Access wizard is completed
Summary

Rule Name: WIZ_VPN_Branch

Secure Gateway: 10.214.30.106

Pre-Shared Key: zyxel123

Local Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** and click **Show Advanced Settings**. Configure **Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPSec router.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type

Authentication

☒ Pre-Shared Key

☐ unmasked

☐ Certificate

 (See [My Certificates](#))

☐ User Based PSK

 ⓘ

☒ Advance

Local ID Type:

Content:

Peer ID Type:

Content:

Set up the Policy Route (ZyWALL/USG_HQ)

Go to ZyWALL/USG_HQ **CONFIGURATION > Network > Routing > Add**. Set **Source Address** to be the subnet (192.168.2.0/24 in this example) allows joining the VPN tunnel. Set **Destination Address** to be the remote LAN subnet (192.168.10.0/24 in this example).

CONFIGURATION > Network > Routing > Add

Add Policy Route

Show Advanced Settings Create new Object ▼

Configuration

☒ Enable

Description: (Optional)

Criteria

User: any ▼

Incoming: any (Excluding ZyV) ▼

Source Address: LAN2_SUBNET ▼

Destination Address: WIZ_VPN_HQ_REM ▼

DSCP Code: any ▼

Schedule: none ▼

Service: any ▼

Next-Hop

Type: VPN Tunnel ▼

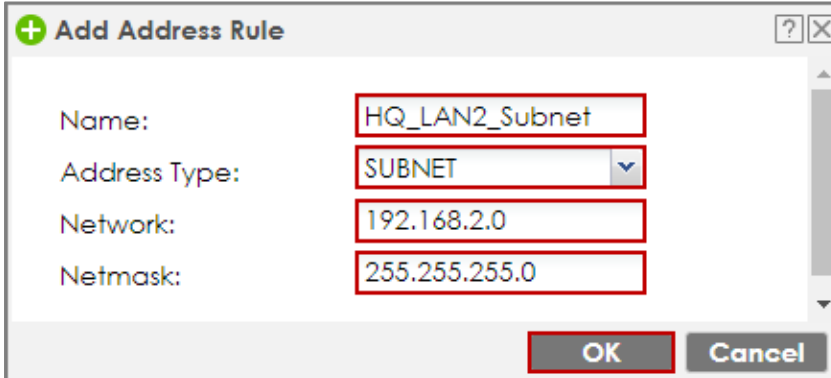
VPN Tunnel: WIZ_VPN_HQ ▼

OK Cancel

Set up the Policy Route (ZyWALL/USG_Branch)

Go to ZyWALL/USG_Branch **CONFIGURATION > Network > Routing > Add**, create **Address** to be the remote LAN subnet (192.168.2.0/24 in this example) allows joining the VPN tunnel.

CONFIGURATION > Object > Address > Add



+ Add Address Rule

Name:

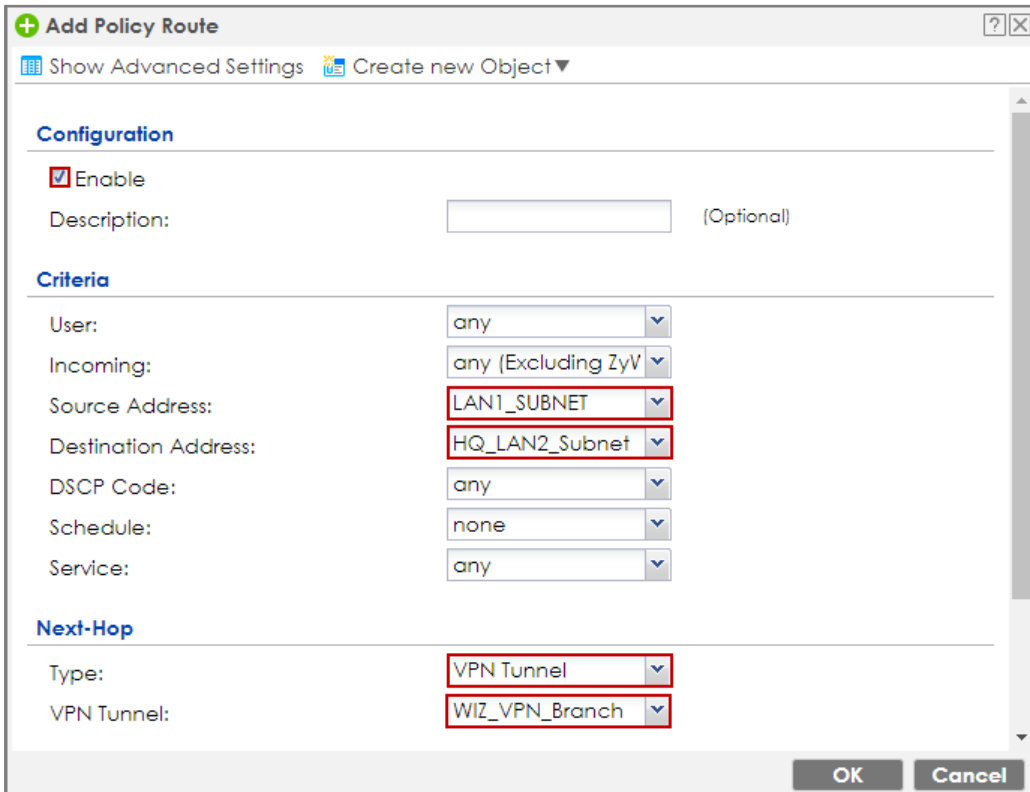
Address Type:

Network:

Netmask:

Go to ZyWALL/USG_Branch **CONFIGURATION > Network > Routing > Add**. Set **Source Address** to be the local subnet (192.168.10.0/24 in this example). Set **Destination Address** to be the remote LAN subnet (192.168.2.0/24 in this example) allows joining the VPN tunnel.

CONFIGURATION > Network > Routing > Add



+ Add Policy Route

Configuration

☒ Enable

Description: (Optional)

Criteria

User:

Incoming:

Source Address:

Destination Address:

DSCP Code:

Schedule:

Service:

Next-Hop


Type:

VPN Tunnel:

Test the IPSec VPN Tunnel

Go to ZYWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

| IPv4 Configuration | | | | |
|--|---|------------|-------------|---|
| Add Edit Remove Activate Inactivate Connect Disconnect Object References | | | | |
| # | Status | Name | VPN Gateway | Policy |
| 1 |  | WIZ_VPN_HQ | WIZ_VPN_HQ | WIZ_VPN_HQ_LOCAL WIZ_VPN... |

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and **Inbound(Bytes)/Outbound(Bytes)** Traffic.

MONITOR > VPN Monitor > IPSec

| Disconnect Connection Check | | | | | | | | | | |
|---|---------------|--------------|-------------|--------------------|--------------|----------------|---------|---------|--------------|--------------|
| # | Serial Num... | System Na... | Name | Policy | My Address | Secure G... | Up Time | Timeout | Inbound(B... | Outbound... |
| 1 | S162L44290 | VPN100 | WIZ_VPN_... | 192.168.1.0/24<... | 10.214.30... | P: 10.214.3... | 1260 | 72180 | 31(1674 b... | 31(1860 b... |

To test whether or not a tunnel is working, ping from a computer at one site to a computer at the other. Ensure that both computers have Internet access (via the IPSec devices).

PC at HQ Office > Window 7 > cmd > ping 192.168.10.33

```
C:\Documents and Settings\ZyXEL>ping 192.168.10.33

Pinging 192.168.10.33 with 32 bytes of data:

Reply from 192.168.10.33: bytes=32 time=18ms TTL=54
Reply from 192.168.10.33: bytes=32 time=17ms TTL=54
Reply from 192.168.10.33: bytes=32 time=17ms TTL=54
Reply from 192.168.10.33: bytes=32 time=16ms TTL=54

Ping statistics for 192.168.10.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 18ms, Average = 17ms
```

PC at Branch Office > Window 7 > cmd > ping 192.168.1.33


```
C:\Documents and Settings\ZyXEL>ping 192.168.1.33

Pinging 192.168.1.33 with 32 bytes of data:

Reply from 192.168.1.33: bytes=32 time=27ms TTL=43
Reply from 192.168.1.33: bytes=32 time=32ms TTL=43
Reply from 192.168.1.33: bytes=32 time=26ms TTL=43
Reply from 192.168.1.33: bytes=32 time=27ms TTL=43

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 32ms, Average = 28ms
```

PC at Branch Office > Window 7 > cmd > ping 192.168.2.33

```
C:\Documents and Settings\ZyXEL>ping 192.168.2.33

Pinging 192.168.2.33 with 32 bytes of data:

Reply from 192.168.2.33: bytes=32 time=27ms TTL=43
Reply from 192.168.2.33: bytes=32 time=27ms TTL=43
Reply from 192.168.2.33: bytes=32 time=26ms TTL=43
Reply from 192.168.2.33: bytes=32 time=32ms TTL=43

Ping statistics for 192.168.2.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 32ms, Average = 28ms
```

What Could Go Wrong?

If you see below [info] or [error] log message, please check ZyWALL/USG Phase 1 Settings. Both ZyWALL/USG at the HQ and Branch sites must use the same Pre-Shared Key, Encryption, Authentication method, DH key group and ID Type to establish the IKE SA.

MONITOR > Log

| Priority | Category | Message | Note |
|----------|----------|---|---------|
| info | IKE | [COOKIE] Invalid cookie, no sa found | IKE_LOG |
| Priority | Category | Message | Note |
| info | IKE | Recv:[NOTIFY:NO_PROPOSAL_CHOSEN] | IKE_LOG |
| info | IKE | [SA] : Tunnel [HQ1] Phase 1 proposal mismatch | IKE_LOG |

If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG Phase 2 Settings. Both ZyWALL/USG at the HQ and Branch sites must use the same Protocol, Encapsulation, Encryption, Authentication method and PFS to establish the IKE SA.

MONITOR > Log

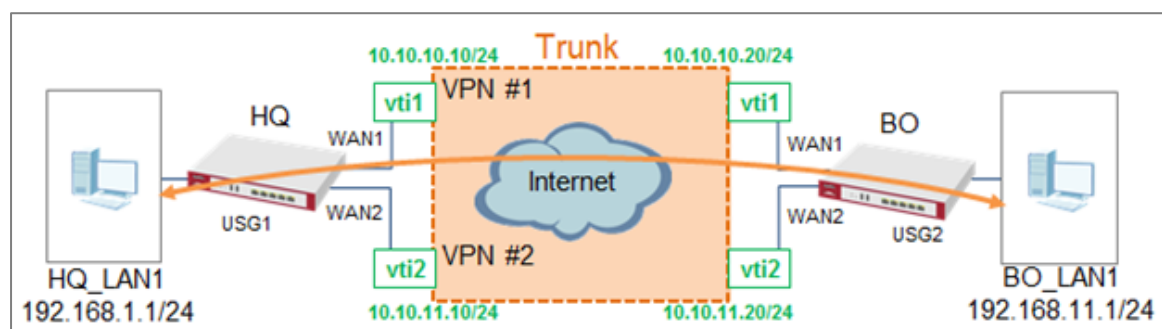
| Priority | Cate... | Message | Note |
|----------|---------|---|---------|
| info | IKE | Recv:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN] | IKE_LOG |
| info | IKE | Send:[HASH][SA][NONCE][ID][ID] | IKE_LOG |
| info | IKE | Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN] | IKE_LOG |
| info | IKE | [SA] : No proposal chosen | IKE_LOG |
| info | IKE | [SA] : Tunnel [BO1] Phase 2 proposal mismatch | IKE_LOG |
| info | IKE | Recv:[HASH][SA][NONCE][ID][ID] | IKE_LOG |
| info | IKE | Phase 1 IKE SA process done | IKE_LOG |

Make sure the both ZyWALL/USG at the HQ and Branch sites security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.


Default NAT traversal is enable on ZyWALL/USG, please make sure the remote IPSec device must also have NAT traversal enabled.

How to Create VTI and Configure VPN Failover with VTI

This example illustrates how to create a VTI object and configure a policy route with the VTI. Furthermore, it applies the VTI to the WAN trunk to achieve VPN load balancing.



VPN Load Balance with VTI

 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG110 (Firmware Version: ZLD 4.25).

VTI Deployment Flow

- 1 Configure the VPN gateways.
- 2 Configure a VPN tunnel for each VPN gateway with the application scenario VPN Tunnel Interface.
- 3 Create a VTI for each VPN tunnel.
- 4 Create a trunk with the VTIs.
- 5 Configure a policy route.
- 6 Connect the VPN tunnels.

Set Up the ZyWALL/USG VTI of Corporate Network (HQ)

- 1 In the ZyWALL/USG, go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Add** to create the VPN gateway **HQ1** with **wan1**.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Add

General Settings

☒ Enable

VPN Gateway Name:

IKE Version

☒ IKEv1

☐ IKEv2

Gateway Settings

My Address

☒ Interface DHCP client -- 10.214.30.106/255.255.255.252

☐ Domain Name / IPv4

Peer Gateway Address

☒ Static Address i

Primary

Secondary

☐ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: (60-86400 seconds)

☐ Dynamic Address i

Authentication

☒ Pre-Shared Key

- 2 In the same screen, create the VPN gateway **HQ2** with **wan2**.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Add

General Settings

☒ Enable

VPN Gateway Name:

IKE Version

☒ IKEv1

☐ IKEv2

Gateway Settings

My Address

☒ Interface DHCP client -- 10.214.30.107/255.255.255.252

☐ Domain Name / IPv4

Peer Gateway Address

☒ Static Address i

Primary

Secondary

☐ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: (60-86400 seconds)

☐ Dynamic Address i

Authentication

☒ Pre-Shared Key

- 3 Go to **CONFIGURATION > VPN > IPsec VPN > VPN Connection > Add** and configure a VPN tunnel for the VPN gateway **HQ1**. Select **VPN Tunnel Interface** as the application scenario.

CONFIGURATION > VPN > IPsec VPN > VPN Connection > Add

| General Settings | |
|---|--------------------------------|
| <input checked="" type="checkbox"/> Enable | |
| Connection Name: | HQ1 |
| <input checked="" type="checkbox"/> Advance | |
| VPN Gateway | |
| Application Scenario | |
| <input type="radio"/> Site-to-site | |
| <input type="radio"/> Site-to-site with Dynamic Peer | |
| <input type="radio"/> Remote Access (Server Role) | |
| <input type="radio"/> Remote Access (Client Role) | |
| <input checked="" type="radio"/> Vpn Tunnel Interface | |
| VPN Gateway: | HQ1 wan1 10.214.30.77, 0.0.0.0 |
| Phase 2 Setting | |
| SA Life Time: | 86400 (180 - 3000000 Seconds) |

- 4 In the same screen, create a VPN tunnel for the VPN gateway **HQ2**. Select **VPN tunnel Interface** as the application scenario.

CONFIGURATION > VPN > IPsec VPN > VPN Connection > Add

| General Settings | |
|---|--------------------------------|
| <input checked="" type="checkbox"/> Enable | |
| Connection Name: | HQ2 |
| <input checked="" type="checkbox"/> Advance | |
| VPN Gateway | |
| Application Scenario | |
| <input type="radio"/> Site-to-site | |
| <input type="radio"/> Site-to-site with Dynamic Peer | |
| <input type="radio"/> Remote Access (Server Role) | |
| <input type="radio"/> Remote Access (Client Role) | |
| <input checked="" type="radio"/> Vpn Tunnel Interface | |
| VPN Gateway: | HQ2 wan2 10.214.30.84, 0.0.0.0 |
| Phase 2 Setting | |
| SA Life Time: | 86400 (180 - 3000000 Seconds) |

- 5 Go to **CONFIGURATION > Network > Interface > VTI > Add** to create a VTI for the VPN tunnel **HQ1**. Enable the connectivity check. Enter the IP address of **vti1**, which is configured on **USG2**.

CONFIGURATION > Network > Interface > VTI > Add

| General Settings | |
|--|---------------|
| <input checked="" type="checkbox"/> Enable | |
| Interface Properties | |
| Interface Name: | vti1 |
| Zone: | IPSec_VPN |
| vpn-rule: | HQ1 |
| IP Address Assignment | |
| IP Address: | 10.10.10.10 |
| Subnet Mask: | 255.255.255.0 |
| Metric: | 0 (0-15) |

CONFIGURATION > Network > Interface > VTI > vti1 > Connectivity Check

| Connectivity Check | |
|---|--------------------|
| <input checked="" type="checkbox"/> Enable Connectivity Check | |
| Check Method: | icmp |
| Check Period: | 30 (5-600 seconds) |
| Check Timeout: | 5 (1-10 seconds) |
| Check Fail Tolerance: | 5 (1-10) |
| Check this address: | 10.10.10.20 |

- 6 In the same screen, create a VTI for the VPN tunnel **HQ2**.

CONFIGURATION > Network > Interface > VTI > Add

| General Settings | |
|--|---------------|
| <input checked="" type="checkbox"/> Enable | |
| Interface Properties | |
| Interface Name: | vti2 |
| Zone: | IPSec_VPN |
| vpn-rule: | HQ2 |
| IP Address Assignment | |
| IP Address: | 10.10.11.10 |
| Subnet Mask: | 255.255.255.0 |
| Metric: | 0 (0-15) |

CONFIGURATION > Network > Interface > VTI > vti2 > Connectivity Check

Connectivity Check

☒ Enable Connectivity Check

Check Method:

Check Period: (5-600 seconds)

Check Timeout: (1-10 seconds)

Check Fail Tolerance: (1-10)

Check this address:

7 Go to CONFIGURATION > Network > Interface > Trunk > User

Configuration > Add to create a new trunk. Add **vti1** and **vti2** to the new trunk.

CONFIGURATION > Network > Interface > Trunk > User Configuration > Add

Name:

Load Balancing Algorithm:

Load Balancing Index(es):

+ Add
 Edit
 Remove
 Move

| # | Member | Mode | Egress Bandwidth |
|---|--------|--------|------------------|
| 1 | vti1 | Active | 1048576 kbps |
| 2 | vti2 | Active | 1048576 kbps |

Page 0 of 0
 Show 50 items
 No data to display

8 Go to CONFIGURATION > Network > Routing > Policy Route > Add to configure a policy route.

Source Address: LAN1_SUBNET (192.168.1.0/24)

Destination Address: BO_subnet (192.168.11.0/24)

Next-Hop: HQ_vti_trunk

SNAT: none

CONFIGURATION > Network > Routing > Policy Route > Add

Configuration

☒ Enable

Description: (Optional)

Criteria

User:

Incoming:

Source Address:

Destination Address:

DSCP Code:

Schedule:

Service:

Next-Hop

Type:

Trunk:

DSCP Marking

DSCP Marking:

Address Translation

Source Network Address Translation:

9 Connect the VPN tunnels when the VTIs are ready. Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** to connect the VPN tunnels.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Connect

VPN Connection
VPN Gateway
Concentrator
Configuration Provisioning

Global Setting
Configuration Walkthrough
Troubleshooting
Download VPN Client
VPN

☐ Use Policy Route to control dynamic IPSec rules
 ☐ Ignore "Don't Fragment" setting in IPv4 header

IPv4 Configuration

Add
Edit
Remove
Activate
Inactivate
Connect
Disconnect
Object References

| # | Status | Name | VPN Gateway | Policy |
|---|--------|------|-------------|---------|
| 1 | | HQ1 | HQ1 | any/any |
| 2 | | HQ2 | HQ2 | any/any |

Page 1 of 1
Show 50 items

Displaying 1 - 2 of 2

10 Go to **CONFIGURATION > Network > Interface > VTI**. You will see that the status of the VTI is up when the corresponding VPN tunnel is established.

CONFIGURATION > Network > Interface > VTI

General Settings

☒ Enable

VPN Gateway Name:

IKE Version

☒ IKEv1
 ☐ IKEv2

Gateway Settings

My Address

☒ Interface

DHCP client -- 10.214.30.84/255.255.255.255

☐ Domain Name / IPv4

Peer Gateway Address

☒ Static Address

Primary

Secondary

☐ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval:

(60-86400 seconds)

☐ Dynamic Address

Authentication

☒ Pre-Shared Key

- Go to **CONFIGURATION > VPN > IPsec VPN > VPN Connection > Add** and configure a VPN tunnel for the VPN gateway **BO1**. Select **VPN Tunnel Interface** as the application scenario.

CONFIGURATION > VPN > IPsec VPN > VPN Connection > Add

General Settings

☒ Enable

Connection Name:

☒ Advance

VPN Gateway

Application Scenario

☐ Site-to-site
 ☐ Site-to-site with Dynamic Peer
 ☐ Remote Access (Server Role)
 ☐ Remote Access (Client Role)
 ☒ Vpn Tunnel Interface

VPN Gateway:

wan1 10.214.30.106, 0.0.0.0

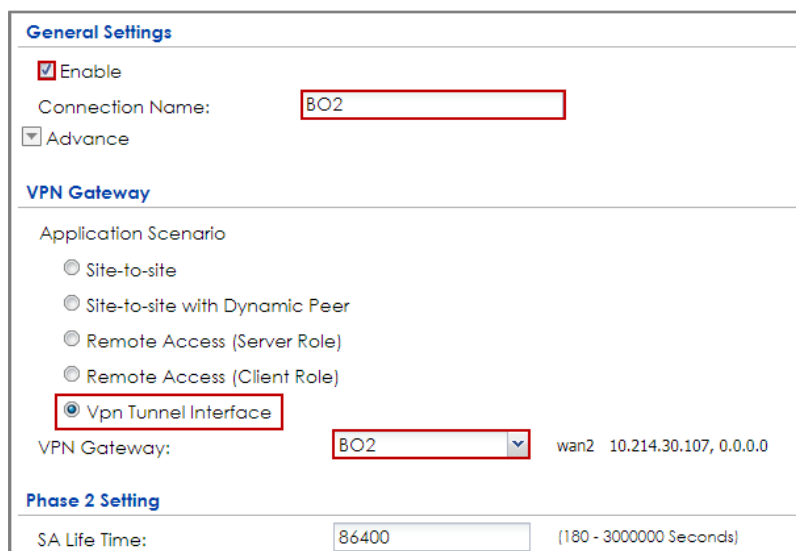
Phase 2 Setting

SA Life Time:

(180 - 3000000 Seconds)

- 4 In the same screen, create a VPN tunnel for the VPN gateway **BO2**.
Select **VPN tunnel Interface** as the application scenario.

CONFIGURATION > VPN > IPsec VPN > VPN Connection > Add



General Settings

☒ Enable

Connection Name:

☐ Advance

VPN Gateway

Application Scenario

- ☐ Site-to-site
- ☐ Site-to-site with Dynamic Peer
- ☐ Remote Access (Server Role)
- ☐ Remote Access (Client Role)
- ☒ Vpn Tunnel Interface

VPN Gateway: wan2 10.214.30.107, 0.0.0.0

Phase 2 Setting

SA Life Time: (180 - 3000000 Seconds)

- 5 Go to **CONFIGURATION > Network > Interface > VTI > Add** to create a VTI for the VPN tunnel **BO1**. Be aware that the IP address of this VTI must be in the same subnet as **vti1** on **USG1**.

In this example, the IP address and subnet mask of **vti1** on **USG1** is **10.10.10.10** and **255.255.255.0** respectively. The IP address of **vti1** on **USG2** must be in the subnet of **10.10.10.0/24**. Enable the connectivity check. Enter the IP address of **vti1**, which is configured on **USG1**.

CONFIGURATION > Network > Interface > VTI > Add

| General Settings | |
|--|--|
| <input checked="" type="checkbox"/> Enable | |
| Interface Properties | |
| Interface Name: | <input type="text" value="vti1"/> |
| Zone: | <input type="text" value="IPSec_VPN"/> ⓘ |
| vpn-rule: | <input type="text" value="BO1"/> ⓘ |
| IP Address Assignment | |
| IP Address: | <input type="text" value="10.10.10.20"/> |
| Subnet Mask: | <input type="text" value="255.255.255.0"/> |
| Metric: | <input type="text" value="0"/> (0-15) |

CONFIGURATION > Network > Interface > VTI > vti1 > Connectivity Check

| Connectivity Check | |
|---|---|
| <input checked="" type="checkbox"/> Enable Connectivity Check | |
| Check Method: | <input type="text" value="icmp"/> |
| Check Period: | <input type="text" value="30"/> (5-600 seconds) |
| Check Timeout: | <input type="text" value="5"/> (1-10 seconds) |
| Check Fail Tolerance: | <input type="text" value="5"/> (1-10) |
| Check this address: | <input type="text" value="10.10.10.10"/> |

6 In the same screen, create a VTI for the VPN tunnel **BO2**. Be aware that the IP address of this VTI must be in the same subnet as **vti2** on **USG1**. In this example, the IP address and subnet mask of **vti2** on **USG1** is **10.10.11.10** and **255.255.255.0** respectively. The IP address of **vti2** on **USG2** must be in the subnet of **10.10.11.0/24**. Enable the connectivity check. Enter the IP address of **vti2**, which is configured on **USG1**.

CONFIGURATION > Network > Interface > VTI > Add

General Settings

☒ Enable

Interface Properties

Interface Name: vti2
 Zone: IPSec_VPN
 vpn-rule: BO2

IP Address Assignment

IP Address: 10.10.11.20
 Subnet Mask: 255.255.255.0
 Metric: 0 (0-15)

CONFIGURATION > Network > Interface > VTI > vti1 > Connectivity Check

Connectivity Check

☒ Enable Connectivity Check

Check Method: icmp
 Check Period: 30 (5-600 seconds)
 Check Timeout: 5 (1-10 seconds)
 Check Fail Tolerance: 5 (1-10)
 Check this address: 10.10.11.10

7 Go to **CONFIGURATION > Network > Interface > Trunk > User Configuration > Add** to create a new trunk. Add **vti1** and **vti2** to the new trunk.

CONFIGURATION > Network > Interface > Trunk > User Configuration > Add

Name: BO_vti_trunk
 Load Balancing Algorithm: Least Load First
 Load Balancing Index(es): Outbound

+ Add Edit Remove Move

| # | Member | Mode | Egress Bandwidth |
|---|--------|--------|------------------|
| 1 | vti1 | Active | 1048576 kbps |
| 2 | vti2 | Active | 1048576 kbps |

Page 0 of 0 Show 50 items No data to display

- 8 Go to **CONFIGURATION > Network > Routing > Policy Route > Add** to configure a policy route.

Source Address: LAN1_SUBNET (192.168.11.0/24)

Destination Address: HQ_subnet (192.168.1.0/24)

Next-Hop: BO_vti_trunk

SNAT: none

CONFIGURATION > Network > Routing > Policy Route > Add

| Configuration | |
|--|---------------------------------|
| <input checked="" type="checkbox"/> Enable | |
| Description: | <input type="text"/> (Optional) |
| Criteria | |
| User: | any |
| Incoming: | any (Excluding ZyV) |
| Source Address: | LAN1_SUBNET |
| Destination Address: | HQ_subnet |
| DSCP Code: | any |
| Schedule: | none |
| Service: | any |
| Next-Hop | |
| Type: | Trunk |
| Trunk: | BO_vti_trunk |
| DSCP Marking | |
| DSCP Marking: | preserve |
| Address Translation | |
| Source Network Address Translation: | none |

- 9 Connect the VPN tunnels when the VTIs are ready. Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** to connect the VPN tunnels.

CONFIGURATION > VPN > IPsec VPN > VPN Connection > Connect

Configuration

☒ Enable

Description:

 (Optional)

Criteria

User: any
 Incoming: any (Excluding ZyV
 Source Address: LAN1_SUBNET
 Destination Address: HQ_subnet
 DSCP Code: any
 Schedule: none
 Service: any

Next-Hop

Type: Trunk
 Trunk: BO_vti_trunk

DSCP Marking

DSCP Marking: preserve

Address Translation

Source Network Address Translation: none

10 Go to **CONFIGURATION > Network > Interface > VTI**. You will see that the status of the VTI is up when the corresponding VPN tunnel is established.

CONFIGURATION > Network > Interface > VTI

| Port Role | Ethernet | PPP | Cellular | Tunnel | VLAN | Bridge | VTI | Trunk |
|--|----------|-----|----------|--------|------|--------|-----|-------|
| Configuration | | | | | | | | |
| <div><div><div><div><div><div></div><div></div></div><div><div></div><div></div></div></div><div><div></div><div></div></div><div><div></div><div></div></div><div><div></div><div></div></div><div><div></div><div></div></div><div><div></div><div></div></div></div><div><div></div><div></div></div><div><div></div><div></div></div><div><div></div><div></div></div><div><div></div><div></div></div><div><div></div><div></div></div></div><div><div></div><div></div></div><div><div></div><div></div></div><div><div></div><div></div></div><div><div></div><div></div></div><div><div></div><div></div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div><div></div></div> <div><div></div></div> | | | | | | | | |

Test the IPsec VPN Tunnel

1 To test whether or not a tunnel is working, ping from a PC in LAN1 of USG1 to a PC in LAN1 of USG2 and vice versa.

PC of USG1 (192.168.1.34) > Window 7 > cmd > ping 192.168.11.33

```
C:\Users>ping 192.168.11.33 -t

Ping 192.168.11.33 <使用 32 位元組的資料>:
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=125
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=124
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=125
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=124
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=125
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=124
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=125
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=124
```

PC of USG2 (192.168.11.33) > Window 7 > cmd > ping 192.168.1.34

```
C:\Users>ping 192.168.1.34 -t

Ping 192.168.1.34 <使用 32 位元組的資料>:
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=124
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=125
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=124
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=125
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=124
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=125
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=124
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=125
```

2 To test whether or not VPN failover is working, unplug wan1 of USG1. Then ping from a PC in LAN1 of USG1 to a PC in LAN1 of USG2 and vice versa.

Check the VPN status of the USG1 in the MONITOR > VPN Monitor > IPsec screen.

| Disconnect | | Connection Check | | | | | | | | |
|------------|--------------|--|------|-----------------------|---------------|-----------------|---------|---------|--------------|--------------|
| # | Serial Nu... | System N... | Name | Policy | My Address | Secure Gate... | Up Time | Timeout | Inbound(... | Outbound... |
| 1 | S162L44290 | VPN100 | HQ2 | 0.0.0.0/1<=>0.0.0.0/1 | 10.214.30.107 | P: 10.214.30.84 | 562 | 72878 | 205(11070... | 285(17100... |

PC of USG1 (192.168.1.34) > Window 7 > cmd > ping 192.168.11.33

```
C:\Users>ping 192.168.11.33 -t

Ping 192.168.11.33 <使用 32 位元組的資料>:
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=125
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=124
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=125
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=124
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=125
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=124
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=125
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=124
```


Check the VPN status of the USG2 in the **MONITOR > VPN Monitor > IPSec** screen.

| Disconnect | | Connection Check | | | | | | | | |
|------------|--------------|--|------|-------------------|---------------|-----------------|---------|---------|--------------|--------------|
| # | Serial Nu... | System N... | Name | Policy | My Address | Secure Gate... | Up Time | Timeout | Inbound(... | Outbound... |
| 1 | S162L44290 | VPN100 | HQ2 | 0.0.0.0/1<>0.0... | 10.214.30.107 | P: 10.214.30.84 | 562 | 72878 | 205(11070... | 285(17100... |

PC of USG2 (192.168.11.33) > Window 7 > cmd > ping 192.168.1.34

```
C:\Users>ping 192.168.1.34 -t

Ping 192.168.1.34 <使用 32 位元組的資料>:
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=124
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=125
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=124
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=125
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=124
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=125
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=124
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=125
```

What Can Go Wrong?

- 1 If you see below [info] or [error] log message, please check ZyWALL/USG Phase 1 Settings. Both ZyWALL/USG at the HQ and Branch sites must use the same Pre-Shared Key, Encryption, Authentication method, DH key group and ID Type to establish the IKE SA.

MONITOR > Log

| Priority | Category | Message | Note |
|----------|----------|---|---------|
| info | IKE | [COOKIE] Invalid cookie, no sa found | IKE_LOG |
| Priority | Category | Message | Note |
| info | IKE | Recv:[NOTIFY:NO_PROPOSAL_CHOSEN] | IKE_LOG |
| info | IKE | [SA] : Tunnel [HQ1] Phase 1 proposal mismatch | IKE_LOG |

- 2 If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG Phase 2 Settings. Both ZyWALL/USG at the HQ and Branch sites must use the same Protocol, Encapsulation, Encryption, Authentication method and PFS to establish the IKE SA.

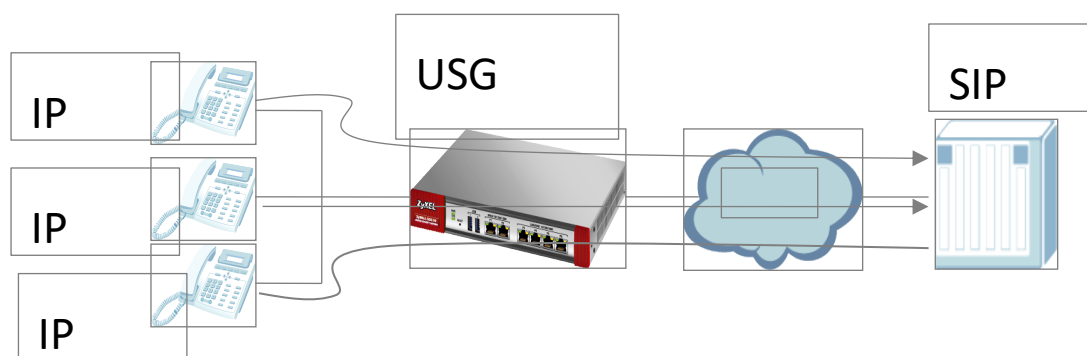
MONITOR > Log

| Priority | Cate... | Message | Note |
|----------|---------|---|---------|
| info | IKE | Recv:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN] | IKE_LOG |
| info | IKE | Send:[HASH][SA][NONCE][ID][ID] | IKE_LOG |
| info | IKE | Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN] | IKE_LOG |
| info | IKE | [SA] : No proposal chosen | IKE_LOG |
| info | IKE | [SA] : Tunnel [BO1] Phase 2 proposal mismatch | IKE_LOG |
| info | IKE | Recv:[HASH][SA][NONCE][ID][ID] | IKE_LOG |
| info | IKE | Phase 1 IKE SA process done | IKE_LOG |

- 3 Make sure the both ZyWALL/USG at the HQ and Branch sites security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.
- 4 Default NAT traversal is enable on ZyWALL/USG, please make sure the remote IPSec device must also have NAT traversal enabled.
- 5 Make sure the both ZyWALL/USG at the HQ and Branch sites use static IP address because VPN Tunnel Interface does not support dynamic peer.
- 6 Make sure policy routes are configured to control traffic between the subnet of HQ and Branch through VTI.
- 7 Make sure that the IP address of VTI at the Branch must be in the same subnet as vti1 on HQ. For example, the IP address and subnet mask of vti1 on HQ is 10.10.10.10 and 255.255.255.0 respectively. The IP address of vti1 on the Branch must be in the subnet of 10.10.10.0/24; the IP address and subnet mask of vti2 on HQ is 10.10.11.10 and 255.255.255.0 respectively. The IP address of vti2 on the Branch must be in the subnet of 10.10.10.0/24, and so on.

How to configure the USG when using a Cloud Based SIP system

This example shows how to configure USG when there is a Cloud Based SIP system. The IP phones are more and more popular nowadays. USG supports the scenario as IP phones located in LAN and connect to internet to register the SIP server.



SIP Phone connects to SIP server via USG.



Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG210 (Firmware Version: ZLD 4.25).

Set Up the SIP ALG

Go to **CONFIGURATION > Network > ALG**, and check **"Enable SIP ALG"**. Also, check the **"Enable SIP Transformations"** if the SIP content which is needed to be transform. Then click **"Apply"**.

CONFIGURATION > Network > ALG

ALG

SIP Settings

- ☒ Enable SIP ALG
 - ☒ Enable SIP Transformations
 - ☒ Enable Configure SIP Inactivity Timeout
 - SIP Media Inactivity Timeout : (seconds)
 - SIP Signaling Inactivity Timeout : (seconds)
 - ☒ Restrict Peer to Peer Signaling Connection
 - ☒ Restrict Peer to Peer Media Connection i
- SIP Signaling Port :

+ Add ✎ Edit ✖ Remove

| # | Port ▲ |
|---|--------|
| 1 | 5060 |

Direct-media and Direct-signalling are activated after ZLD 4.25. We can use the CLI to show the status. When the two options are yes, it will change the original sip alg behavior.

direct-signalling will expect incoming calls from register only.

direct-media will expect media streams between signalling endpoints only.

Test result

Connect SIP phone to the USG, and check the register status. Register successfully.

| SIP Accounts | | | | | |
|--------------|--------------|---------------------|------------|--------------|--|
| # | Display Name | Registration Server | Status | Registration | |
| 1 | 2436 | 10.214.30.86 | registered | Enable | |

Check the SIP register status on PBX.

| # | Time | Priority | Category | Message |
|---|----------------------|----------|----------|--|
| 2 | 2017-07-07 04:20:... | notice | PBX SIP | Extension '2436' registered successfully at 10.214.30.90:5061 with expire time 3276. |
| 3 | 2017-07-07 04:20:... | notice | PBX SIP | Extension 2436 registered successfully with expire time 3276 |

What could go wrong?

SIP phone does not support transform itself, but the **"SIP Transformations"** does not be checked.

| | | | | | |
|----|----------|--------------|--------------|-----|--|
| 48 | 5.700826 | 10.251.30.94 | 10.251.30.58 | SIP | 523 Request: REGISTER sip:10.251.30.58 |
| 49 | 5.704336 | 10.251.30.58 | 10.251.30.94 | SIP | 559 Status: 401 unauthorized (0 bindings) |
| 50 | 5.737000 | 10.251.30.94 | 10.251.30.58 | SIP | 681 Request: REGISTER sip:10.251.30.58 |
| 51 | 5.742023 | 10.251.30.58 | 10.251.30.94 | SIP | 586 Request: NOTIFY sip:2436@192.168.1.33:5060 |

| | | | | | |
|---|--|--|--|--|--|
| Frame 51: 586 bytes on wire (4688 bits), 586 bytes captured (4688 bits) | | | | | |
| Ethernet II, Src: ZyxelCom_33:cf:8e (cc:5d:4e:33:cf:8e), Dst: 5c:f4:ab:f8:fd:54 (5c:f4:ab:f8:fd:54) | | | | | |
| Internet Protocol Version 4, Src: 10.251.30.58 (10.251.30.58), Dst: 10.251.30.94 (10.251.30.94) | | | | | |
| User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060) | | | | | |
| Source port: sip (5060) | | | | | |
| Destination port: sip (5060) | | | | | |
| Length: 552 | | | | | |
| Checksum: 0x0571 [validation disabled] | | | | | |
| Session Initiation Protocol | | | | | |
| Request-Line: NOTIFY sip:2436@192.168.1.33:5060 SIP/2.0 | | | | | |
| Message Header | | | | | |
| Via: SIP/2.0/UDP 10.251.30.58:5060;branch=z9hg4bk10f6cfa3;rport | | | | | |
| Max-Forwards: 70 | | | | | |
| From: "TSG" <sin:tsg@10.251.30.58>;tag=as7ebe60ba | | | | | |

SIP phone will contact with outside as not direct-signalling and direct media, but the default setting on USG is on

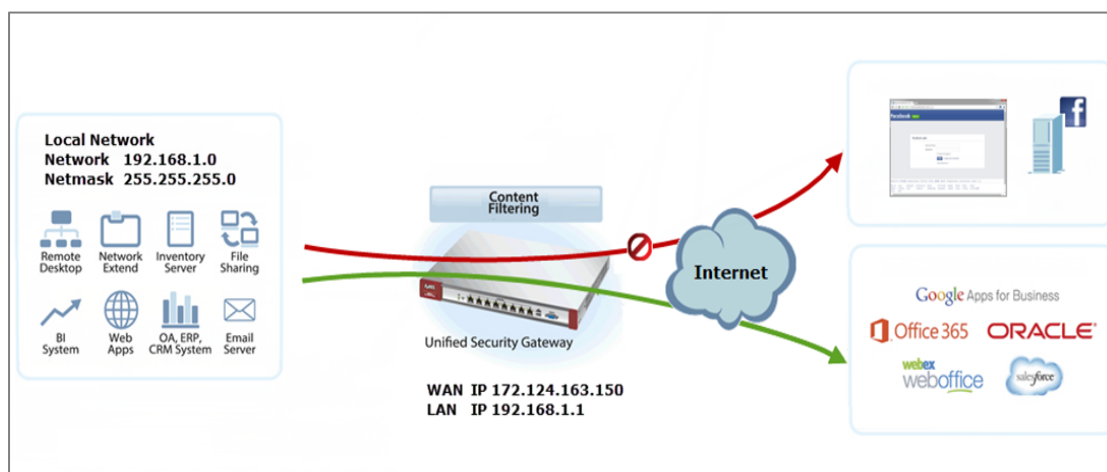
How to block HTTPS websites by Domain Filter without applying SSL Inspection


The Content Filter with HTTPs Domain Filter allows you to block HTTPs websites by category service without SSL-Inspection. The filtering feature is based on more than 50 Managed Categories built in ZyWALL/USG such as pornography, gambling, hacking, etc.

When user makes HTTPS request, the information contains a Server Name Indication

(SNI) extension fields in server FQDN. Using the SNI to query category from Commtouch engine, then take action when it matches the block category in Content Filter profile.

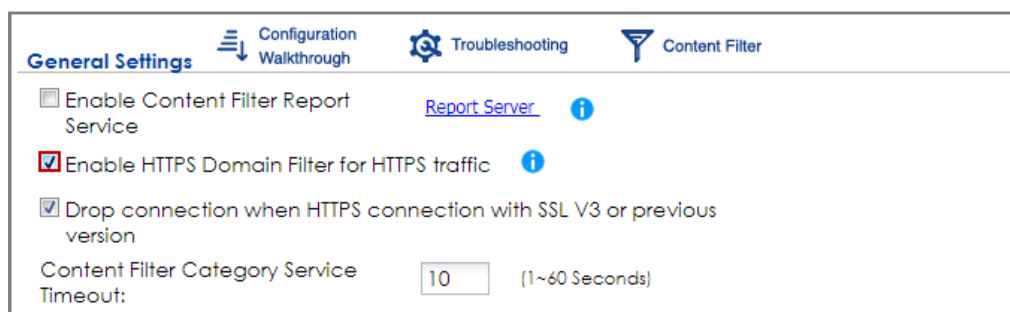
ZyWALL/USG Domain Filter Example



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: 4.25)

Set Up the Content Filter on the ZyWALL/USG

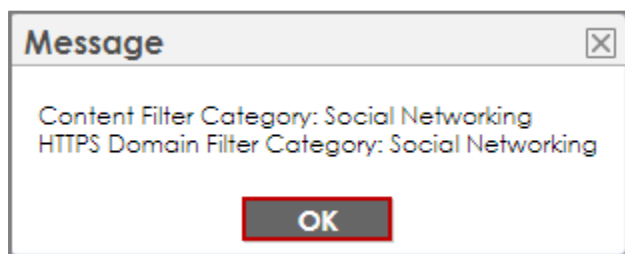
Go to **CONFIGURATION > UTM Profile> Content Filter > Profile > General Settings**. Select **Enable HTTPS Domain Filter for HTTPS traffic**.



Go to **CONFIGURATION > UTM Profile> Content Filter > Profile Management > Add Filter**

Profile > Test Web Site Category. Type URL to test the category and click **Test Against Content Filter Category Server**.

You will see the category recorded in the external content filter server's database for both HTTP and HTTPS Domain you specified.



Go to **CONFIGURATION > UTM Profile > Content Filter > Profile Management > Add Filter File > Custom Service**. Configure a **Name** for you to identify the **Content Filter Profile** and select **Enable Content Filter Category Service**. Select **Block** to prevent users from accessing web pages that match the managed categories that you select below. Select **Log** to record attempts to access web pages that match the unsafe categories that you select below.

General Settings

License Status: Licensed

License Type: Standard

Name: **Social_Net_Block**

Description: (Optional)

☐ Enable SafeSearch

☒ Enable Content Filter Category Service

☐ Log all web pages

Action for Unsafe Web Pages: Block ☐ Log

Action for Managed Web Pages: **Block** ☒ Log

Action for Unrated Web Pages: Warn ☐ Log

Action When Category Server Is Unavailable: Warn ☐ Log

Scroll down to the **Managed Categories** section, select categories in this section to control access to specific types of Internet content. You must have the Content Filtering license to filter these categories.

Managed Categories

| | | |
|--|---|---|
| <input type="checkbox"/> Advertisements & Pop-Ups | <input type="checkbox"/> Alcohol/Tobacco | <input type="checkbox"/> Arts |
| <input type="checkbox"/> Business | <input type="checkbox"/> Transportation | <input type="checkbox"/> Chat |
| <input type="checkbox"/> Forums & Newsgroups | <input type="checkbox"/> Computers & Technology | <input type="checkbox"/> Criminal Activity |
| <input type="checkbox"/> Dating & Personals | <input type="checkbox"/> Download Sites | <input type="checkbox"/> Education |
| <input type="checkbox"/> Entertainment | <input type="checkbox"/> Finance | <input type="checkbox"/> Gambling |
| <input type="checkbox"/> Games | <input type="checkbox"/> Government | <input type="checkbox"/> Hate & Intolerance |
| <input type="checkbox"/> Health & Medicine | <input type="checkbox"/> Illegal Drugs | <input type="checkbox"/> Job Search |
| <input type="checkbox"/> Streaming Media & Downloads | <input type="checkbox"/> News | <input type="checkbox"/> Non-profits & NGOs |
| <input type="checkbox"/> Nudity | <input type="checkbox"/> Personal Sites | <input type="checkbox"/> Politics |
| <input type="checkbox"/> Pornography/Sexually Explicit | <input type="checkbox"/> Real Estate | <input type="checkbox"/> Religion |
| <input type="checkbox"/> Restaurants & Dining | <input type="checkbox"/> Search Engines/Portals | <input type="checkbox"/> Shopping |
| <input checked="" type="checkbox"/> Social Networking | <input type="checkbox"/> Sports | <input type="checkbox"/> Translators |
| <input type="checkbox"/> Travel | <input type="checkbox"/> Violence | <input type="checkbox"/> Weapons |
| <input type="checkbox"/> Web-based Email | <input type="checkbox"/> General | <input type="checkbox"/> Leisure & Recreation |
| <input type="checkbox"/> Cults | <input type="checkbox"/> Fashion & Beauty | <input type="checkbox"/> Greeting Cards |
| <input type="checkbox"/> Hacking | <input type="checkbox"/> Illegal Software | <input type="checkbox"/> Image Sharing |
| <input type="checkbox"/> Information Security | <input type="checkbox"/> Instant Messaging | <input type="checkbox"/> Peer to Peer |
| <input type="checkbox"/> Private IP Addresses | <input type="checkbox"/> School Cheating | <input type="checkbox"/> Sex Education |
| <input type="checkbox"/> Tasteless | <input type="checkbox"/> Child Abuse Images | |

Set Up the Security Policy on the ZyWALL/USG

Go to **CONFIGURATION > Security Policy > Policy Control**, configure a **Name** for you to identify the **Security Policy** profile. Scroll down to **UTM Profile**, select **Content Filter** and select a profile from the list box (Social_Net_Block in this example).

☒ Enable

Name:

Description: (Optional)

From:

To:

Source:

Destination:

Service:

User:

Schedule:

Action:

Log matched traffic:

UTM Profile

☒ Content Filter: Log:

☐ SSL Inspection: Log:

Set Up the System Policy on the ZyWALL/USG

Go to **CONFIGURATION > System > WWW > Show Advanced Settings > Other**, click **Enable Content Filter HTTPS Domain Filter Block/Warn Page**.

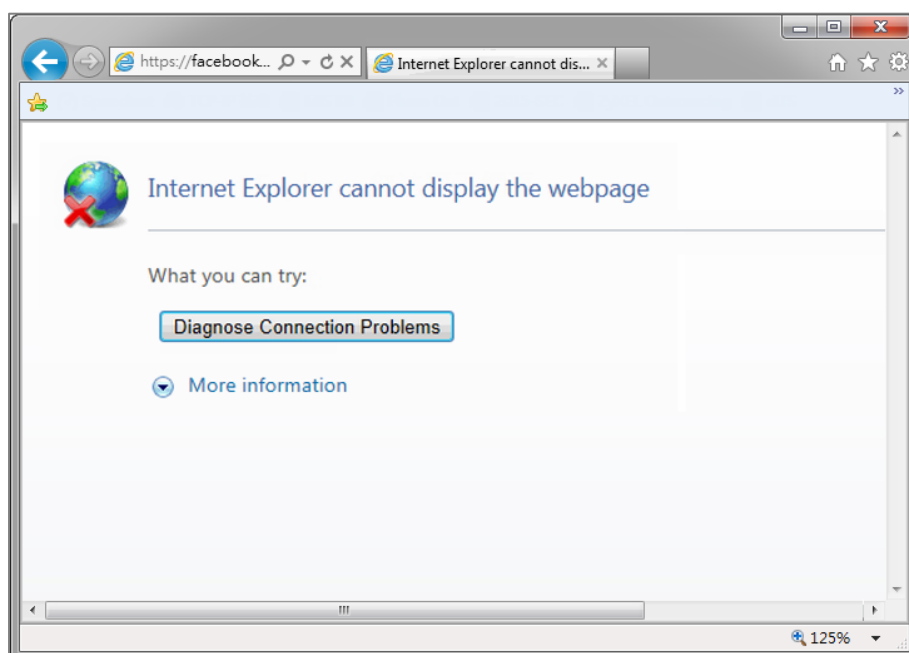
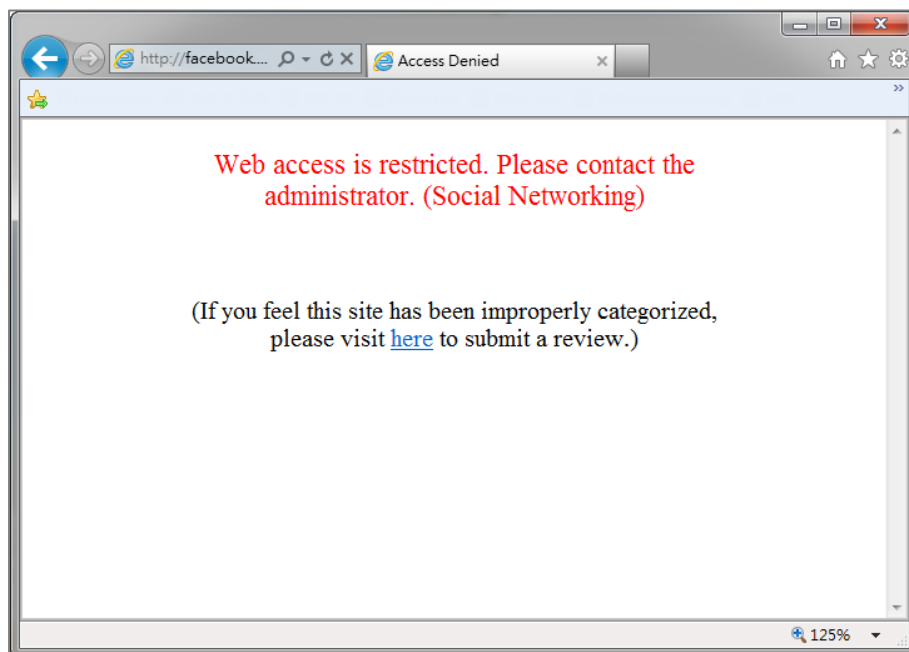
Other

☒ Enable Content Filter HTTPS Domain Filter Block/Warn Page

Block/Warn Page Port:

Test the Result

Type <http://www.facebook.com/> or <https://www.facebook.com/> into the browser, the error message occurs.



Go to the ZyWALL/USG **Monitor > Log**, you will see [alert] log message such as below. HTTP traffic log matches (Content Filter) and HTTPS traffic log matches (HTTPS Domain Filter) in message field.

Monitor > Log

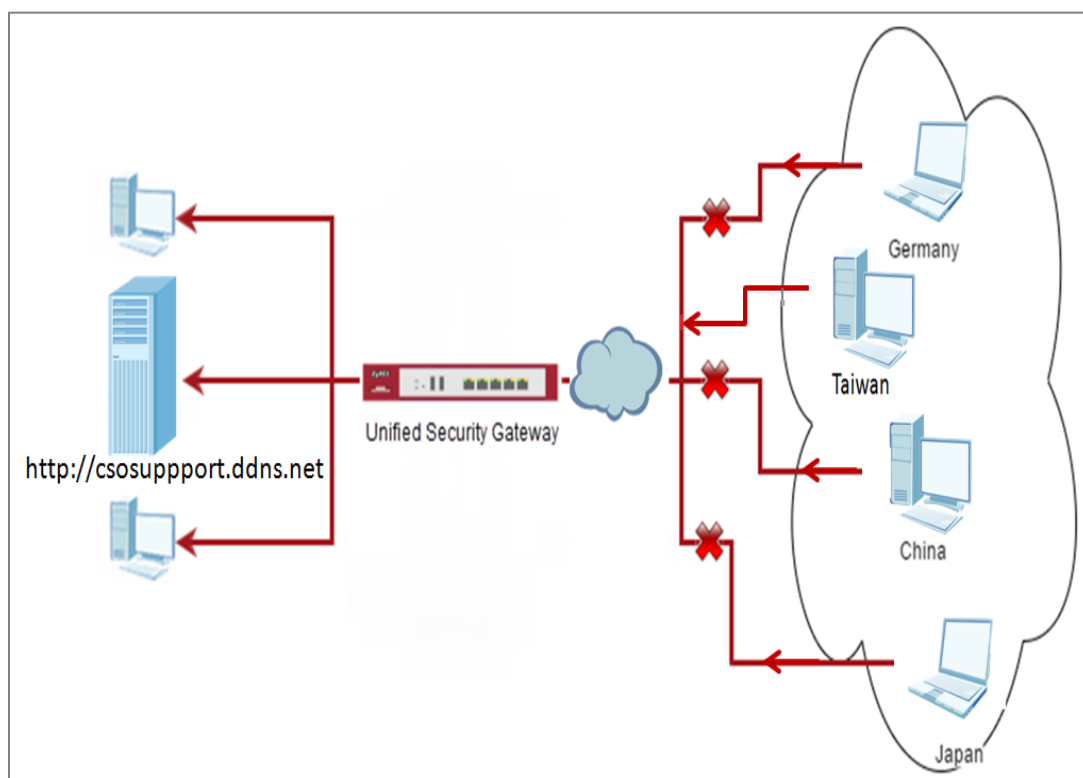
| # | Time | Priority | Category | Message | Source | Destination | Note |
|---|---------------------|----------|-------------------------|---|--------------------|-----------------------|--------------|
| 1 | 2016-03-17 02:22:39 | notice | Security Policy Control | Match default rule, DROP [count=2] | 10.251.31.91:17500 | 255.255.255.255:17500 | ACCESS BLOCK |
| 2 | 2016-03-17 02:33:09 | alert | Blocked web sites | facebook.com : Social Networking, Rule_id=1 (Content Filter) | 192.168.1.33:18424 | 66.220.158.68:80 | WEB BLOCK |
| 3 | 2016-03-17 02:22:35 | alert | Blocked web sites | www.facebook.com : Social Networking, Rule_id=1 (HTTPS Domain Filter) | 192.168.1.33:51728 | 31.13.79.220:443 | WEB BLOCK |

How to Configure Content Filter 2.0 with Geo IP Blocking

The Content Filter 2.0 - Geo IP blocking offers identify the country based on IP address, it allows you to block the client accessing to certain country based on organizational policy.

When user makes HTTP or HTTPS request, ZyWALL/USG query IP address from MaxMind database, then take action when it matches the block country in Content Filter profile. If you have a local web site and your primary market is local people, then there is no need to let any other countries index or waste bandwidth on your server.

Also this feature offer an easy and effective way to prevent bogus, bots, brute force hacks, vulnerability scanners, and web crawlers from other countries.



Set Up the Address Object with Geo IP on the ZyWALL/USG

Go to **CONFIGURATION > Object > Address/Geo IP > Address > Add Address Rule**.



Edit Address Rule Taiwan

Name:

Address Type:

Country:

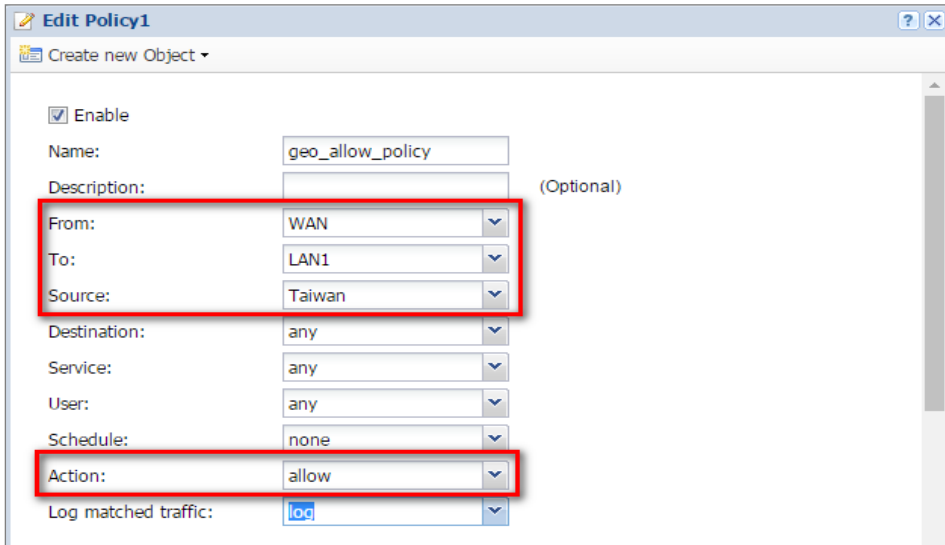
OK Cancel

Go to **CONFIGURATION > Object > Address/Geo IP > Address**, you can see the customized GEOGRAPHY address.

| Address | | | |
|-----------------------------------|--------------|------------------|-----------------------------|
| Address Group | | | |
| Geo IP | | | |
| IPv4 Address Configuration | | | |
| Add Edit Remove Object References | | | |
| # | Name | Type | IPv4 Address |
| 1 | wan2 | INTERFACE IP | wan2-10.251.30.90 |
| 2 | LAN2_SUBNET | INTERFACE SUBNET | lan2-192.168.2.0/24 |
| 3 | LAN1_SUBNET | INTERFACE SUBNET | lan1-192.168.1.0/24 |
| 4 | DMZ_SUBNET | INTERFACE SUBNET | dmz-192.168.3.0/24 |
| 5 | Taiwan | GEOGRAPHY | Taiwan-All |
| 6 | IP6to4-Relay | HOST | 192.88.99.1 |
| 7 | l2tp_pool | RANGE | 192.168.10.10-192.168.10.20 |
| 8 | RFC1918_3 | SUBNET | 192.168.0.0/16 |
| 9 | RFC1918_2 | SUBNET | 172.16.0.0/12 |

Set Up the Security Policy on the ZyWALL/USG

Go to **CONFIGURATION > Security Policy > Policy Control**, configure a **Name** for you to identify the **Security Policy** profile. Set Geo IP traffic from WAN to LAN allow source from local country (geo_allow_policy in this example).



Edit Policy1

Create new Object ▾

☒ Enable

Name: geo_allow_policy

Description: (Optional)

From: WAN

To: LAN1

Source: Taiwan

Destination: any

Service: any

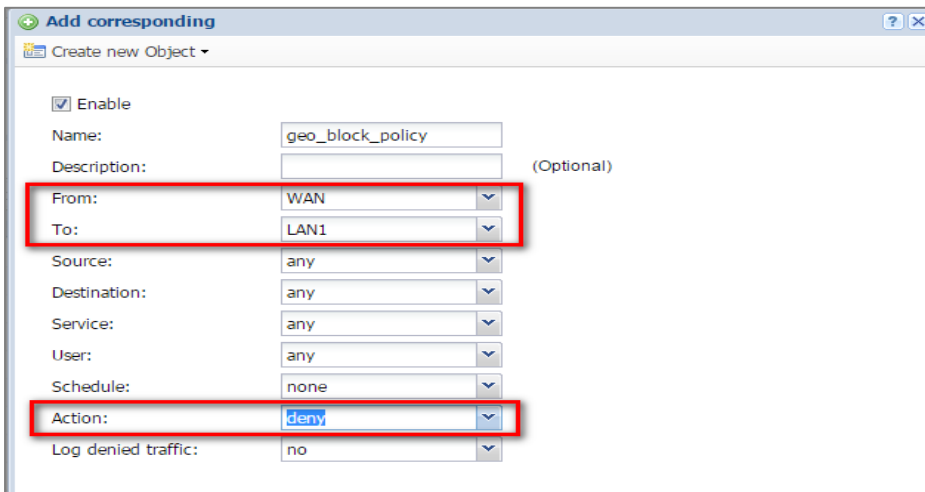
User: any

Schedule: none

Action: allow

Log matched traffic: ☒

Go to **CONFIGURATION > Security Policy > Policy Control**, configure a **Name** for you to identify the **Security Policy** profile. Set traffic from WAN to LAN deny (geo_block_policy in this example).



Add corresponding

Create new Object ▾

☒ Enable

Name: geo_block_policy

Description: (Optional)

From: WAN

To: LAN1

Source: any

Destination: any

Service: any

User: any

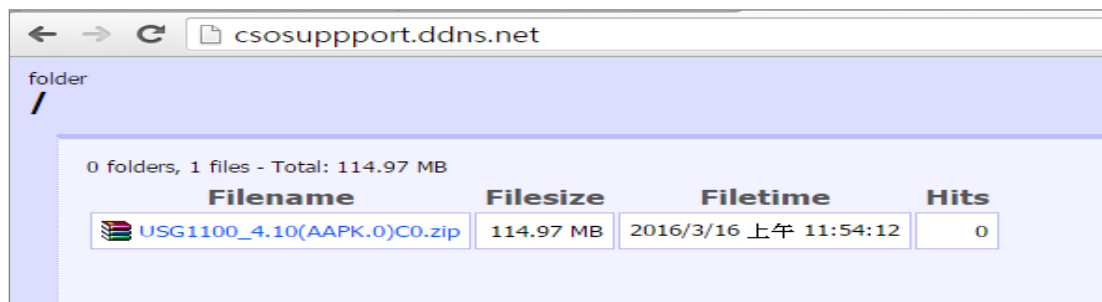
Schedule: none

Action: deny

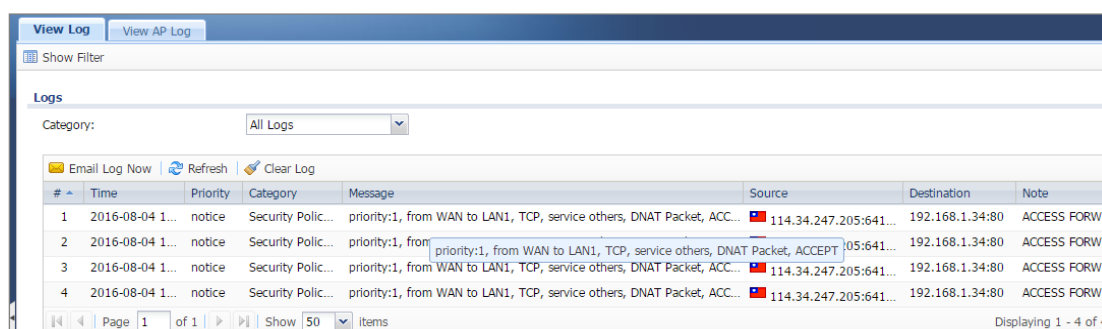
Log denied traffic: ☒

Test the Result

Type <http://csosupport.ddns.net/> into the browser, and the http can be reached.



Go to the ZyWALL/USG **Monitor > Log**, you will see [notice] log message such as below. Traffic matches Geo IP policy will be blocked and shows in message field.



What Could Go Wrong?

1. The Security Policy configured wrong. The traffic cannot access the LAN server.

| # | Time | Priority | Category | Message | Source | Destination | Note |
|---|-----------------|----------|-------------------|---|--------------------|-----------------|--------------|
| 5 | 2016-08-19 1... | alert | Security Polic... | Match default rule, DNAT Packet, DROP [count=3] | 114.34.247.205:... | 192.168.1.34:80 | ACCESS BLOCK |
| 6 | 2016-08-19 1... | alert | Security Polic... | Match default rule, DNAT Packet, DROP [count=3] | 114.34.247.205:... | 192.168.1.34:80 | ACCESS BLOCK |

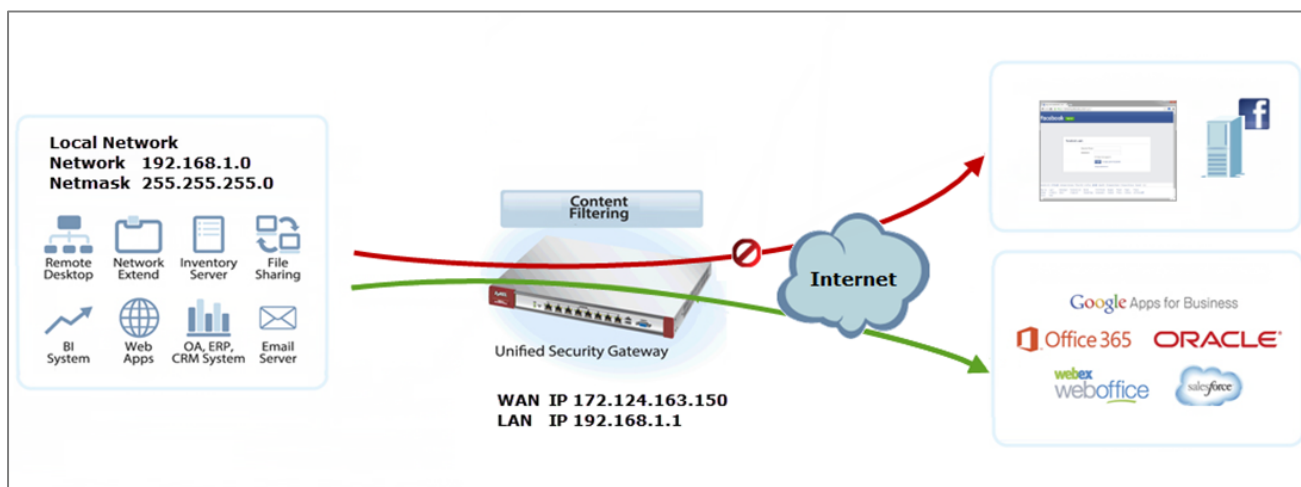
2. The Content-Filter service is expired. Since Geo-IP server is bind with Content-Filter license, there must be available date for Content-Filter service.

How to Configure Content Filter 2.0 with HTTPs Domain Filter

Application Scenario

The Content Filter with HTTPs Domain Filter allows you to block HTTPs websites by category service without SSL-Inspection. The filtering feature is based on 64 categories built in ZyWALL/USG such as pornography, gambling, hacking, etc.

When user makes HTTPS request, the information contains a Server Name Indication (SNI) extension fields in server FQDN. Using the SNI to query category from local cache then cloud database, then take action when it matches the block category in Content Filter profile.



Set Up the Content Filter on the ZyWALL/USG

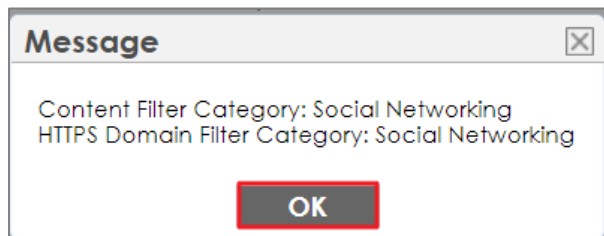
Go to **CONFIGURATION > UTM Profile > Content Filter > Profile > General Settings**. Select **Enable HTTPS Domain Filter for HTTPS traffic**.

| General Settings | Configuration Walkthrough | Troubleshooting | Content Filter |
|---|---------------------------|-----------------|----------------|
| <input type="checkbox"/> Enable Content Filter Report Service Report Server ⓘ | | | |
| <input checked="" type="checkbox"/> Enable HTTPS Domain Filter for HTTPS traffic ⓘ | | | |
| <input checked="" type="checkbox"/> Drop connection when HTTPS connection with SSL V3 or previous version | | | |
| Content Filter Category Service Timeout: <input type="text" value="10"/> (1~60 Seconds) | | | |

Go to **CONFIGURATION > UTM Profile > Content Filter > Profile Management > Add Filter Profile > Test Web Site Category**. Type URL to test the category and click **Test Against Content Filter Category Server**.

| Test Web Site Category | |
|---|---|
| URL to test: | <input type="text" value="https://facebook.com"/> |
| <input type="button" value="Test Against Content Filter Category Server"/> | |
| If you think the category is incorrect, click this link to submit a request to review it. | |

You will see the category recorded in the external content filter server's database for both HTTP and HTTPS Domain you specified.



Go to **CONFIGURATION > UTM Profile > Content Filter > Profile Management > Add Filter File > Custom Service**. Configure a **Name** for you to identify the **Content Filter Profile** and select **Enable Content Filter Category Service**. Select **Block** to prevent users from accessing web pages that match the managed categories that you select below. Select **Log** to record attempts to access web pages that match the unsafe categories that you select below.

General Settings

License Status: Licensed
License Type: Standard
Name: Social_Net_Block
Description: (Optional)

☐ Enable SafeSearch
☒ Enable Content Filter Category Service

☐ Log all web pages

Action for Unsafe Web Pages: Block

☐ Log

Action for Managed Web Pages: Block

☒ Log

Action for Unrated Web Pages: Warn

☐ Log

Action When Category Server Is Unavailable: Warn

☐ Log

Scroll down to the **Managed Categories** section, select categories in this section to control access to specific types of Internet content. You must have the Content Filtering license to filter these categories.

| Category Service | Custom Service | |
|--|---|---|
| <input type="checkbox"/> Advertisements & Pop-Ups | <input type="checkbox"/> Alcohol/Tobacco | <input type="checkbox"/> Arts |
| <input type="checkbox"/> Business | <input type="checkbox"/> Transportation | <input type="checkbox"/> Chat |
| <input type="checkbox"/> Forums & Newsgroups | <input type="checkbox"/> Computers & Technology | <input type="checkbox"/> Criminal Activity |
| <input type="checkbox"/> Dating & Personals | <input type="checkbox"/> Download Sites | <input type="checkbox"/> Education |
| <input type="checkbox"/> Entertainment | <input type="checkbox"/> Finance | <input type="checkbox"/> Gambling |
| <input type="checkbox"/> Games | <input type="checkbox"/> Government | <input type="checkbox"/> Hate & Intolerance |
| <input type="checkbox"/> Health & Medicine | <input type="checkbox"/> Illegal Drugs | <input type="checkbox"/> Job Search |
| <input type="checkbox"/> Streaming Media & Downloads | <input type="checkbox"/> News | <input type="checkbox"/> Non-profits & NGOs |
| <input type="checkbox"/> Nudity | <input type="checkbox"/> Personal Sites | <input type="checkbox"/> Politics |
| <input type="checkbox"/> Pornography/Sexually Explicit | <input type="checkbox"/> Real Estate | <input type="checkbox"/> Religion |
| <input type="checkbox"/> Restaurants & Dining | <input type="checkbox"/> Search Engines/Portals | <input type="checkbox"/> Shopping |
| <input checked="" type="checkbox"/> Social Networking | <input type="checkbox"/> Sports | <input type="checkbox"/> Translators |
| <input type="checkbox"/> Travel | <input type="checkbox"/> Violence | <input type="checkbox"/> Weapons |
| <input type="checkbox"/> Web-based Email | <input type="checkbox"/> General | <input type="checkbox"/> Leisure & Recreation |
| <input type="checkbox"/> Cults | <input type="checkbox"/> Fashion & Beauty | <input type="checkbox"/> Greeting Cards |
| <input type="checkbox"/> Hacking | <input type="checkbox"/> Illegal Software | <input type="checkbox"/> Image Sharing |
| <input type="checkbox"/> Information Security | <input type="checkbox"/> Instant Messaging | <input type="checkbox"/> Peer to Peer |

Set Up the Security Policy on the ZyWALL/USG

Go to **CONFIGURATION > Security Policy > Policy Control**, configure a **Name** for you to identify the **Security Policy** profile. Scroll down to **UTM Profile**, select **Content Filter** and select a profile from the list box (Social_Net_Block in this example).

Create new Object ▼

☒ Enable

Name:

Description: (Optional)

From:

To:

Source:

Destination:

Service:

User:

Schedule:

Action:

Log matched traffic:

UTM Profile

☒ Content Filter: Log:

Set Up the System Policy on the ZyWALL/USG

Go to **CONFIGURATION > System > WWW > Show Advanced Settings > Other**, click **Enable Content Filter HTTPS Domain Filter Block/Warn Page**.

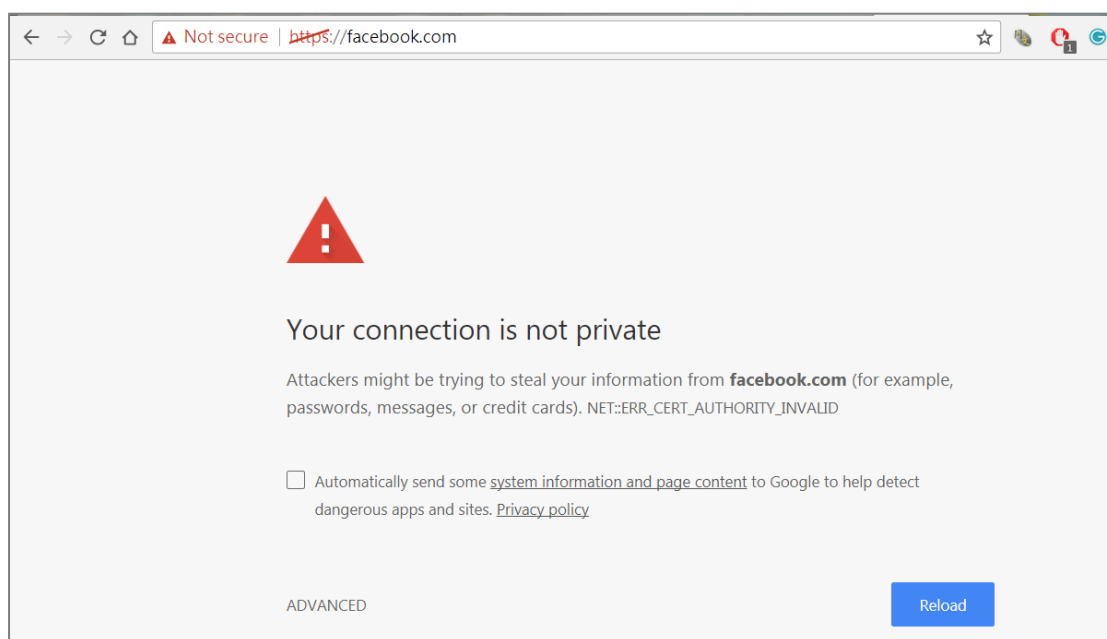
Other

☒ Enable Content Filter HTTPS Domain Filter Block/Warn Page

Block/Warn Page Port:

Test the Result

Type <http://www.facebook.com/> or <https://www.facebook.com/> into the browser, the error message occurs.



Go to the ZyWALL/USG **Monitor > Log**, you will see [alert] log message such as below. HTTP traffic log matches (Content Filter) and HTTPS traffic log matches (HTTPS Domain Filter) in message field.

Monitor > Log

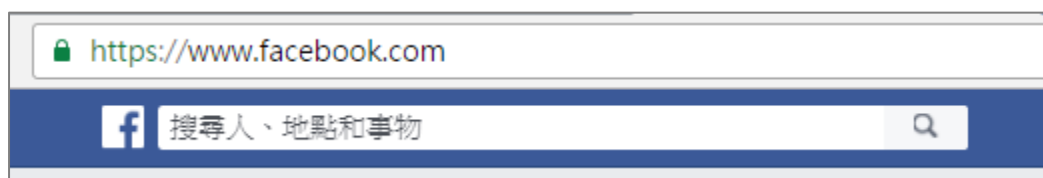
| # | Time | Pri... | Category | Message | Source | Desti... | Note |
|----|-------|--------|--------------|---|----------------|----------|-----------|
| 28 | 20... | alert | Blocked w... | facebook.com : Social Networking, Rule_Id=1, SSI=N (HTTPS Domain... | 192.168.2.3... | 31... | WEB BLOCK |
| 29 | 20... | alert | Blocked w... | facebook.com : Social Networking, Rule_Id=1, SSI=N (HTTPS Domain... | 192.168.2.3... | 31... | WEB BLOCK |
| 30 | 20... | alert | Blocked w... | facebook.com : Social Networking, Rule_Id=1, SSI=N (HTTPS Domain... | 192.168.2.3... | 31... | WEB BLOCK |

What Could Wrong?

1. "Enable HTTPS Domain Filter for HTTPS traffic" is not checked.

| Profile | Trusted Web Sites | Forbidden Web Sites |
|--|---------------------------------|---------------------|
| General Settings Configuration Walkthrough Troubleshooting Content Filter | | |
| <input type="checkbox"/> Enable Content Filter Report Service Report Server | | |
| <input type="checkbox"/> Enable HTTPS Domain Filter for HTTPS traffic i | | |
| <input checked="" type="checkbox"/> Drop connection when HTTPS connection with SSL V3 or previous version i | | |
| Content Filter Category Service Timeout: | <input type="text" value="10"/> | (1~60 Seconds) |

HTTPs traffic will pass.

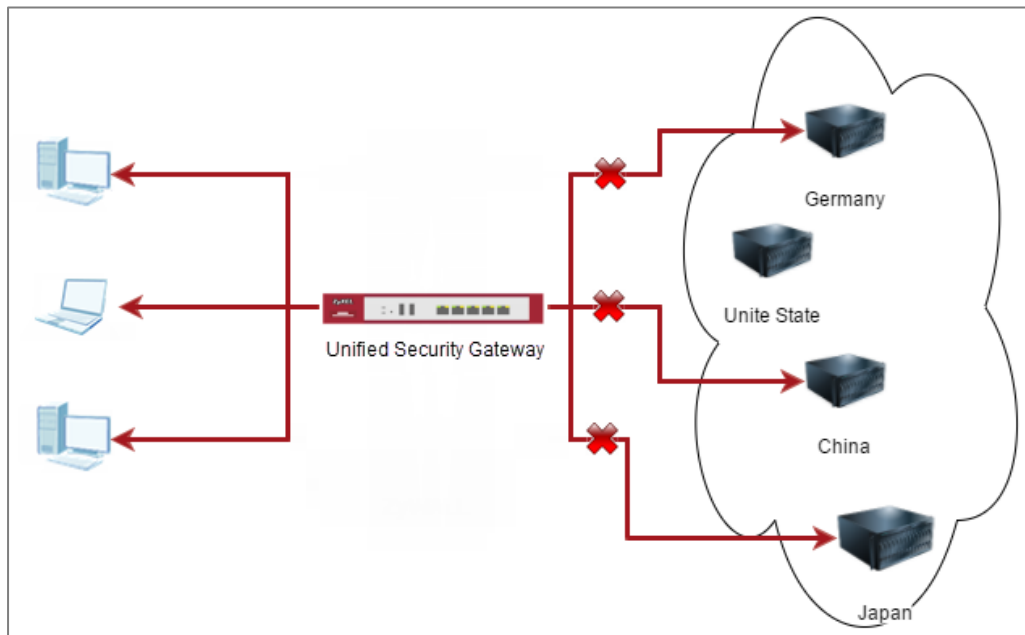



How to block the client accessing to certain country using Geo IP and Content Filter

The Content Filter with Geo IP offers identify the country based on IP address, it allows you to block the client accessing to certain country based on organizational policy.

When user makes HTTP or HTTPS request, ZyWALL/USG query IP address from MaxMind database, then take action when it matches the block country in Content Filter profile.

ZyWALL/USG Geo IP Example



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: 4.25)

Check Geo IP License Status on the ZyWALL/USG

Go to **CONFIGURATION > Licensing > Registration > Service**, the **Geo IP Service** should be **Licensed** to configure this feature.

| # | Service | Status | Service Type | Expiration ... | Count | Action |
|---|---------------------------|---------------|--------------|----------------|-------|-----------------------|
| 1 | Content Filter 2.0 | Licensed | Standard | 2018-7-6 | N/A | Renew |
| 2 | SSL VPN Service | Licensed | Standard | | 60 | Buy |
| 3 | Managed AP Service | Default | Standard | | 4 | Buy |
| 4 | Zymesh Service | Not Licens... | | | N/A | |
| 5 | Concurrent Device Upgr... | Default | Standard | | 200 | Buy |
| 6 | Device HA Pro | Not Licens... | | | N/A | Buy |
| 7 | Firmware Upgrade Service | Not Licens... | | | N/A | |
| 8 | SecuReporter | Not Licens... | | | N/A | Buy |

Set Up the Address Object with Geo IP on the ZyWALL/USG

Go to **CONFIGURATION > Object > Address/Geo IP > Address > Add Address Rule**.

+

Add Address Rule

?

×

Name:

geo1

Address Type:

GEOGRAPHY

Country:

China

OK

Cancel

Go to **CONFIGURATION > Object > Address/Geo IP > Address**, you can see the customized GEOGRAPHY address.

| <div> <div>+</div> <div>Add</div> <div>✎</div> <div>Edit</div> <div>✖</div> <div>Remove</div> <div>🔗</div> <div>Object References</div> </div> | | | | |
|--|----------------|------------------|--------------------|----------|
| # | Name ▲ | Type | IPv4 Address | Refer... |
| 1 | DMZ_SUBNET | INTERFACE SUBNET | ge6-192.168.3.0/24 | 0 |
| 2 | IP6to4-Relay | HOST | 192.88.99.1 | 0 |
| 3 | LAN_SUBNET_GE4 | INTERFACE SUBNET | ge4-192.168.1.0/24 | 0 |
| 4 | LAN_SUBNET_GE5 | INTERFACE SUBNET | ge5-192.168.2.0/24 | 0 |
| 5 | RFC1918_1 | SUBNET | 10.0.0.0/8 | 1 |
| 6 | RFC1918_2 | SUBNET | 172.16.0.0/12 | 1 |
| 7 | RFC1918_3 | SUBNET | 192.168.0.0/16 | 1 |
| 8 | Taiwan | GEOGRAPHY | 🇹🇼 Taiwan-All | 1 |
| 9 | geo1 | GEOGRAPHY | 🇨🇳 China-All | 0 |
| 10 | geo2 | GEOGRAPHY | 🇩🇪 Germany-All | 0 |

Go to **CONFIGURATION > Object > Address/Geo IP > Address Group > Add Address Group Rule**, add all customized GEOGRAPHY address into the same **Member** object.

Add Address Group Rule

Group members

Name:

Description:

Address Type:

Member List

| Available | | Member |
|----------------|----------------------------------|--------|
| === Object === | | |
| Taiwan | | |
| geo1 | <input type="button" value="→"/> | |
| geo2 | <input type="button" value="←"/> | |

Set Up the Security Policy on the ZyWALL/USG

Go to **CONFIGURATION > Security Policy > Policy Control**, configure a **Name** for you to identify the **Security Policy** profile. Set deny Geo IP traffic from LAN to WAN (geo_block_policy in this example).

+

Add corresponding

Create new Object ▼

☒ Enable

Name:

geo_block_policy

Description:

(Optional)

From:

LAN1

▼

To:

WAN

▼

Source:

any

▼

Destination:

geo_block

▼

Service:

any

▼

User:

any

▼

Schedule:

none

▼

Action:

deny

▼

Log denied traffic:

log alert

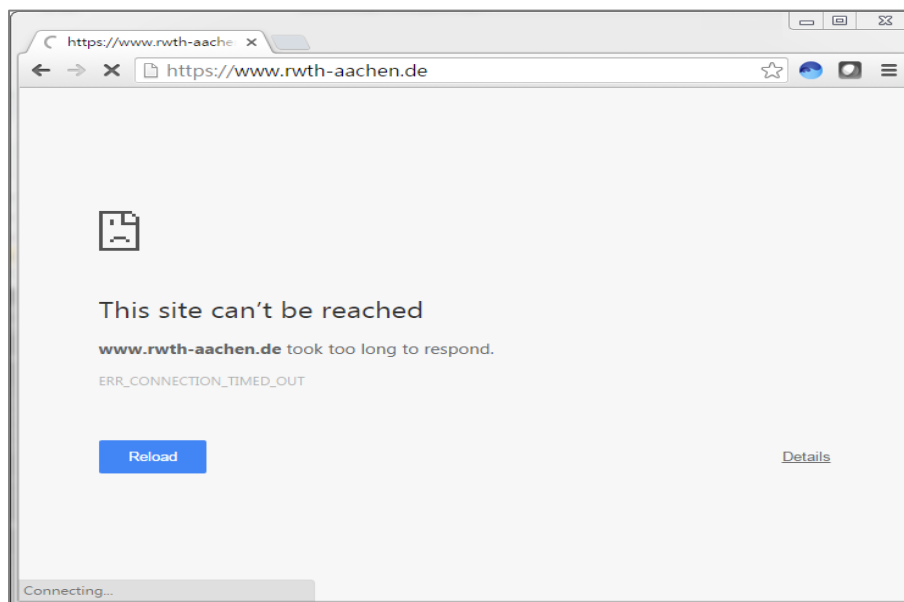
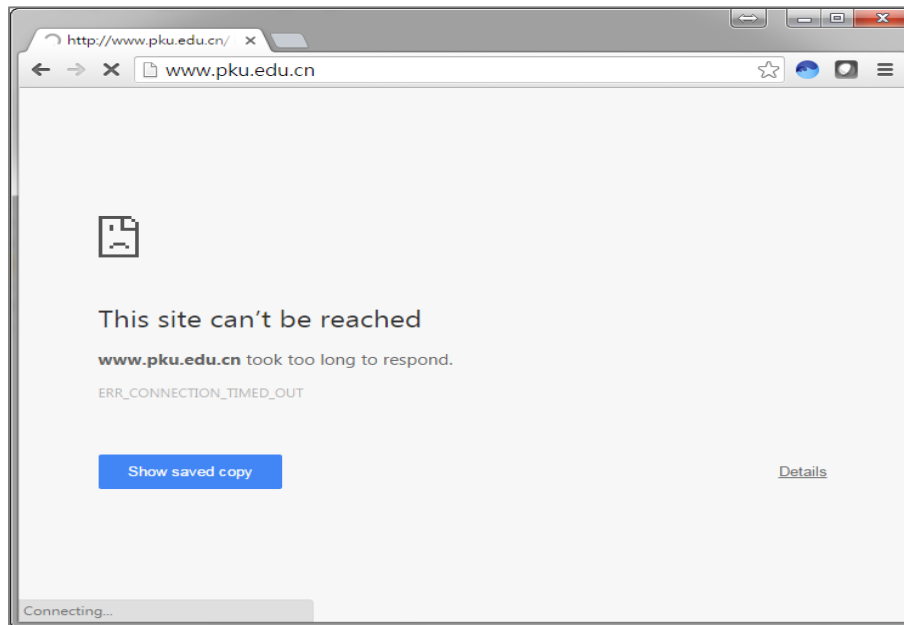
▼

OK

Cancel

Test the Result

Type <http://www.pku.edu.cn/> or <https://www.rwth-aachen.de/> into the browser, sites can't be reached.



Go to the ZyWALL/USG **Monitor > Log**, you will see [notice] log message such as below. Traffic matches Geo IP policy will be blocked and shows in message field.

Logs

Category: All Logs


Email Log NowRefreshClear Log

| # | Ti... | Pr... | Category | Message | Source | Destin... | Note |
|----|-------|-------|---------------|---|----------------|------------|--------------|
| 1 | 2... | al... | Security P... | priority:1, from LAN2 to WAN, TCP, service others, DROP [count=2] | 192.168.2.3... | 61.... | ACCESS BLOCK |
| 2 | 2... | al... | Security P... | priority:1, from LAN2 to WAN, TCP, service others, DROP [count=2] | 192.168.2.3... | 115... | ACCESS BLOCK |
| 3 | 2... | al... | Security P... | priority:1, from LAN2 to WAN, TCP, service others, DROP [count=2] | 192.168.2.3... | 61.... | ACCESS BLOCK |
| 4 | 2... | al... | Security P... | priority:1, from LAN2 to WAN, TCP, service others, DROP [count=2] | 192.168.2.3... | 115... | ACCESS BLOCK |
| 5 | 2... | al... | Security P... | priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3] | 192.168.2.3... | 137... | ACCESS BLOCK |
| 6 | 2... | al... | Security P... | priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3] | 192.168.2.3... | 137... | ACCESS BLOCK |
| 7 | 2... | al... | Security P... | Match default rule, DROP [count=6] | 10.214.30.3... | 10.214.... | ACCESS BLOCK |
| 8 | 2... | al... | Security P... | priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3] | 192.168.2.3... | 61.... | ACCESS BLOCK |
| 9 | 2... | al... | Security P... | priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3] | 192.168.2.3... | 61.... | ACCESS BLOCK |
| 10 | 2... | al... | Security P... | priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3] | 192.168.2.3... | 61.... | ACCESS BLOCK |
| 11 | 2... | al... | Security P... | priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3] | 192.168.2.3... | 61.... | ACCESS BLOCK |
| 12 | 2... | al... | Security P... | priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3] | 192.168.2.3... | 61.... | ACCESS BLOCK |
| 13 | 2... | al... | Security P... | priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3] | 192.168.2.3... | 61.... | ACCESS BLOCK |
| 14 | 2... | al... | Security P... | priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3] | 192.168.2.3... | 162... | ACCESS BLOCK |
| 15 | 2... | al... | Security P... | priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3] | 192.168.2.3... | 162... | ACCESS BLOCK |
| 16 | 2... | al... | Security P... | priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3] | 192.168.2.3... | ... | ACCESS BLOCK |

How to Restrict Web Portal access from the Internet

This example shows how to use the VPN Setup Wizard to create a site-to-site VPN with multiple LAN access to the VPN tunnel. The example instructs how to configure the VPN tunnel between each site and redirect multiple LAN interface traffic to the VPN tunnel. When the VPN tunnel is configured, multiple LAN subnets can be accessed securely.

ZyWALL/USG Restrict Web Portal Access from the Internet

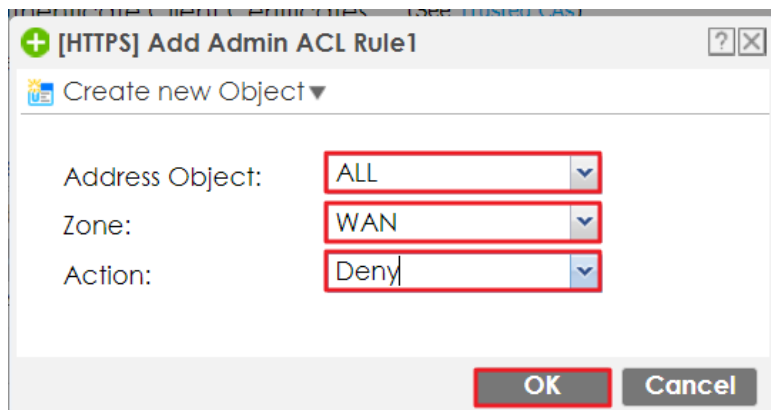
 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG60 (Firmware Version: ZLD 4.25).

Set Up the ZyWALL/USG System Setting

Go to **CONFIGURATION > System > WWW > Admin Service Control > Add Admin ACL**

Rule 1. Set the address access action as **Deny** for **ALL** address in **WAN**.

CONFIGURATION > System > WWW > Admin Service Control > Add Admin ACL Rule 1



HTTPS

☒ Enable

Server Port:

☐ Authenticate Client Certificates (See [Trusted CAs](#))

Server Certificate:

☒ Redirect HTTP to HTTPS

Admin Service Control

+ Add Edit Remove Move

| # | Zone | Address | Action |
|---|------|---------|--------|
| 1 | WAN | ALL | deny |
| - | ALL | ALL | accept |

Test the Web Access

Login to the device via the WAN interface with the administrator's user name and password. The screen will show **Login denied**.

Login to the device via the WAN interface

← → ↻ 🏠

⚠ Not secure | <https://10.214.30.93>

☆ 🔍 🔒 🔄

ZYXEL

VPN300

Enter User Name/Password and click to login.

👤

🔑

Login denied

Login to the device via the LAN interface with the administrator's user name and password. The management portal will be displayed.

Login to the device via the LAN interface

▲ Not secure | <https://192.168.2.1>

ZYXEL

VPN300

Enter User Name/Password and click to login.

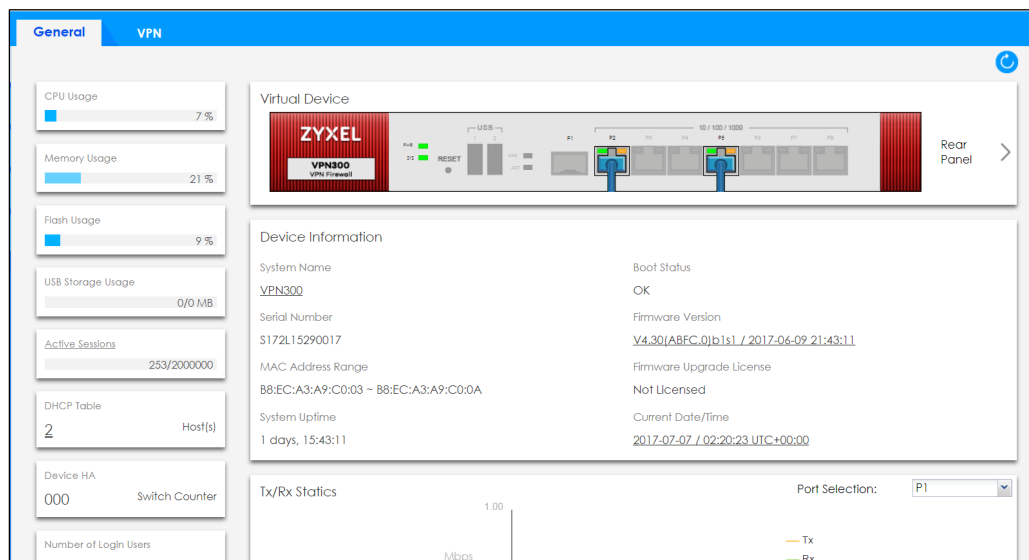
User Name:

Password:

[Login](#) [SSL VPN](#)

Note:

1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.
4. Allow Gears if you are using Google Chrome.



Go to **MONITOR > Log**. You can see that the admin login has been denied access from the WAN interface but it is allowed from the LAN interface.

MONITOR > Log

Logs

Category: User

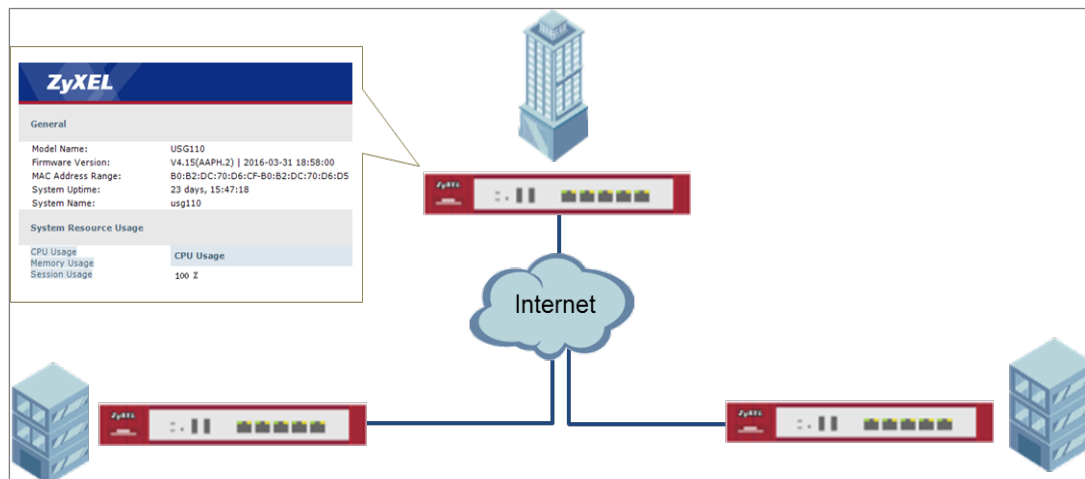
Email Log Now | Refresh | Clear Log

| # | Time | Priority | C... | Message | Source | Destination | Note |
|----|----------|----------|------|---|--------------------|------------------|------------|
| 1 | 2017-... | notice | User | User admin has been denied access from HTTPS | 10.214.30.66:63823 | 10.214.30.93:443 | Account:.. |
| 51 | 2017-... | notice | User | Administrator admin(MAC=3C:97:0E:30:0E:B8) f... | 192.168.2.33 | 192.168.2.1 | Account:.. |


Page 1 of 1 | Show 50 items | Displaying 1 - 2 of 2

How to Setup and Configure Daily Report

This example shows how to set up the data collection and view various statistics about traffic passing through your ZyWALL/USG. When the Daily Report is configured, you will receive statistics report every day.



ZyWALL/USG Setup and Configure Daily Report

 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG110 (Firmware Version: ZLD 4.25).

Set Up the ZyWALL/USG Email Daily Report Setting

Go to **CONFIGURATION > Log & Report > Email Daily Report > General Settings**. Select **Enable Email Daily Report** to send reports by e-mail every day.

CONFIGURATION > Log & Report > Email Daily Report > General Settings

General Settings

☒ Enable Email Daily Report

Type the SMTP server name or IP address. In **Mail From**, type the e-mail address from which the outgoing e-mail is delivered. In **Mail To**, type the e-mail address to which the outgoing e-mail is delivered. Select **SMTP Authentication** if it is necessary to provide a user name and password to the SMTP server.

CONFIGURATION > Log & Report > Email Daily Report > Email Settings

Mail Server

General Settings

Mail Server: mail.zyxel.com.tw (Outgoing SMTP Server Name or IP Address)

Mail Subject: ☐ Append system name ☐ Append date time

Mail Server Port: 25 ☐ TLS Security ☒ STARTTLS ☐ Authenticate Server

Mail From: [redacted]@zyxel.com. (Email Address)

☒ SMTP Authentication

User Name : ZT [redacted]

Password: [redacted]

Retype to Confirm: [redacted]

Schedule

Time For Sending Report: 0 (hours) 0 (minutes)

In the **CONFIGURATION > Log & Report > Email Daily Report > Schedule**. Select the time of day (hours and minutes) when the log is e-mailed. Use 24-hour notation.

CONFIGURATION > Log & Report > Email Daily Report > Schedule

Schedule

Time For Sending Report: 12 (hours) 0 (minutes)

Select the information to include in the report. Types of information include **System Resource Usage**, **Wireless Report**, **Threat Report**, and **Interface Traffic Statistics**.

Select **Reset counters after sending report successfully** if you only want to see statistics for a 24 hour period.

CONFIGURATION > Log & Report > Email Daily Report > Report Items

Report Items

System Resource Usage

- ☒ CPU Usage
- ☒ Memory Usage
- ☒ Session Usage
- ☒ Port Usage

Wireless Report

- ☐ Station Count
- ☐ TX Statistics
- ☐ RX Statistics
- ☒ Content Filter

- ☒ Interface Traffic Statistics
- ☒ DHCP Table

- ☐ Reset counters after sending report successfully

Test the Daily Log Report

Click **Send Report Now** to have the ZyWALL/USG send the daily e-mail report immediately.

CONFIGURATION > Log & Report > Email Daily Report > Email Settings

General Settings

☒ Enable Email Daily Report

Email Settings

Mail Subject:

Handbook mail

Mail To:

@zyxel.com.

(Email Address)

(Email Address)

(Email Address)

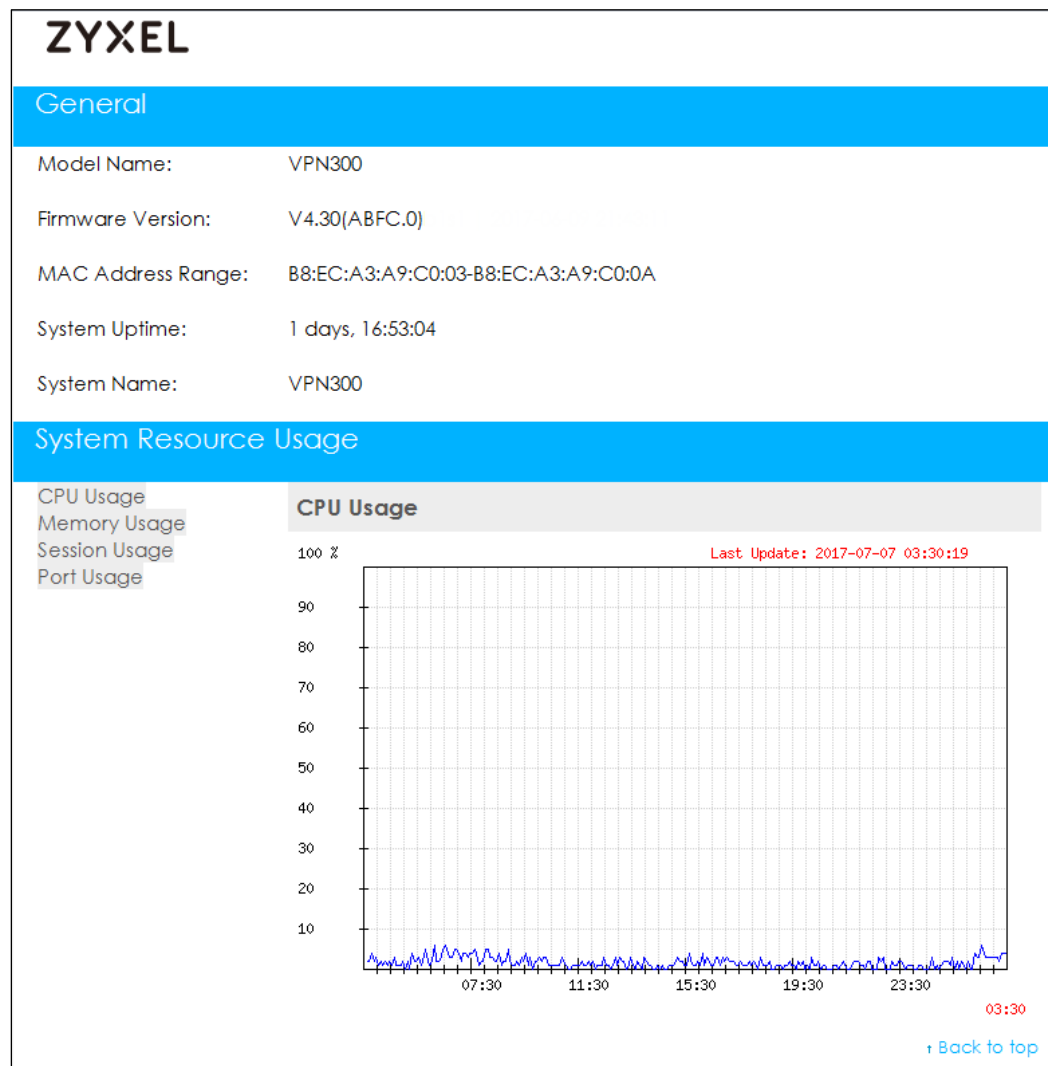
(Email Address)

(Email Address)

Send Report Now

You will receive a daily report mail.

ZyXEL Daily Report Mail



Mail Server

General Settings

Mail Server:

mail.zyxel.com.tw

(Outgoing SMTP Server Name or IP Address)

Mail Subject:

☐ Append system name
 ☐ Append date time

Mail Server Port:

25

☐ TLS Security
 ☒ STARTTLS
 ☐ Authenticate Server

Mail From:

@zyxel.com.

(Email Address)

☒ SMTP Authentication

User Name :

ZT

Password:

.....

Retype to Confirm:

.....

Schedule

Time For Sending Report:

0

(hours)

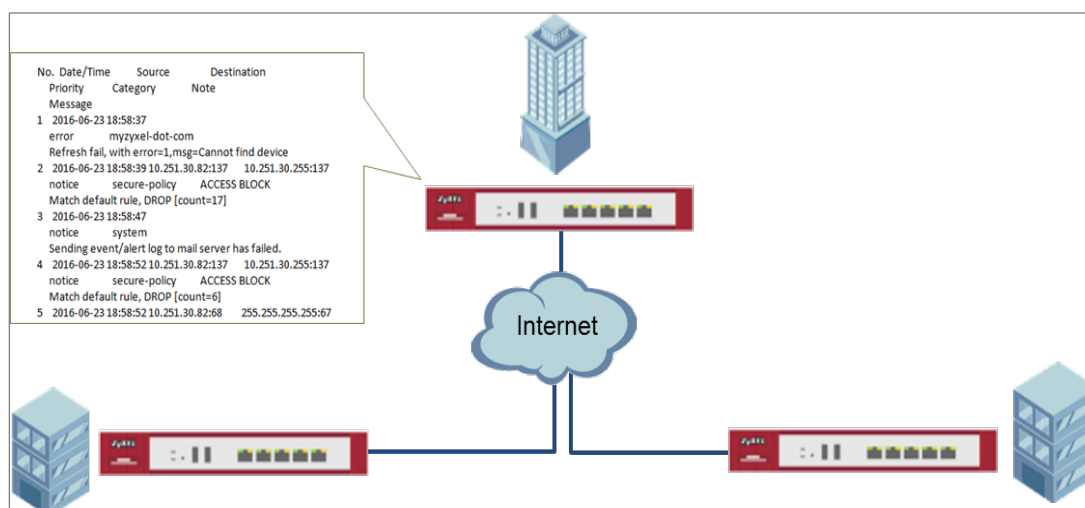
0

(minutes)

Make sure your ZyWALL to WAN security policy allow.

How to Setup and Configure Email Logs

This example shows how to set up the e-mail profiles to mail ZyWALL/USG log messages to the specific destinations. You can also specify which log messages to e-mail, and where and how often to e-mail them. When the Email Logs is configured, you will receive logs email report base on customized schedule.



ZyWALL/USG Setup and Configure E-mail Logs

Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG110 (Firmware Version: ZLD 4.25).

Set Up the ZyWALL/USG Email Logs Setting

1. Go to **CONFIGURATION > Log & Report > Log Settings > System Log > Edit > E-mail Server 1**. Select **Active**. Type the SMTP server name or IP address. In **Mail From**, type the e-mail address from which the outgoing e-mail is delivered. In **Mail To**, type the e-mail address to which the outgoing e-mail is delivered.
2. **Day for Sending Log** is available if the log is e-mailed weekly. Select the day of the week the log is e-mailed.
3. **Time for Sending Log** is available if the log is e-mailed weekly or daily. Select the time of day (hours and minutes) when the log is e-mailed. Use 24-hour notation.
4. Select **SMTP Authentication** if it is necessary to provide a user name and password to the SMTP server.

CONFIGURATION > Log & Report > Log Settings > System Log > Edit > E-mail Server 1

E-mail Server 1

☒ Active

Mail Server: (Outgoing SMTP Server Name or IP Address)

Mail Server Port: ☒ TLS ☒ STARTTLS ☐ Authentica Security

Mail Subject:

Send From: (E-Mail Address)

Send Log to: (E-Mail Address)

Send Alerts to: (E-Mail Address)

Sending Log:

Day for Sending Log:

Time for Sending Log:

☒ SMTP Authentication

User Name :

Password:

Retype to Confirm:

5. Go to **CONFIGURATION > Log & Report > Log Settings > System Log > Edit > Active Log and Alert**. Use the **System Log** drop-down list to change the log settings for all of the log categories.

CONFIGURATION > Log & Report > Log Settings > System Log > Edit > Active Log and Alert.

Active Log and Alert

| Log Category + | System Log | | | E-mail Server 1 | | E-mail Server 2 | |
|-------------------------|-----------------------|-----------------------|-----------------------|-------------------------------------|--------------------------|-------------------------------------|--------------------------|
| | disable | normal | debug | normal | alert | normal | alert |
| Auth | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| - PKI | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| - Authentication Server | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| - Auth. Policy | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| - SSO | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| - Web Authentication | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| - Account | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| - User | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| BWM | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Device HA | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| File manager | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| License | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Log & Report | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Network | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

Active Log and Alert (AP)

| Log Category + | System Log | | | E-mail Server 1 | | E-mail Server 2 | |
|----------------|-----------------------|-----------------------|-----------------------|-------------------------------------|--------------------------|-------------------------------------|--------------------------|
| | disable | normal | debug | normal | alert | normal | alert |
| Auth | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| File manager | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Log & Report | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Network | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Routing | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| System | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Wireless | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

Test the Email Log

You will receive a log mail depends on the time you set in the E-mail Server.

ZyXEL Log Mail

From: zyxelsupporttest.com.tw
To: zyxelsupporttest.com.tw
Cc: zyxelsupporttest.com.tw
Subject: ZyXEL Log Report

| No. | Date/Time | Source | Destination |
|----------|---------------------|--------------|-----------------------|
| Priority | Category | Note | |
| 1 | 2016-06-23 15:52:53 | system | |
| | Message | | |
| 1 | 2016-06-23 15:52:53 | notice | 10.251.30.255:137 |
| | Secure-policy | ACCESS BLOCK | |
| 2 | 2016-06-23 15:52:59 | notice | 10.251.30.255:138 |
| | Secure-policy | ACCESS BLOCK | |
| 3 | 2016-06-23 15:53:03 | notice | 255.255.255.255:17500 |
| | Secure-policy | ACCESS BLOCK | |
| 4 | 2016-06-23 15:53:03 | notice | 10.251.30.255:17500 |
| | Secure-policy | ACCESS BLOCK | |
| 5 | 2016-06-23 15:53:03 | notice | 10.251.30.255:137 |
| | Secure-policy | ACCESS BLOCK | |
| 6 | 2016-06-23 15:53:10 | notice | 10.251.30.255:137 |
| | Secure-policy | ACCESS BLOCK | |
| 7 | 2016-06-23 15:53:10 | notice | 10.251.30.255:137 |
| | Secure-policy | ACCESS BLOCK | |
| 8 | 2016-06-23 15:53:10 | notice | 255.255.255.255:67 |
| | Secure-policy | ACCESS BLOCK | |

What Could Go Wrong?

Make sure your Email settings are all correct.

CONFIGURATION > Log & Report > Email Daily Report > Email Settings

E-mail Server 1

☒ Active

Mail Server: (Outgoing SMTP Server Name or IP Address)

Mail Server Port:

☒ TLS ☒ STARTTLS ☐ Authentica

Security

Mail Subject:

Send From: (E-Mail Address)

Send Log to: (E-Mail Address)

Send Alerts to: (E-Mail Address)

Sending Log:

Day for Sending Log:

Time for Sending Log:

☒ SMTP Authentication

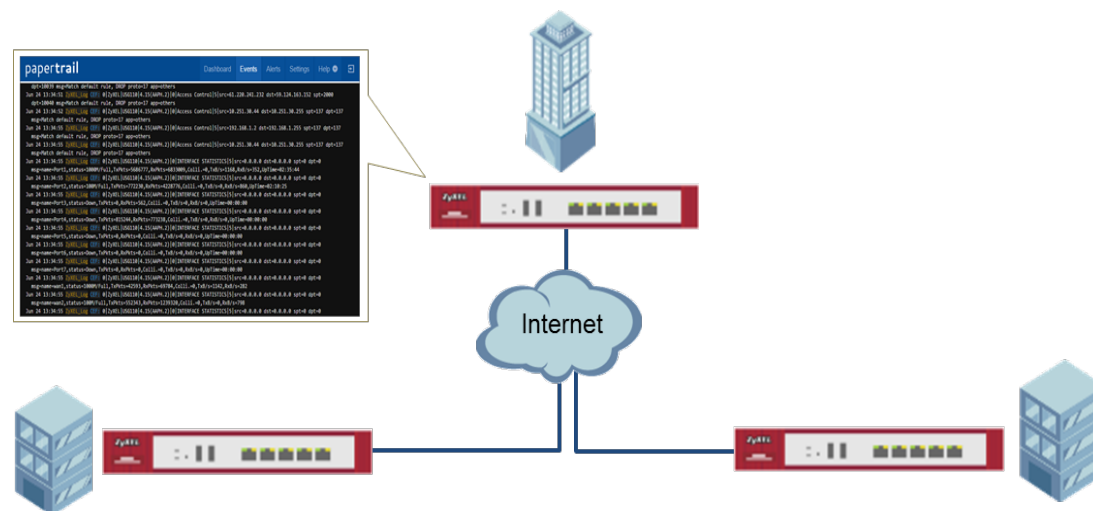
User Name :

Password:

Retype to Confirm:

Make sure your ZyWALL to WAN security policy allow.

This example shows how to set up the syslog server profiles to mail ZyWALL/USG log messages to the specific destinations. You can also specify which log messages to syslog server. When the syslog server is configured, you will receive the real time system logs.



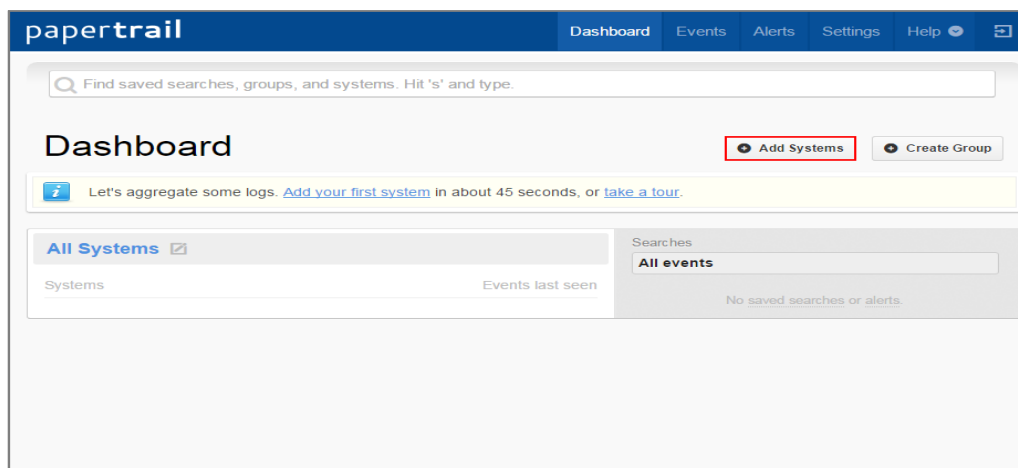
ZyWALL/USG Setup and Configure sending logs to a syslog and Vantage Reports Server

💡 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG110 (Firmware Version: ZLD 4.25).

Register an account on Papertrail: <https://papertrailapp.com>

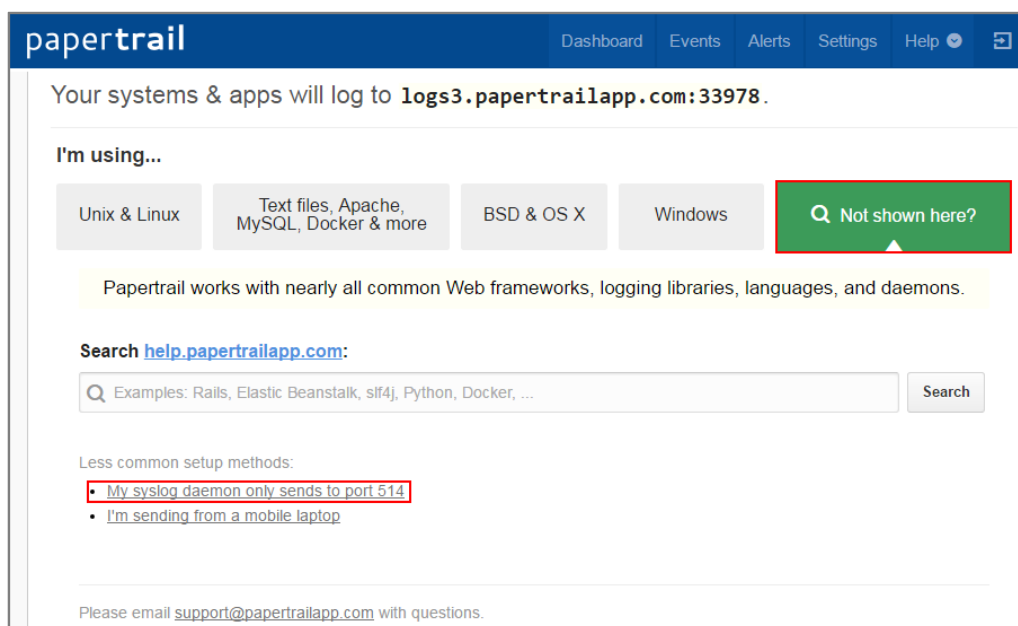
Go to **Dashboard > Add Systems**.

Dashboard > Add Systems



Select **Not shown here?** and **My syslog daemon only sends to port 514**.

Dashboard > Add Systems > I'm using



Select **My syslogd only uses the default port**, set ZyWALL/USG public IP address (111.250.188.9 in this example) and name the log system. Click **Save**.

Dashboard > Add Systems > > I'm using > Choose your situation

papertrail Dashboard Events Alerts Settings Help

Choose your situation:

- A My syslogd only uses the default port**
GNU syslogd and some embedded devices will only log to port 514. A few old Linux distro versions use GNU syslogd (mostly CentOS and Gentoo).
- B I use Cloud Foundry**
Register each app separately. Use Heroku? [Here's how](#).
- C My system's hostname changes**
In rare cases, one system may change hostnames frequently. For example, a roaming laptop which sets its hostname based on DHCP (and roams across networks).

Let's create a log destination on port 514 that works with GNU syslogd.

Multiple systems share 1 IP (NAT)? Enter the same IP for each. We'll do the rest.

111.250.188.9
Example: 208.57.123.234

What should we call it?
ZyXEL_Log
Examples: www42, SYS_1, db1.example.com. Does not need to match hostname.

Save

Write down the Papertrail-provided domain name (logs.papertrailapp.com in this example).

Dashboard > Add Systems > > I'm using > Choose your situation > System Created

papertrail Dashboard Events Alerts Settings Help

Setup ZyXEL_Log... Edit Settings

✓ System created.

ZyXEL_Log will log to logs.papertrailapp.com.

I'm using...

Unix & Linux Text files, Apache, MySQL, Docker & more BSD & OS X Windows Q Not shown here?

1 See which logger your system uses. Run:

```
ls -d /etc/*syslog*
```

Which filename is listed?

✓ rsyslog.conf

Set Up the ZyWALL/USG Remote Server Setting

1. Go to **CONFIGURATION > Log & Report > Log Settings > Remote Server > Edit**. Set **Log Format** to be **CEF/Syslog**. Type the **Server Address** to be the Papertrail- provided domain name (logs.papertrailpp.com in this example).
2. Use the **System Log** drop-down list to change the log settings for all of the log categories.

CONFIGURATION > Log & Report > Log Settings > Remote Server > Edit

Log Settings for Remote Server

☒ Active

Log Format: CEF/Syslog

Server Address: logs.papertrailpp.com (Server Name or IP Address)

Log Facility: Local 1

Active Log

| Log Category + | Selection | | |
|----------------|----------------------------------|-----------------------|-----------------------|
| | disable | normal | debug |
| + Auth | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| + BWM | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| + Device HA | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| + File manager | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| + License | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| + Log & Report | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| + Network | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| + None | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Test the Remote Server

You will receive a log mail depends on the time you set in the E-mail Server.

ZyXEL Log Mail

| papertrail | | Dashboard | Events | Alerts | Settings | Help | |
|---|--|-----------|--------|--------|----------|------|--|
| dpt=10039 | msg=Match default rule, DROP proto=17 app=others | | | | | | |
| Jun 24 13:34:51 | ZyXEL_Log CEF: 0 ZyXEL USG110 4.15(AAPH.2) 0 Access Control 5 src=61.220.241.232 dst=59.124.163.152 spt=2000 | | | | | | |
| dpt=10040 | msg=Match default rule, DROP proto=17 app=others | | | | | | |
| Jun 24 13:34:52 | ZyXEL_Log CEF: 0 ZyXEL USG110 4.15(AAPH.2) 0 Access Control 5 src=10.251.30.44 dst=10.251.30.255 spt=137 dpt=137 | | | | | | |
| msg=Match default rule, DROP proto=17 app=others | | | | | | | |
| Jun 24 13:34:55 | ZyXEL_Log CEF: 0 ZyXEL USG110 4.15(AAPH.2) 0 Access Control 5 src=192.168.1.2 dst=192.168.1.255 spt=137 dpt=137 | | | | | | |
| msg=Match default rule, DROP proto=17 app=others | | | | | | | |
| Jun 24 13:34:55 | ZyXEL_Log CEF: 0 ZyXEL USG110 4.15(AAPH.2) 0 Access Control 5 src=10.251.30.44 dst=10.251.30.255 spt=137 dpt=137 | | | | | | |
| msg=Match default rule, DROP proto=17 app=others | | | | | | | |
| Jun 24 13:34:55 | ZyXEL_Log CEF: 0 ZyXEL USG110 4.15(AAPH.2) 0 INTERFACE STATISTICS 5 src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0 | | | | | | |
| msg=name=Port1,status=100M/Full,TxPkts=5686777,RxPkts=6833009,Colli.=0,TxB/s=1168,RxB/s=352,UpTime=02:35:44 | | | | | | | |
| Jun 24 13:34:55 | ZyXEL_Log CEF: 0 ZyXEL USG110 4.15(AAPH.2) 0 INTERFACE STATISTICS 5 src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0 | | | | | | |
| msg=name=Port2,status=100M/Full,TxPkts=772230,RxPkts=4228776,Colli.=0,TxB/s=0,RxB/s=860,UpTime=02:10:25 | | | | | | | |
| Jun 24 13:34:55 | ZyXEL_Log CEF: 0 ZyXEL USG110 4.15(AAPH.2) 0 INTERFACE STATISTICS 5 src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0 | | | | | | |
| msg=name=Port3,status=Down,TxPkts=0,RxPkts=562,Colli.=0,TxB/s=0,RxB/s=0,UpTime=00:00:00 | | | | | | | |
| Jun 24 13:34:55 | ZyXEL_Log CEF: 0 ZyXEL USG110 4.15(AAPH.2) 0 INTERFACE STATISTICS 5 src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0 | | | | | | |
| msg=name=Port4,status=Down,TxPkts=815244,RxPkts=773238,Colli.=0,TxB/s=0,RxB/s=0,UpTime=00:00:00 | | | | | | | |
| Jun 24 13:34:55 | ZyXEL_Log CEF: 0 ZyXEL USG110 4.15(AAPH.2) 0 INTERFACE STATISTICS 5 src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0 | | | | | | |
| msg=name=Port5,status=Down,TxPkts=0,RxPkts=0,Colli.=0,TxB/s=0,RxB/s=0,UpTime=00:00:00 | | | | | | | |
| Jun 24 13:34:55 | ZyXEL_Log CEF: 0 ZyXEL USG110 4.15(AAPH.2) 0 INTERFACE STATISTICS 5 src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0 | | | | | | |
| msg=name=Port6,status=Down,TxPkts=0,RxPkts=0,Colli.=0,TxB/s=0,RxB/s=0,UpTime=00:00:00 | | | | | | | |
| Jun 24 13:34:55 | ZyXEL_Log CEF: 0 ZyXEL USG110 4.15(AAPH.2) 0 INTERFACE STATISTICS 5 src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0 | | | | | | |
| msg=name=Port7,status=Down,TxPkts=0,RxPkts=0,Colli.=0,TxB/s=0,RxB/s=0,UpTime=00:00:00 | | | | | | | |
| Jun 24 13:34:55 | ZyXEL_Log CEF: 0 ZyXEL USG110 4.15(AAPH.2) 0 INTERFACE STATISTICS 5 src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0 | | | | | | |
| msg=name=wan1,status=100M/Full,TxPkts=42593,RxPkts=69784,Colli.=0,TxB/s=1142,RxB/s=282 | | | | | | | |
| Jun 24 13:34:55 | ZyXEL_Log CEF: 0 ZyXEL USG110 4.15(AAPH.2) 0 INTERFACE STATISTICS 5 src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0 | | | | | | |
| msg=name=wan2,status=100M/Full,TxPkts=552343,RxPkts=1239320,Colli.=0,TxB/s=0,RxB/s=798 | | | | | | | |
| Jun 24 13:34:55 | ZyXEL_Log CEF: 0 ZyXEL USG110 4.15(AAPH.2) 0 INTERFACE STATISTICS 5 src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0 | | | | | | |

What Could Go Wrong?

Make sure your **Log settings for Remote Server** are all correct.

CONFIGURATION > Log & Report > Log Settings > Remote Server

Log Settings for Remote Server

☒ Active

Log Format: CEF/Syslog

Server Address: logs.papertrailapp (Server Name or IP Address)

Log Facility: Local 1

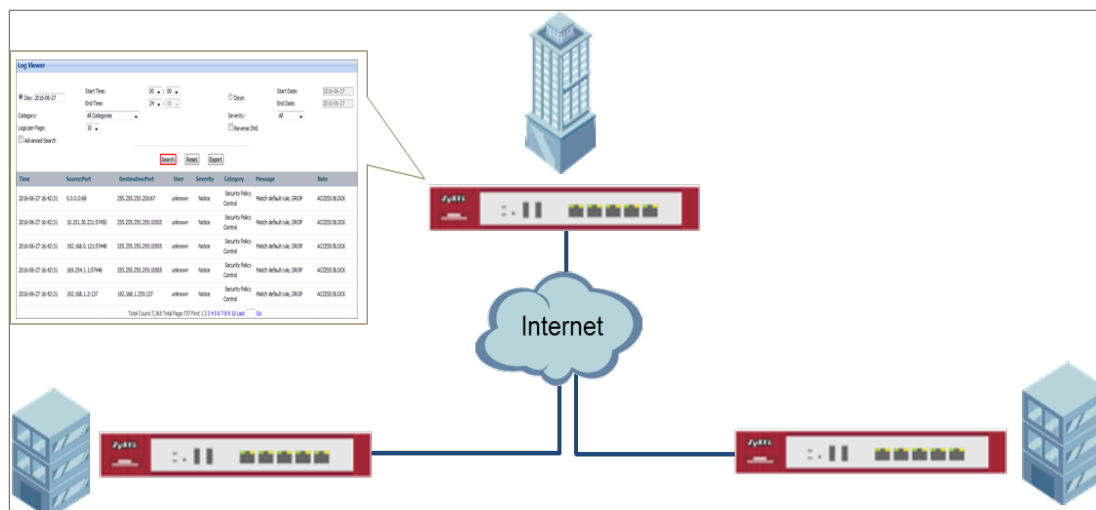
Active Log

| Log Category + | disable | normal | debug |
|----------------|-----------------------|-----------------------|-----------------------|
| + Auth | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| + BWM | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| + Device HA | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| + File manager | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| + License | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| + Log & Report | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| + Network | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| + None | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |


Make sure your ZyWALL to WAN security policy allow traffic to log server.

How to Setup and send logs to a Vantage Reports Server

This example shows how to set up the Vantage Report Server profiles to mail ZyWALL/USG log messages to the specific destinations. You can also specify which log messages to Vantage Report Server. When the Vantage Report Server is configured, you will receive the real time system logs.

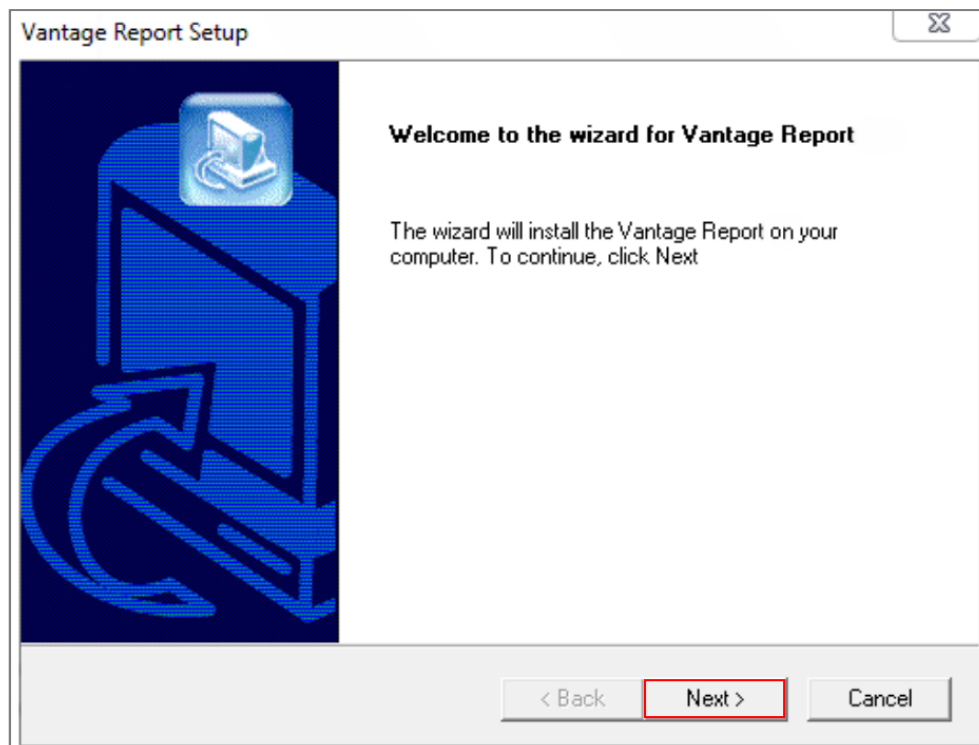


ZyWALL/USG Setup and Configure sending logs to a syslog and Vantage Reports Server

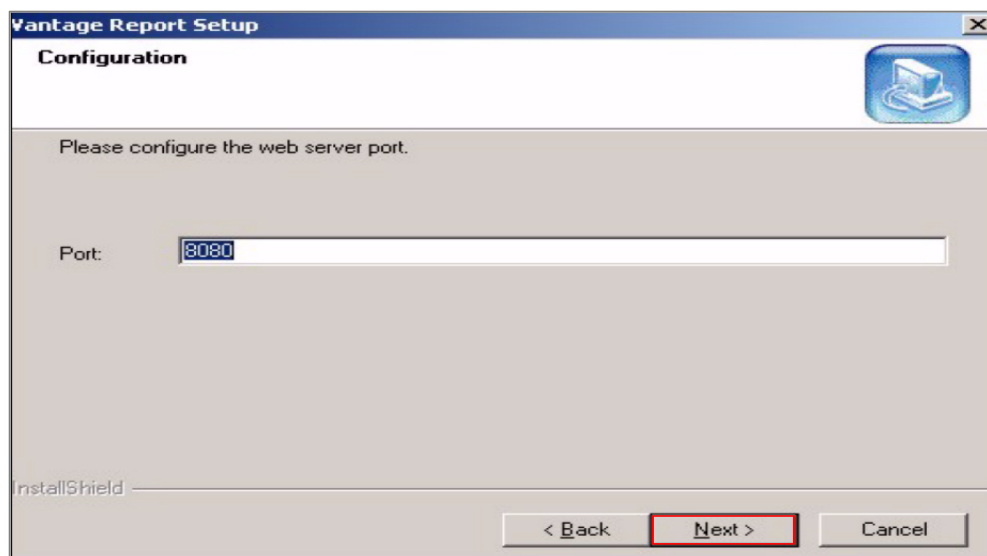
 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG110 (Firmware Version: ZLD 4.25).

Set Up the VRPT Server

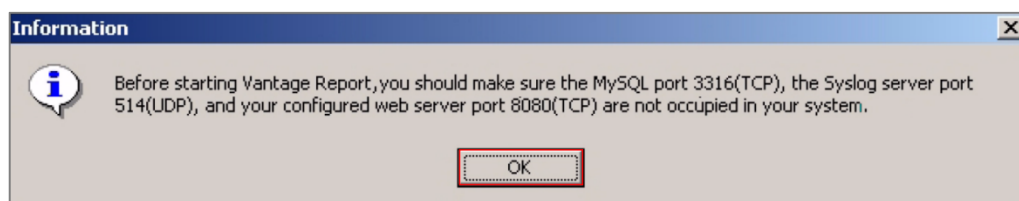
1. The Vantage Report server must have register an account in <http://www.myZyXEL.com>.
2. Install VRPT software:
3. <http://www.zyxel.com/support/DownloadLandingSR.shtml?c=gb&l=en&kbid=M-01339&md=VRPT>
4. Unzipped the file and click **Vantage Reepport.exe** to start installing Vantage Report.
Then, the Vantage Report installation wizard appears. Click **Next**.



5. Enter the port number you want Vantage Report to use for web services. Make sure this port number does not conflict with the other services in your network. Click **Next**.



6. Check if any applications also use port 3316 (TCP), 514 (UDP) or 8080 (UDP) by entering "netstat -a" into the command line. Uninstall them if any. Click **OK**.

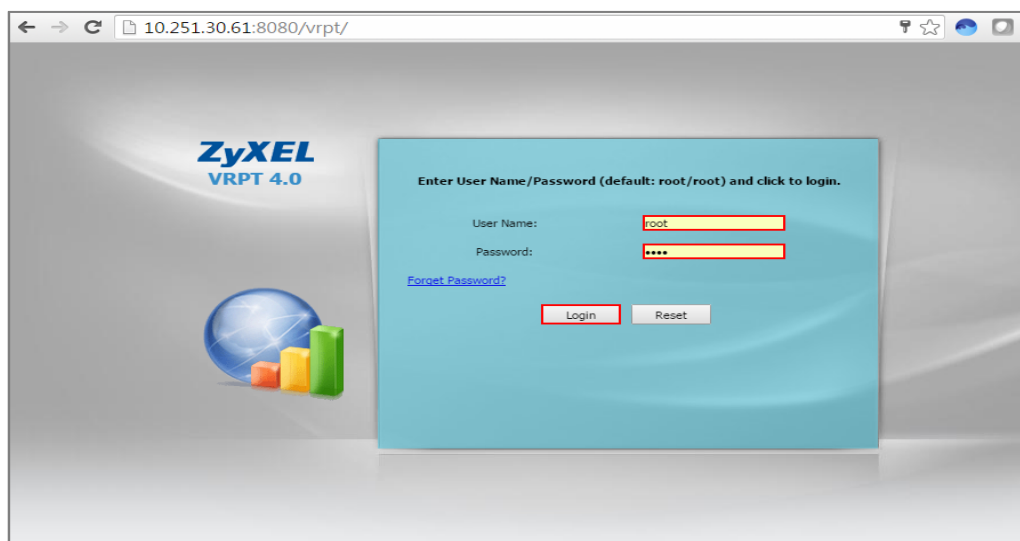


When you finish installing Vantage Report, restart the Vantage Report server.

7. Open the browser window and go to <http://a.b.c.d:xxxxxx/vrpt>, where **a.b.c.d** is the IP address of the Vantage Report server. If you open the configurator on the same computer on which you installed Vantage Report server, enter **localhost**.

Xxxx is the port number you entered during installation (10.251.30.61:8080/vrpt/ in this example).

In the login screen, enter default login **User Name** and **Password: root**.



8. Go to **Dashboard > License Information > Manage Device**, click **Add Device**, the **Add Device** screen appears on the left side. Enter the **Name** of the device you want to add to Vantage Report. Enter the LAN **MAC** address of the device you want to add. Select the model **Type** of the device you want to add. Click the **Add** button.

Dashboard > License Information > Manage Device

The screenshot shows the ZyXEL web interface. On the left, there is a sidebar with a tree view showing 'root' and 'usg110'. A red box highlights the 'Add Device' dialog box. The dialog has fields for 'Name', 'MAC', 'Type' (set to 'ZyWALL 110'), and 'Note'. There is an 'Add' button at the bottom. On the right, the 'Dashboard' section is visible. It contains two panels: 'Server Information' and 'License Information'. The 'Server Information' panel shows details like Software Version (4.0.05.61.00), Release Date (2014-09-15), Free Disk Space (55GB), and memory usage. The 'License Information' panel shows Status (Full Version), Account on myzyxel.com (MichelleTest), Authentication Code(AC) (05509D53671C821CD16CF4D210DF4E93880C), Max Supported Devices (100), License Allowed Devices (1), and Managed Devices (1). A red box highlights the '1' in the 'Managed Devices' row. At the bottom right of the 'License Information' panel, there is an 'Add Device' button and the text 'Copyright © ZyXEL Communications Corporation'.

Set Up the ZyWALL/USG Remote Server Setting

Go to **CONFIGURATION > Log & Report > Log Settings > Remote Server > Edit**. Set **Log Format** to be **VRPT/Syslog**. Type the **Server Address** to be the Vantage Report server IP address (10.251.30.61 in this example).

Use the **System Log** drop-down list to change the log settings for all of the log categories.

CONFIGURATION > Log & Report > Log Settings > Remote Server > Edit

Log Settings for Remote Server

☒ Active

Log Format: VRPT/Syslog

Server Address: 10.251.30.61 (Server Name or IP Address)

Log Facility: Local 1

Active Log (AC)

Selection

| # | Log Category | Selection |
|---|-----------------------|--|
| 1 | Account | <input checked="" type="radio"/> <input checked="" type="radio"/> <input checked="" type="radio"/> |
| 2 | ADP | <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> |
| 3 | Anti-Spam | <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> |
| 4 | Anti-Virus | <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> |
| 5 | AP Firmware | <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> |
| 6 | Application Patrol | <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> |
| 7 | Auth. Policy | <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> |
| 8 | Authentication Server | <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> |
| 9 | Blocked web sites | <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> |

Test the Remote Server

In the VRPT Sever, go to **Logs > Log Viewer**, click **Search**. The screen displays the device log information. (It may take 5 - 10 minutes to display the log after just added the device)

VRPT Server > Logs > Log Viewer

Log Viewer

Day: 2016-06-27 Start Time: 00 : 00 End Time: 24 : 00 Days: ☐ Start Date: 2016-06-27 End Date: 2016-06-27

Category: All Categories Severity: All

Logs per Page: 10 ☐ Advanced Search ☐ Reverse DNS

Search Reset Export

| Time | Source:Port | Destination:Port | User | Severity | Category | Message | Note |
|---------------------|---------------------|-----------------------|---------|----------|-------------------------|--------------------------|--------------|
| 2016-06-27 16:42:31 | 0.0.0.0:68 | 255.255.255.255:67 | unknown | Notice | Security Policy Control | Match default rule, DROP | ACCESS BLOCK |
| 2016-06-27 16:42:31 | 10.251.30.231:57450 | 255.255.255.255:10505 | unknown | Notice | Security Policy Control | Match default rule, DROP | ACCESS BLOCK |
| 2016-06-27 16:42:31 | 192.168.0.121:57448 | 255.255.255.255:10505 | unknown | Notice | Security Policy Control | Match default rule, DROP | ACCESS BLOCK |
| 2016-06-27 16:42:31 | 169.254.1.1:57446 | 255.255.255.255:10505 | unknown | Notice | Security Policy Control | Match default rule, DROP | ACCESS BLOCK |
| 2016-06-27 16:42:31 | 192.168.1.2:137 | 192.168.1.255:137 | unknown | Notice | Security Policy Control | Match default rule, DROP | ACCESS BLOCK |

Total Count:7,365 Total Page:737 First 1 2 3 4 5 6 7 8 9 10 Last Go

What Could Go Wrong?

Make sure your **Log settings for Remote Server** are all correct.

CONFIGURATION > Log & Report > Log Settings > Remote Server

Log Settings for Remote Server

☒ Active

Log Format: VRPT/Syslog

Server Address: 10.251.30.61 (Server Name or IP Address)

Log Facility: Local 1

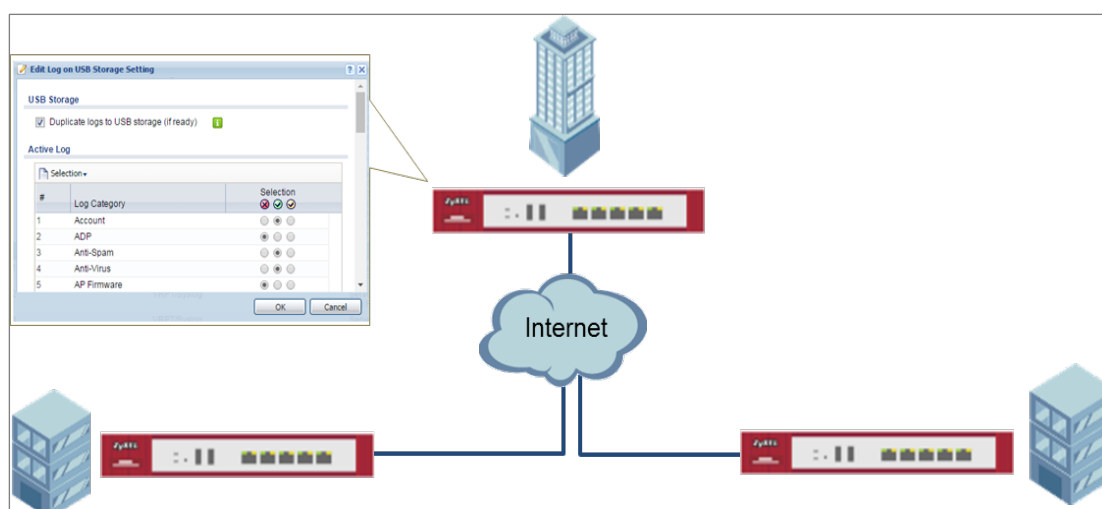
Active Log (AC)

| # | Log Category | Selection |
|---|-----------------------|--|
| 1 | Account | <input checked="" type="radio"/> <input checked="" type="radio"/> <input checked="" type="radio"/> |
| 2 | ADP | <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> |
| 3 | Anti-Spam | <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> |
| 4 | Anti-Virus | <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> |
| 5 | AP Firmware | <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> |
| 6 | Application Patrol | <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> |
| 7 | Auth. Policy | <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> |
| 8 | Authentication Server | <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> |
| 9 | Blocked web sites | <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> |


Make sure your ZyWALL to WAN security policy allow traffic to log server.

How to Setup and send logs to the USB storage

This example shows how to use the USB device to store the system log information.



ZyWALL/USG enable and send logs to the USB storage

 **Note:** Only connect one USB device. It must allow writing (it cannot be read-only) and use the FAT16, FAT32, EXT2, or EXT3 file system. This example was tested using USG110 (Firmware Version: ZLD 4.25).

Set Up the USB System Settings

Go to **CONFIGURATION > System > USB Storage > Settings > General**. Select **Activate USB storage service** if you want to use the connected USB device(s).

Set a number and select a unit (MB or %) to have the ZyWALL/USG send a warning message when the remaining USB storage space is less than the value you set here.

CONFIGURATION > System > USB Storage > Settings > General

General

☒ Activate USB storage service

Disk full warning when remaining space is less than:

100

MB

MB

%

Set Up the USB Log Storage

Go to **CONFIGURATION > Log & Report > Log Settings**, select **USB Storage** and click **Activate**. Click **Apply** to save your changes.

CONFIGURATION > Log & Report > Log Settings

| Log Settings | | | | |
|--|--------|-----------------|-------------|---|
| Edit Activate Inactivate | | | | |
| # | Status | Name | Log Format | Summary |
| 1 | | System Log | Internal | E-mail Server 1 Mail Server: mail.zyxel.com.tw Mail Subject: Handbook test Send From: Chris.liao@zyxel.com.tw Send Log to: Chris.liao@zyxel.com.tw Send Alert to: Schedule: Send log daily at 10:00 |
| 2 | | System Log | Internal | E-mail Server 2 Mail Server: Mail Subject: Send From: Send Log to: Send Alert to: Schedule: Send log when full. |
| 3 | | USB Storage | Internal | USB Status: Ready |
| 4 | | Remote Server 1 | VRPT/Syslog | Server Address: Log Facility: Local 1 |
| 5 | | Remote Server 2 | VRPT/Syslog | Server Address: Log Facility: Local 1 |
| 6 | | Remote Server 3 | VRPT/Syslog | Server Address: Log Facility: Local 1 |
| 7 | | Remote Server 4 | VRPT/Syslog | Server Address: Log Facility: Local 1 |

[Page 1 of 1](#)
[Show 50 items](#)
Displaying 1 - 7 of 7

Go to **CONFIGURATION > Log & Report > Log Settings > USB Storage > Edit**. Select **Duplicate logs to USB storage (if ready)** to have the ZyWALL/USG save a copy of its system logs to a connected USB storage device. Use the **Selection** drop-down list to change the log settings for all of the log categories.

CONFIGURATION > Log & Report > Log Settings

USB Storage
☒ Duplicate logs to USB storage (if ready) ⓘ

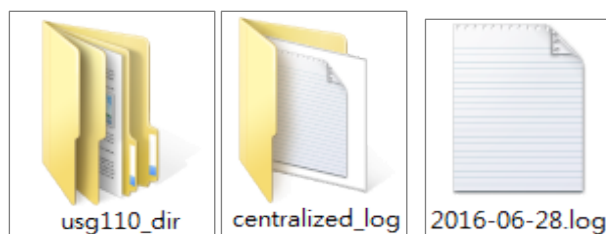
Log Keep duration
☐ Enable log keep duration
 Keep duration: (1-365 days)

Active Log

| Log Category + | disable | Selection normal | debug |
|----------------|----------------------------------|-----------------------|-----------------------|
| + Auth | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| + BWM | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| + Device HA | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| + File manager | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| + License | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| + Log & Report | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| + Network | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| + None | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| + Routing | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| + Security | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| + System | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| + UTM | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| + VPN | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| + Wireless | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Check the USG Log Files

Connect the USB to PC and you can find the files in the following path: \Model Name_dir\centralized_log\YYYY-MM-DD.log

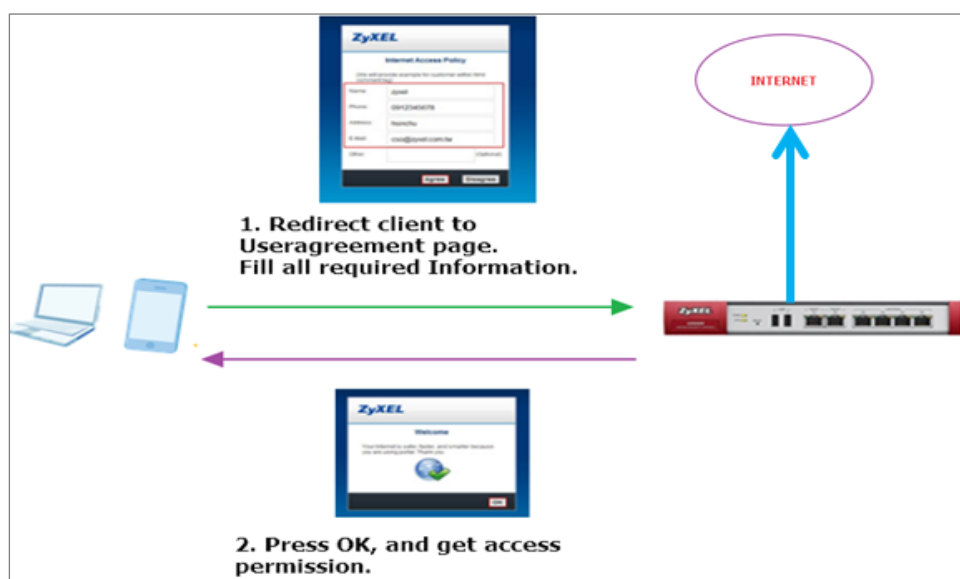


How to Activate a Free Access Hotspot

Some hotels need to provide free Internet services to hundreds of guests on a daily

basis, and managing the Internet access for so many people can be very complicated without the right equipment. With web authentication methods such as user agreement and web portal, hotel guests are redirected to a web-based authentication portal upon the first attempt to access the network. In some countries, the law requires the identification and tracking of users who use public Internet access. The USG1100 can authenticate people by forcing them to receive an authentication code via SMS on their phone. In this way, the USG1100 can authorize the user's Internet access via their mobile phone number and keep track of the device in case of illegal activities via the hotspot. Guests can get free access to the Internet in a matter of seconds simply by entering all required personal contact information and agreeing to the policy of user agreement. If a user that does not have a guest account wants to access the free Internet for a specified period of time, his or her mobile phone number must be entered to receive the guest account information by SMS.

User Agreement



Configuration Guide Network Conditions

- WAN: 10.251.31.112
- LAN 1: 192.168.1.1/255.255.255.0
- User's laptop: 192.168.1.33

Set up the Free Access Hotspot

Configurations on the USG1100

The user agreement of this feature allows clients to access the Internet without a guest account. An advertisement webpage is used as the first page when an authenticated user attempts to access the Internet.

1. On the USG1100, go to **Configuration > Web Authentication > General**. Select **Enable Web Authentication** and click **Add** in the **Web Authentication Policy Summary** section.

(1) Select **Enable Policy**.

(2) Select **Lan_Subnet_GE3**

(3) Select **default-user-agreement** as the **Authentication Type**.

(4) Click **OK** to add the policy.

General Settings

☒ Enable Policy

Description: (Optional)

User Authentication Policy

Incoming Interface:

Source Address: INTERFACE SUBNET, 192.168.1.0/24

Destination Address:

Schedule:

Authentication:

☒ Single Sign-on

☒ Force User Authentication

Authentication Type:

Web Authentication Policy Summary

| # | St... | Priority | Incomin... | Source | Destination | Schedule | Authenti... | Authenticati... | Descripti... |
|---|-------|----------|------------|---------------|-------------|----------|-------------|-----------------|--------------|
| 1 | | 1 | any | LAN_SUBNET... | any | none | SSO/force | default-user... | |
| 2 | | Default | any | any | any | none | unneces... | n/a | n/a |

Page 1 of 1 Show 50 Items Displaying 1 - 2 of 2

Go to

Configuration > Hotspot > Advertisement.

(1) Select **Enable Advertisement**.

(2) Add the URL of the website that you want to advertise.

ZyXEL USG1100 Welcome admin | Logout | ? Help | About | Site Map

CONFIGURATION

- Quick Setup
- Licensing
- Wireless
- Network
 - Interface
 - Routing
 - DDNS
 - NAT
 - Redirect Service
 - ALG
 - UPnP

Advertisement

General Settings

☒ Enable Advertisement

Advertisement Summary

| # | Name | URL |
|---|-------|----------------------|
| 1 | zyxel | http://www.zyxel.com |

Page 1 of 1 Show 50 Items

Test the User Agreement and Advertisement Webpage

1. When a client attempts to access the Internet via a browser, he/she will be

redirected to the user agreement page.



The image shows a ZyXEL web page titled "Internet Access Policy". At the top left is the ZyXEL logo. Below it is a link "View Mobile Version". The main heading is "Internet Access Policy". A note in parentheses says "(We will provide example for customer within html comment tag)". Below this is a form with five input fields: "Name:" with the value "Charlie", "Phone:" with "032235456", "Address:" with "13, mark St. Sang.TW", "E-Mail:" with "zyxel-a@gamil.com", and "Other:" with "Nothing" and "(Optional)" to its right. At the bottom of the form are two buttons: "Agree" and "Disagree". A red rectangular box highlights the "Name", "Phone", "Address", and "E-Mail" fields.

ZyXEL

[View Mobile Version](#)

Internet Access Policy

(We will provide example for customer within html comment tag)

Name: Charlie

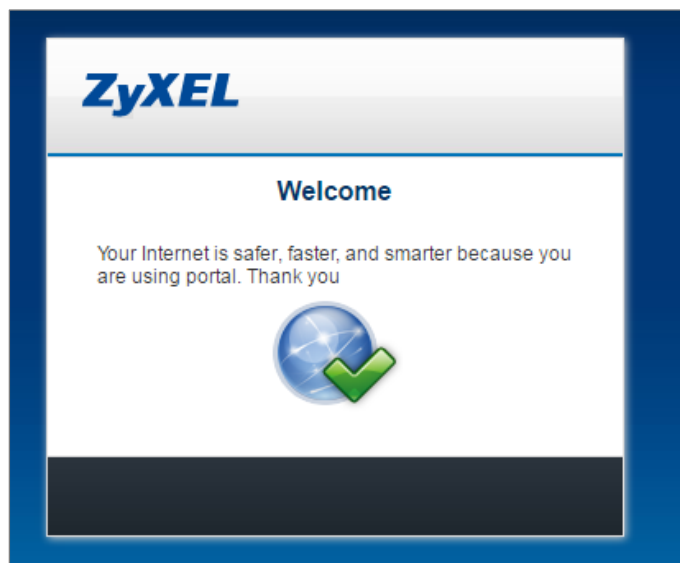
Phone: 032235456

Address: 13, mark St. Sang.TW

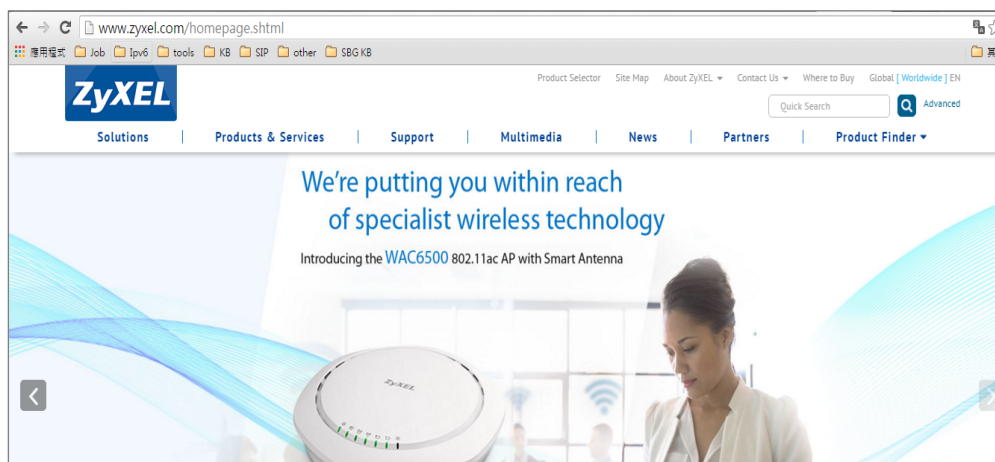
E-Mail: zyxel-a@gamil.com

Other: Nothing (Optional)

Agree **Disagree**

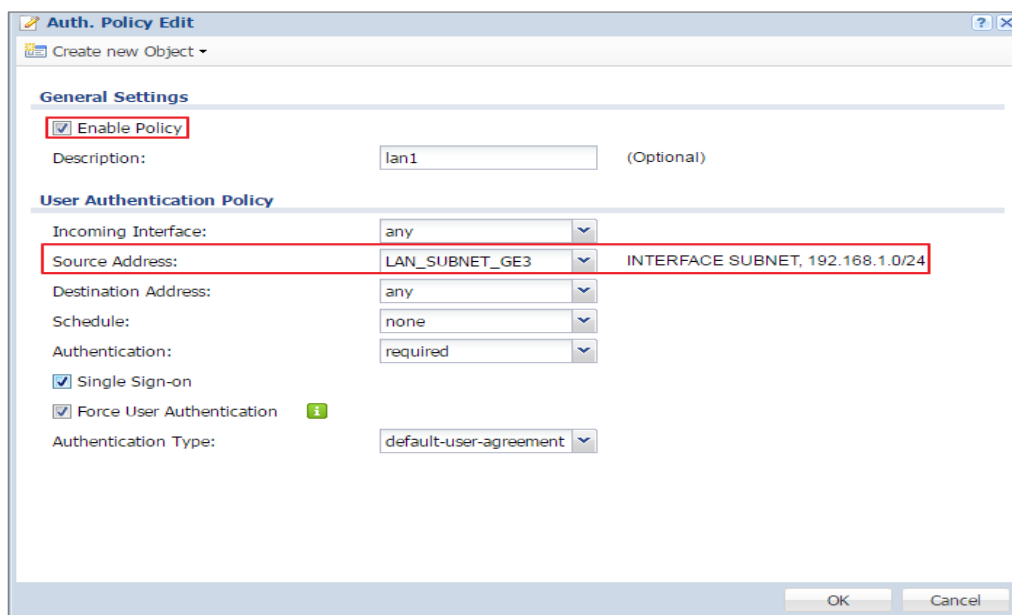


2. The advertisement webpage will be displayed in a new window and it is the first page that appears whenever the user connects to the Internet.



What could Go Wrong?

If users can access the internet without any Authentication, please make sure the Source Address is configured on the correct the subnet. For example, if you want users to be controlled via authentication in Subnet 192.168.1.0/24, you need to make sure the Source Address should be 192.168.1.0/24

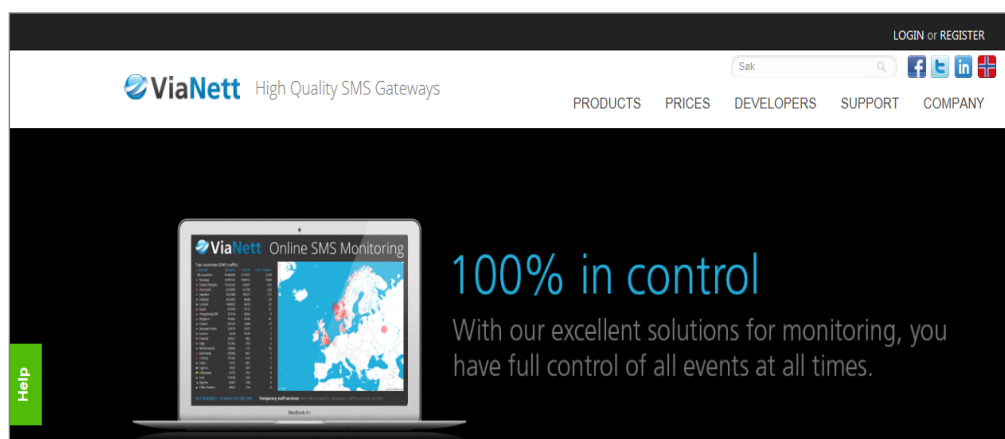


Set up Enable the Free Time Feature

Configurations on the USG1100


On the USG1100, you need to enable the SMS service and select **SMS** as the delivery method in the **Free Time** feature.

1. Register for a ViaNett account at <http://www.vianett.com>.



2. Enter all the required information.

3. After the form has been submitted, the account information will be sent to your E-mail address.



Efficiency with SMS

Welcome! We're happy you joined us!

Here is your account information.

Username s5553897@gmail.com
Password
Try prefix demo Send

[Go to login page](#)

You can send up to 5 SMS messages in the test period, pricegroup and sender address will not be available in this period.

[PURCHASE SMS CREDITS](#)
[SUB ACCOUNTS](#)
[ADMIN USERS](#)
[COMPANY DATA](#)
[INVOICES \(PDF\)](#)
[CHANGE PASSWORD](#)

[Service Setup](#)
[Purchase SMS](#)
[>> SMS API](#)

Purchase SMS credits (Prepaid)

This applies to pre-paid services. Please [contact us](#) if you would like postpaid services.

Purchase SMS credits

Company: Zyxel (s5553897@gmail.com)


Amount: EUR

Your mobile number (international format):

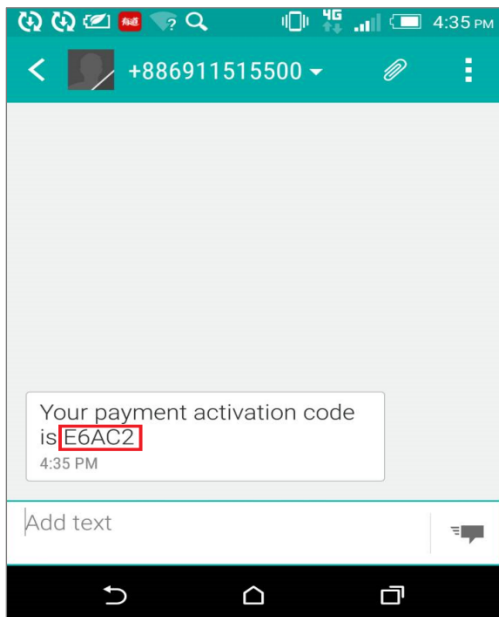
☒ Autofill my account when reaching EUR

☒ I do accept the [agreement](#) and the [anti-spam statement](#), and that in the event of abuse, my account shall be closed without any refund given for unused credits. The account will be active one year after latest purchase. Unused credits after one year will not be returned.

[GO TO PAYMENT](#)



Buy now
and get started!



4. Enter the activation code and proceed to make the payment.

Purchase SMS credits (Prepaid)

This applies to pre-paid services. Please [contact us](#) if you would like postpaid services.

Purchase SMS credits

Company: Zyxel (s5553897@gmail.com)

Amount: EUR 20

Your mobile number (international format): [REDACTED]

☒ Autofill my account when reaching EUR 20

☒ I do accept the [agreement](#) and the [anti-spam statement](#), and that in the event of abuse, my account shall be closed without any refund given for unused credits. The account will be active one year after latest purchase. Unused credits after one year will not be returned.

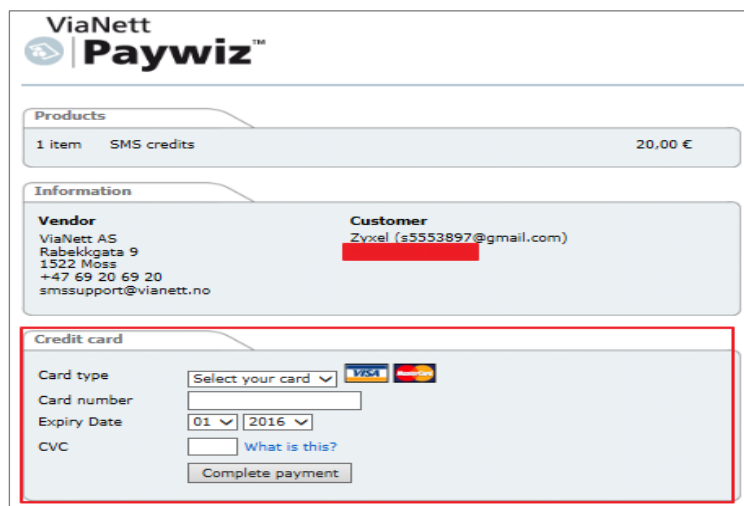
A code is now sent to your mobile.

Enter the code: E6AC2 x

[GO TO PAYMENT](#)

Buy now and get started!

5. Fill-in the credit card information to complete the payment.



ViaNett Paywiz™


Products

| | | |
|--------|-------------|---------|
| 1 item | SMS credits | 20,00 € |
|--------|-------------|---------|

Information

| | |
|---|---|
| Vendor ViaNett AS Rabekkgtata 9 1522 Moss +47 69 20 69 20 smssupport@vianett.no | Customer Zyxel (s5553897@gmail.com) [Redacted] |
|---|---|

Credit card

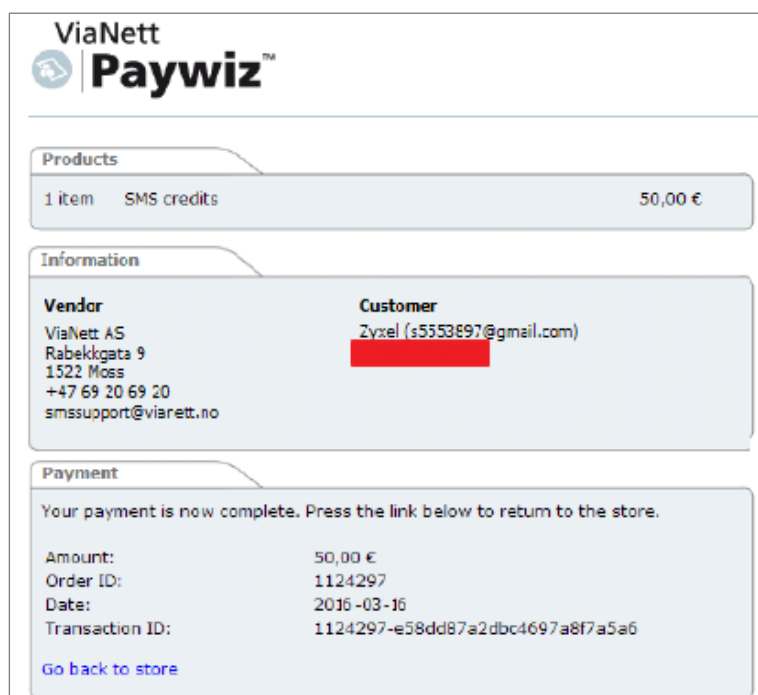
Card type: 

Card number:

Expiry Date:

CVC: [What is this?](#)

The payment is complete.



ViaNett Paywiz™

Products

| | | |
|--------|-------------|---------|
| 1 item | SMS credits | 50,00 € |
|--------|-------------|---------|

Information

| | |
|---|---|
| Vendor ViaNett AS Rabekkgtata 9 1522 Moss +47 69 20 69 20 smssupport@vianett.no | Customer Zyxel (s5553897@gmail.com) [Redacted] |
|---|---|

Payment

Your payment is now complete. Press the link below to return to the store.

| | |
|-----------------|----------------------------------|
| Amount: | 50,00 € |
| Order ID: | 1124297 |
| Date: | 2016-03-16 |
| Transaction ID: | 1124297-e58dd87a2dbc4697a8f7a5a6 |

[Go back to store](#)

6. After the ViaNett account is ready, go to the USG1100's **Configuration > Hotspot > SMS** screen.

(1) Enable SMS.

(2) Fill-in your local phone country code as the default country code.

(3) Add authentication policy for every source.

ZyXEL USG1100

CONFIGURATION

- Quick Setup
- Licensing
- Wireless
- Network
 - Interface
 - Routing
 - DDNS
 - NAT
 - Redirect Service
 - ALG
 - UPnP

SMS

General Settings

☒ Enable SMS

Default country code for phone number: (1-4) digit

ViaNett Configuration

User Name:

Password:

Retype to Confirm:

7. Go to **Configuration > Hotspot > Free Time**.

(1) Select **Enable Free Time** and set up the free time period. By default, the **Reset Time** is at AM 00:00. You can also set up how many times a MAC address can access the Internet.

(2) Select **SMS** as the method to deliver the login information to the mobile phone.

ZyXEL USG1100

Welcome admin | [Logout](#)

CONFIGURATION

- Quick Setup
- Licensing
- Wireless
- Network
 - Interface
 - Routing
 - DDNS
 - NAT
 - Redirect Service
 - ALG
 - UPnP
 - IP/MAC Binding
 - Layer 2 Isolation
 - DNS Inbound LB

Free Time

General Settings

☒ Enable Free Time

Free Time Period: minute

Reset Time:

Time:

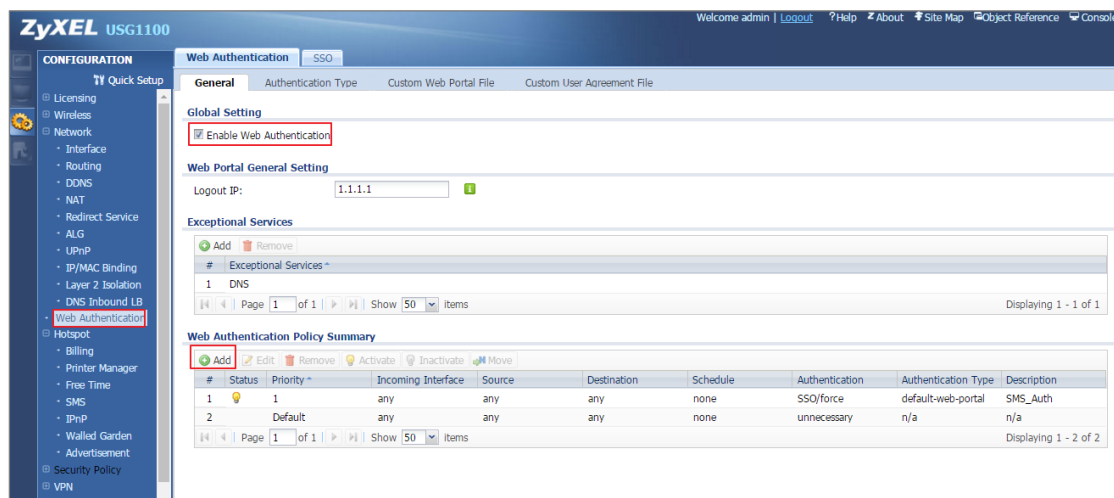
Maximum Registration Number Before Reset Time: (1-5)

Delivery Method:

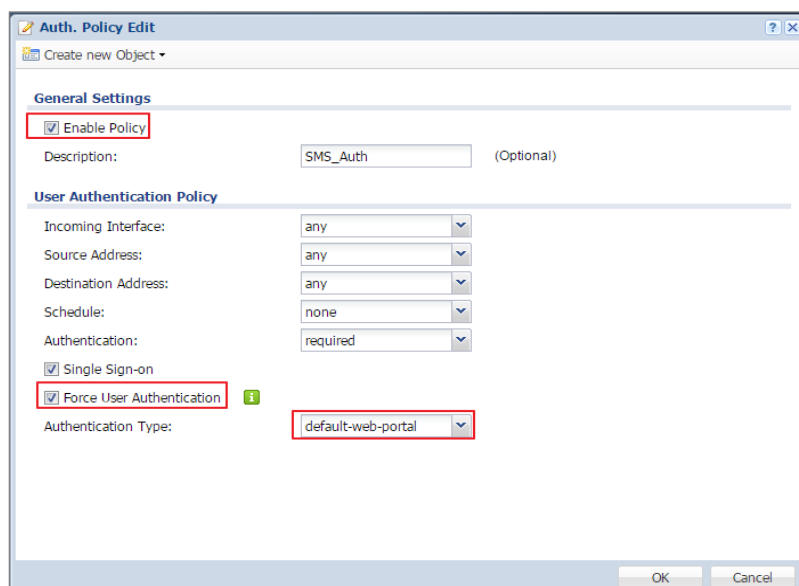
☒ Auto Login

Note:
If you want to configure ssid profile settings of the account, keep user logged in, please go to [Billing](#)

8. Go to **Configuration > Web Authentication**. Select **Enable Web Authentication** and click **Add** in the **Web Authentication Policy Summary** section.

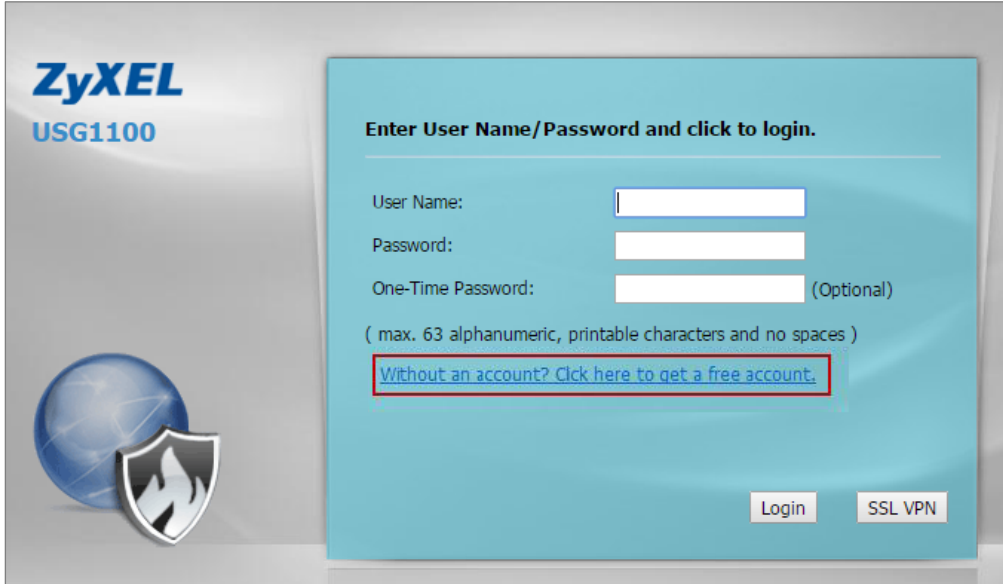


9. Select **Enable Policy, Force User Authentication**, and then select **default-web-portal** as the **Authentication Type**.



Test Free Time Feature

1. The user will be redirected to the **Login** screen before he/she is permitted to access the Internet. Click on the link to get a free account.



ZyXEL
USG1100

Enter User Name/Password and click to login.

User Name:

Password:

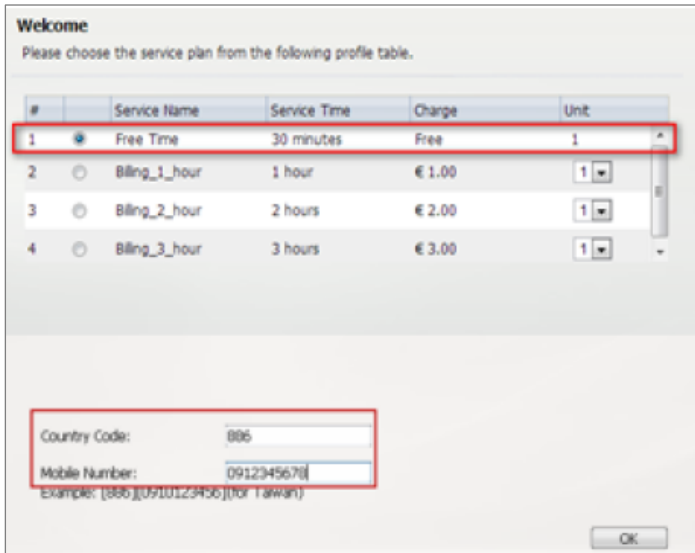
One-Time Password: (Optional)

(max. 63 alphanumeric, printable characters and no spaces)

[Without an account? Click here to get a free account.](#)

Login SSL VPN

2. Select **Free Time** as the service plan. Then submit your country code and mobile phone number.



Welcome
Please choose the service plan from the following profile table.

| # | Service Name | Service Time | Charge | Unit |
|---|--|--------------|--------|------|
| 1 | <input checked="" type="radio"/> Free Time | 30 minutes | Free | 1 |
| 2 | <input type="radio"/> Billing_1_hour | 1 hour | € 1.00 | 1 |
| 3 | <input type="radio"/> Billing_2_hour | 2 hours | € 2.00 | 1 |
| 4 | <input type="radio"/> Billing_3_hour | 3 hours | € 3.00 | 1 |

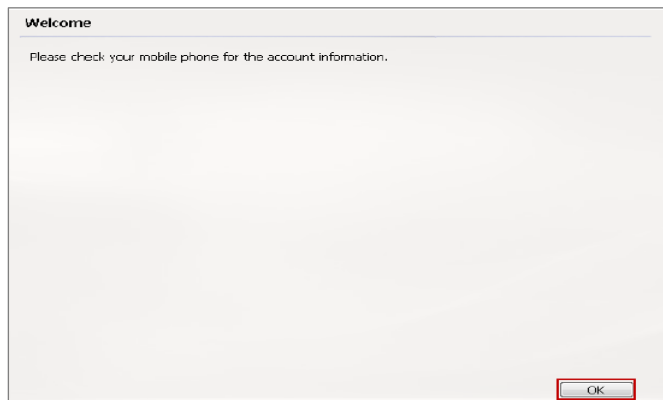
Country Code:

Mobile Number:

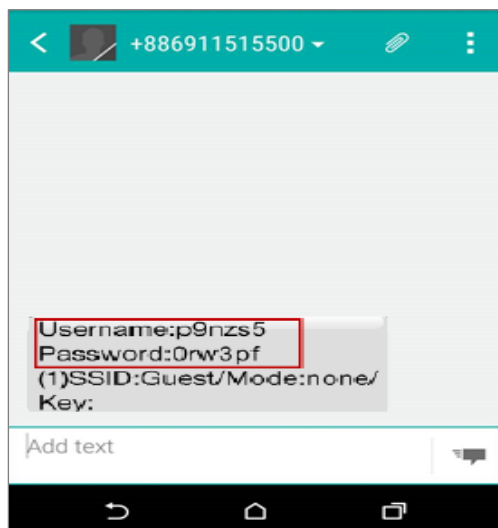
Example: [886][0910123456](for Taiwan)

OK

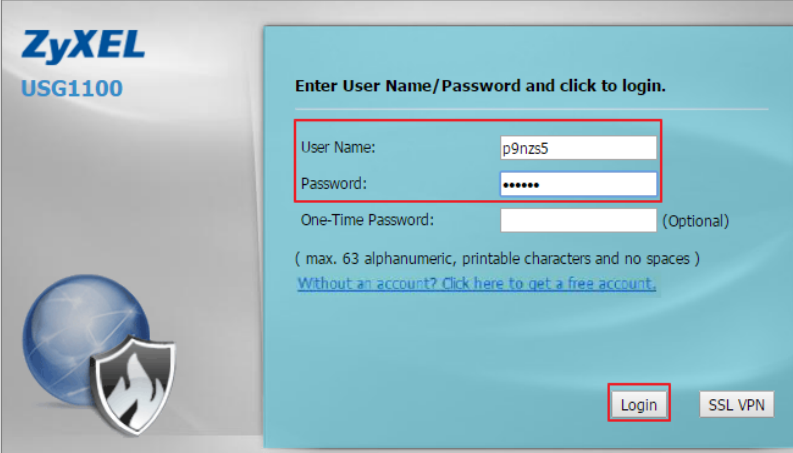
3. The account and password will be sent to your mobile phone.



4. Check your account information.

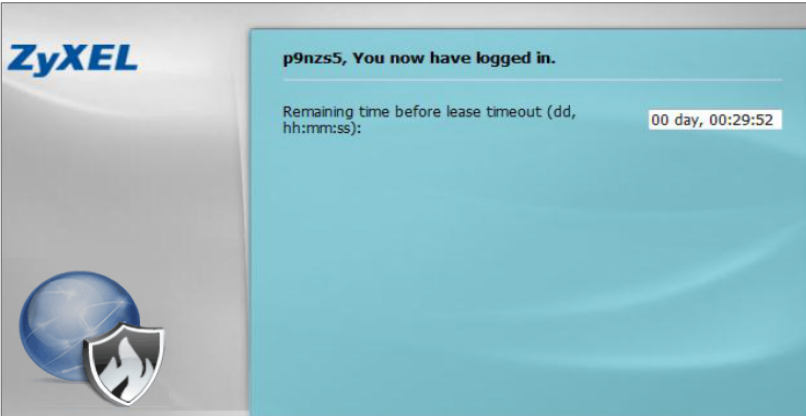


5. Fill-in the account information received on your mobile phone and click **Login**.



The image shows the ZyXEL USG1100 login page. On the left, there is a logo for ZyXEL USG1100 and a graphic of a globe with a shield. The main area is a light blue box with the text "Enter User Name/Password and click to login." Below this, there are three input fields: "User Name:" with the value "p9nzs5", "Password:" with masked characters "*****", and "One-Time Password:" which is empty and marked as "(Optional)". Below the password fields, there is a note "(max. 63 alphanumeric, printable characters and no spaces)" and a link "[Without an account? Click here to get a free account.](#)". At the bottom right of the login box, there are two buttons: "Login" and "SSL VPN".

6. Now the client can start accessing the Internet.



The image shows the ZyXEL USG1100 post-login interface. On the left, there is a logo for ZyXEL and a graphic of a globe with a shield. The main area is a light blue box with the text "p9nzs5, You now have logged in." Below this, there is a label "Remaining time before lease timeout (dd, hh:mm:ss):" and a value "00 day, 00:29:52".

What Can Go Wrong?

If client cannot get the SMS message from ViaNett, please make sure the Country code, Username and Password are all correct.

ZyXEL USG1100

CONFIGURATION **Quick Setup**

- ▣ Licensing
- ▣ Wireless
- ▣ Network
 - Interface
 - Routing
 - DDNS
 - NAT
 - Redirect Service
 - ALG
 - UPnP

SMS

General Settings

☒ Enable SMS

Default country code for phone number: (1-4) digit

ViaNett Configuration

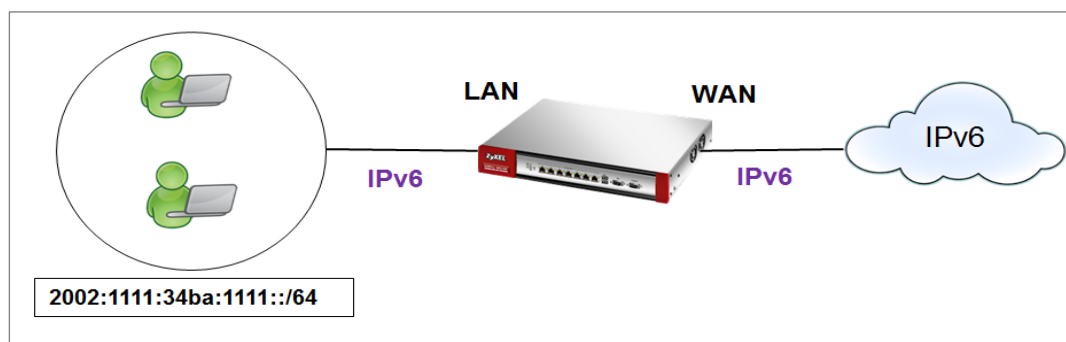
User Name:

Password:

Retype to Confirm:

How to Setup IPv6 Interfaces for Pure IPv6 Routing

This example shows how to configure your USG Z's WAN and LAN interfaces which connects two IPv6 networks. USG Z periodically advertises a network prefix of 2006:1111:1111:1111::/64 to the LAN through router advertisements.



ZyWALL/USG access the internet via IPv6



Note:

Instead of using router advertisement, you can use DHCPv6 to pass the network settings to the computers on the LAN.

This example was tested using USG110 (Firmware Version: ZLD 4.25) and ZyWALL 310 (Firmware Version: ZLD 4.25).

Setting Up the IPv6 Interface

Wan

1. In the CONFIGURATION > Network > Interface > Ethernet screen's IPv6 Configuration section, double-click the wan1.
2. The Edit Ethernet screen appears. Select Enable Interface and Enable IPv6. Select Enable Auto-Configuration. Click OK.

Note: Your ISP or uplink router should enable router advertisement.

| | |
|---|--|
| General Settings | |
| <input checked="" type="checkbox"/> Enable Interface | |
| General IPv6 Setting | |
| <input checked="" type="checkbox"/> Enable IPv6 i | |
| Interface Properties | |
| Interface Type: | external i |
| Interface Name: | ge2 |
| Port: | P2 |
| Zone: | WAN i |
| MAC Address: | B8:EC:A3:A9:C0:04 |
| Description: | <input type="text"/> (Optional) |
| IPv6 Address Assignment | |
| <input type="checkbox"/> Enable Stateless Address Auto-configuration (SLAAC) | |
| Link-Local Address: | n/a |
| IPv6 Address/Prefix Length: | <input type="text"/> (Optional) |
| <input checked="" type="checkbox"/> Advance | |
| DHCPv6 Setting | |
| DHCPv6: | N/A |
| IPv6 Router Advertisement Setting | |
| <input checked="" type="checkbox"/> Enable Router Advertisement | |
| <input checked="" type="checkbox"/> Advance | |
| Router Preference: | Medium |

Lan

1. In the CONFIGURATION > Network > Interface > Ethernet screen, double-click the lan1 in the IPv6 Configuration section.
2. The Edit Ethernet screen appears. Select Enable Interface and Enable IPv6. Select Enable Router Advertisement and click Add and configure a network prefix for the LAN1 (2006:1111:34ba:1111::/64 in this example). Click **OK**.

General Settings

☒ Enable Interface

General IPv6 Setting

☒ Enable IPv6 ?

Interface Properties

Interface Type: Internal ?

Interface Name: ge4

Port: P4

Zone: LAN1 ?

MAC Address: B8:EC:A3:A9:C0:D6

Description: (Optional)

IPv6 Address Assignment

☐ Enable Stateless Address Auto-configuration (SLAAC)

Link-Local Address: n/a

IPv6 Address/Prefix Length: (Optional)

☒ Advance

IPv6 Router Advertisement Setting

☒ Enable Router Advertisement

☒ Advance

Router Preference: Medium

☒ Advance

Advertised Prefix Table

| # | IPv6 Address/Prefix Length |
|---|----------------------------|
| 1 | 2002:1111:34ba:1111::/64 |

Page 0 of 0 Show 50 items No data to display

☒ Advance

3. Using command line ipconfig to check.

```

C:\Windows\system32\cmd.exe

Windows IP Configuration

Wireless LAN adapter Wireless Network Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::5138:dc32:ff2f:6a34%12
    IPv4 Address. . . . . : 10.251.61.91
    Subnet Mask . . . . . : 255.255.254.0
    Default Gateway . . . . . : 10.251.61.253

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2002:1111:34ba:1111:d1b3:8580:1506:4d72
    Temporary IPv6 Address. . . . . : 2002:1111:34ba:1111:5cdd:2779:4c5c:9fe
    Link-local IPv6 Address . . . . . : fe80::d1b3:8580:1506:4d72%11
    IPv4 Address. . . . . : 192.168.2.34
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::5ef4:abff:fef9:d4d4%11
    . . . . . : 192.168.2.1

Tunnel adapter isatap.{1C5CCB06-45A8-4C5E-AB6A-32D5DE7DA785}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter isatap.{7824C2F6-F6C2-4A7C-BBF5-10CF6F23CEE3}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\ZT02340>
  
```

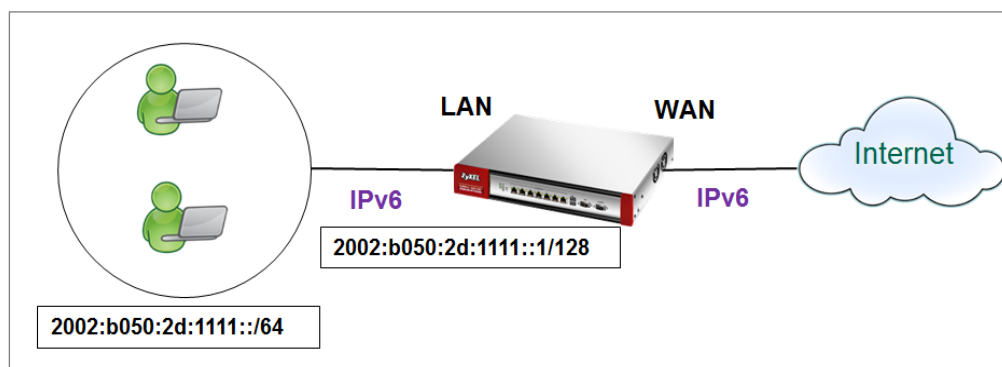
Set up the Prefix Delegation and Router Advertisement

This example shows how to configure prefix delegation on the ZyWALL's WAN and router advertisement on the LAN.

Apply a network Prefix From Your ISP

First of all, you have to apply a network prefix from your ISP or the uplink router's administrator. The WAN port's DUID is required when you apply the prefix. You can check the DUID information in the **WAN IPv6 Interface Edit** screen.

This example assumes that you were given a network prefix of 2001:b050:2d::/48 and you decide to divide it and give 2001:b050:2d:1111::/64 to the LAN network. LAN1's IP address is 2001:b050:2d:1111::1/128.



Setting Up the WAN IPv6 Interface

1. In the **Configuration > Network > Interface > Ethernet** screen's **IPv6 Configuration** section,
double-click the **WAN** interface.
2. The Edit Ethernet screen appears. Select Enable Interface and Enable IPv6.
Click Create new Object to add a DHCPv6 Request object with the Prefix Delegation type.
Select Enable Auto-Configuration.
Select Client in the DHCPv6 field. (WAN1's DUID appears.)

Click Add in the DHCPv6 Request Options table and select the DHCPv6 request object you just created. You cannot see the prefix your ISP gave you in the Value field until you click OK and then come back to this screen again. It is 2001:b050:2d::/48 in this example.

Note: Your ISP or a DHCPv6 server in the same network as the WAN should assign an IPv6 IP address for the WAN interface.

General Settings

☒ Enable Interface

General IPv6 Setting

☒ Enable IPv6 ?

Interface Properties

| | |
|-----------------|---------------------------------|
| Interface Type: | external ? |
| Interface Name: | ge2 |
| Port: | P2 ? |
| Zone: | WAN ? |
| MAC Address: | B8:EC:A3:A9:C0:04 |
| Description: | <input type="text"/> (Optional) |

Create new Object

- DHCPv6 Lease
- DHCPv6 Request**

+ Add Request Object

Name:

Request Type: **Prefix Delegation**

DHCPv6 Setting

DHCPv6: Client

DUID: 00:03:00:01:B8:EC:A3:A9:C0

Advance

☒ DUID as MAC

Customized DUID:

☐ Enable Rapid Commit

☒ Request Address

DHCPv6 Request Options

Add
Remove
Object References

| # | Name | Type | Value |
|---|------------|------------------|------------------------|
| 1 | Prefix_WAN | prefix-delega... | 2002:b050:2d:1111::/64 |

Page 0 of 0
Show 50 items
No data to display

Setting Up the WAN IPv6 Interface

1. In the Configuration > Network > Interface > Ethernet screen, double-click the lan interface in the IPv6 Configuration section.
2. The Edit Ethernet screen appears. Click Show Advanced Settings to display more settings on this screen.

Select Enable Interface and Enable IPv6.

In the Address from DHCPv6 Prefix Delegation table, click Add and select the DHCPv6 request object from the drop-down list, type ::1111:0:0:1/128 in the Suffix Address field. (The combined address 2001:b050:2d:1111::1/128 will display as LAN1's IPv6 address after you click OK and come back to this screen again).

DHCPv6 Setting is **N/A**

Note: You can configure the IPv6 Address/Prefix Length field instead if the delegated prefix is never changed.


3. In the Advertised Prefix from DHCPv6 Prefix Delegation table, click Add and select the DHCPv6 request object from the drop-down list, type ::1111/64 in the Suffix Address field. (The combined prefix 2001:b050:2d:1111::/64 will display for the LAN1's network prefix after you click OK and come back to this screen again)., please note that this is the USG LAN interface IP.

IPv6 Address Assignment

☐ Enable Stateless Address Auto-configuration (SLAAC)

Link-Local Address: n/a





IPv6 Address/Prefix Length: (Optional)

 Advance





Gateway: (Optional)

Metric: (0-15)

Address from DHCPv6 Prefix Delegation

 Add
  Edit
  Remove
  Object References

| # | Delegated Prefix | Suffix Address | Address |
|---|------------------|-----------------|-------------------|
| 1 | Prefix_WAN | ::1111:0:0:1/64 | 2002:b050:2d:1111 |



 Page of 0
 

 Show items
 No data to display

1. Navigate to IPv6 Router Advertisement Setting, enable Router Advertisement, it would advertise the prefix to the Lan host, also enable Advertised Hosts Get Other Configuration From DHCPv6, Lan hosts will get the DNS address from USG.
2. Configure Advertised Prefix from DHCPv6 Prefix Delegation, the Lan hosts will get the Prefix from USG, Suffix address can set 0~F

IPv6 Router Advertisement Setting

☒ Enable Router Advertisement

Advance

☐ Advertised Hosts Get Network Configuration From DHCPv6

☒ Advertised Hosts Get Other Configuration From DHCPv6

Router Preference: Medium

Advance

MTU: 1480 (1280-1500, 0 is disabled)

Hop Limit: 64 (0-255, 0 is disabled)

Advertised Prefix Table

+ Add Edit Remove

| # | IPv6 Address/Prefix Length |
|--|----------------------------|
| Page 0 of 0 Show 50 items No data to display | |

Advance

Advertised Prefix from DHCPv6 Prefix Delegation

+ Add Edit Remove Object References

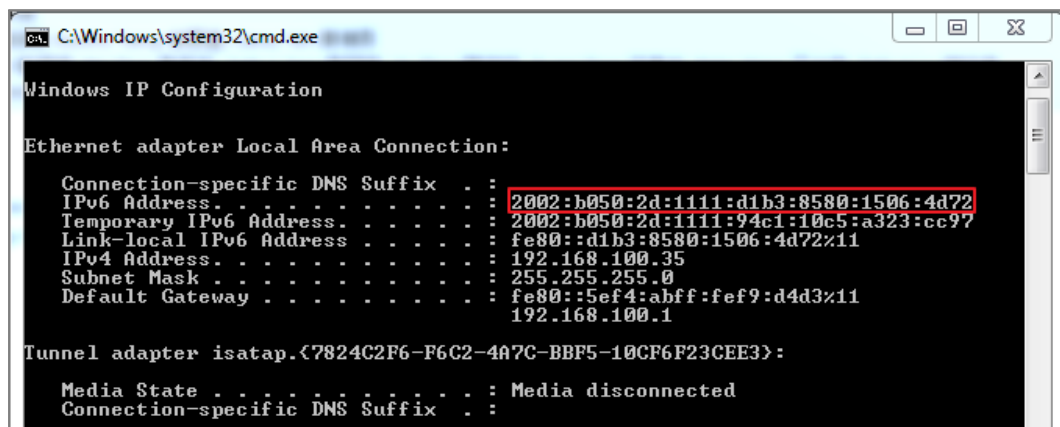
| # | Delegated Prefix | Suffix Address | Address |
|--|------------------|----------------|---------|
| 1 | Prefix_WAN | ::0/64 | |
| Page 0 of 0 Show 50 items No data to display | | | |

Test

1. Connect a computer to the ZyWALL's LAN interface.
2. Enable IPv6 support on you computer.

In Windows XP, you need to use the IPv6 install command in a Command Prompt.

In Windows 7, IPv6 is supported by default. You can enable IPv6 in the Control Panel > Network and Sharing Center > Local Area Connection screen.
3. Your computer should get an IPv6 IP address (starting with 2001:b050:2d:1111: for this example) from the ZyWALL.



```

C:\Windows\system32\cmd.exe
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2002:b050:2d:1111:d1b3:8580:1506:4d72
    Temporary IPv6 Address. . . . . : 2002:b050:2d:1111:94c1:10c5:a323:cc97
    Link-local IPv6 Address . . . . . : fe80::d1b3:8580:1506:4d72%11
    IPv4 Address. . . . . : 192.168.100.35
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::5ef4:abff:fe9:d4d3%11
                                192.168.100.1

Tunnel adapter isatap.{7824C2F6-F6C2-4A7C-BBF5-10CF6F23CEE3}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 
  
```

4. Open a web browser and type <http://www.kame.net>. If your IPv6 settings are correct, you can see a dancing turtle in the website.

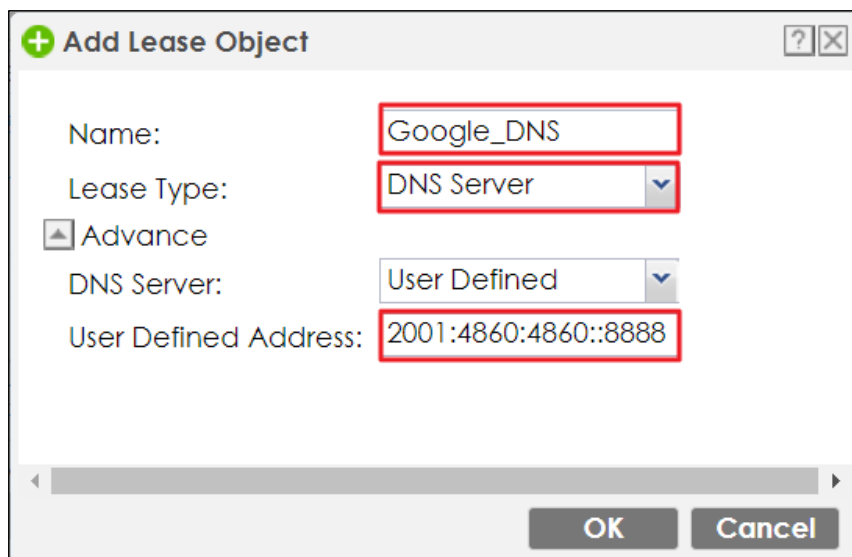
What Can Go Wrong?

1. If you forgot to enable Auto-Configuration on the WAN1 IPv6 interface, you will not have any default route to forward the LAN's IPv6 packets.
2. To use prefix delegation, you must set the WAN interface to a DHCPv6 client, enable router advertisements on the LAN interface as well as configure the Advertised Prefix from DHCPv6 Prefix Delegation table.
3. If the Value field in the WAN1's DHCPv6 Request Options table displays n/a, contact your ISP for further support.
4. In Windows, some IPv6 related tunnels may be enabled by default such as Teredo and 6to4 tunnels. It may cause your computer to handle IPv6 packets in an unexpected way. It is recommended to disable those tunnels on your computer.

Assign the DNS address to the client

1. If you want to assign the DNS server address instead of ISP's , then please create the DNS server object.

Select DHCPv6 Lease and DNS server as lease type. For example set the Google DNS IPv6 address 2001:4860:4860::8888



Add Lease Object

Name: Google_DNS

Lease Type: DNS Server

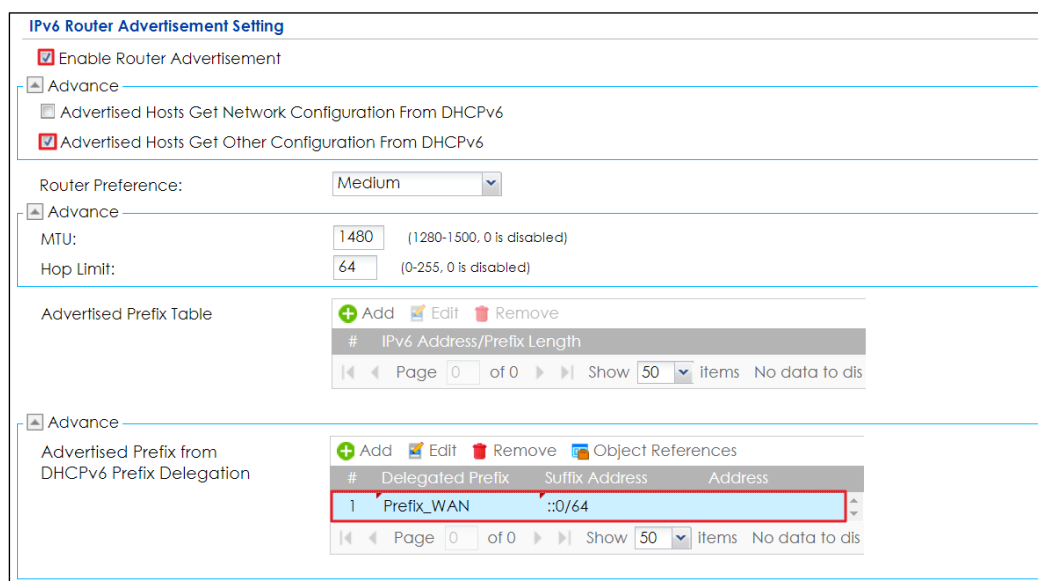
Advance

DNS Server: User Defined

User Defined Address: 2001:4860:4860::8888

OK Cancel

2. Select the drop-down list DHCPv6 as server type, add the DNS server object in DHCPv6 lease options and enable **Router Advertisement**.



IPv6 Router Advertisement Setting

☒ Enable Router Advertisement

Advance

☐ Advertised Hosts Get Network Configuration From DHCPv6

☒ Advertised Hosts Get Other Configuration From DHCPv6

Router Preference: Medium

Advance

MTU: 1480 (1280-1500, 0 is disabled)

Hop Limit: 64 (0-255, 0 is disabled)

Advertised Prefix Table

| # | IPv6 Address/Prefix Length |
|--------------------|----------------------------|
| No data to display | |

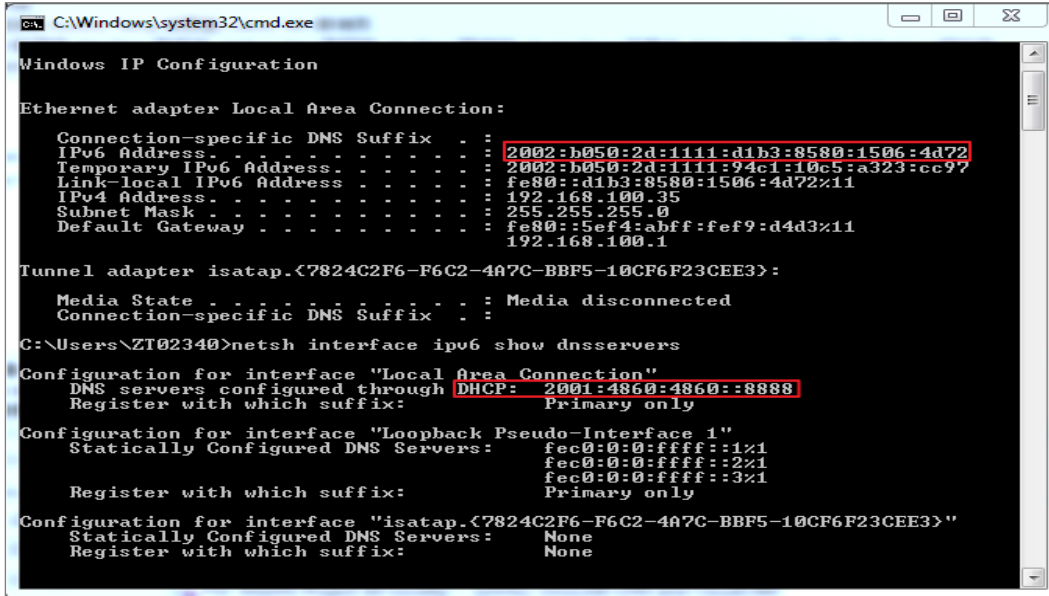
Advance

Advertised Prefix from DHCPv6 Prefix Delegation

| # | Delegated Prefix | Suffix Address | Address |
|---|------------------|----------------|---------|
| 1 | Prefix_WAN | ::0/64 | |

Test

You can use command "netsh interface ipv6 show dnsservers" to check the DNS server IP.



```

C:\Windows\system32\cmd.exe
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . . . : 
    IPv6 Address . . . . . : 2002:b050:2d:1111:d1b3:8580:1506:4d72
    Temporary IPv6 Address . . . . . : 2002:b050:2d:1111:94c1:10c5:a323:cc97
    Link-local IPv6 Address . . . . . : fe80::d1b3:8580:1506:4d72%11
    IPv4 Address . . . . . : 192.168.100.35
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::5ef4:abff:fef9:d4d3%11
    192.168.100.1

Tunnel adapter isatap.{7824C2F6-F6C2-4A7C-BBF5-10CF6F23CEE3}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . : 

C:\Users\ZT02340>netsh interface ipv6 show dnsservers

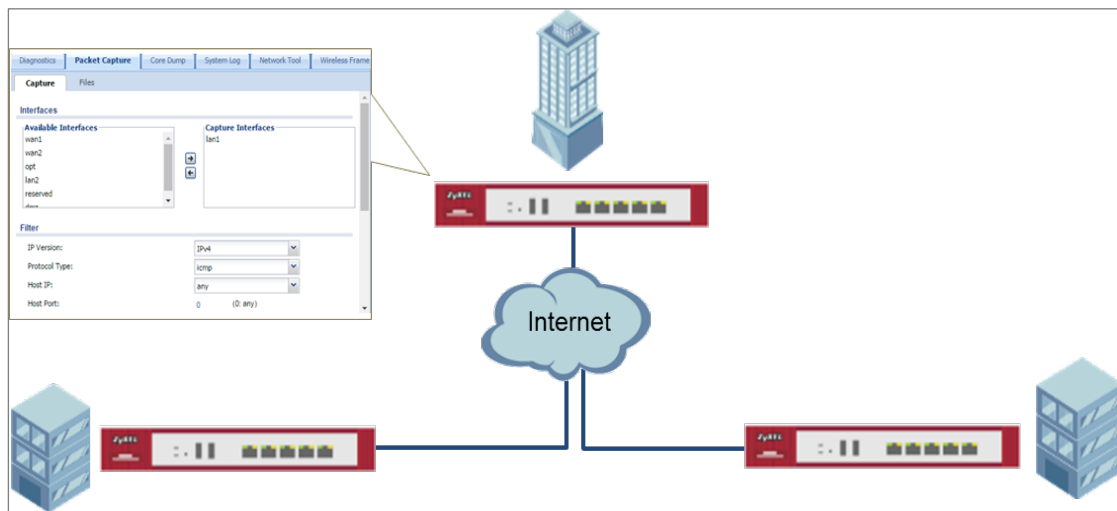
Configuration for interface "Local Area Connection"
    DNS servers configured through DHCP: 2001:4860:4860::8888
    Register with which suffix: Primary only

Configuration for interface "Loopback Pseudo-Interface 1"
    Statically Configured DNS Servers: fec0:0:0:ffff::1%1
    fec0:0:0:ffff::2%1
    fec0:0:0:ffff::3%1
    Register with which suffix: Primary only


Configuration for interface "isatap.{7824C2F6-F6C2-4A7C-BBF5-10CF6F23CEE3}"
    Statically Configured DNS Servers: None
    Register with which suffix: None
  
```

How to Perform and Use the Packet Capture Feature on the ZyWALL/USG

This example shows how to use the Packet Capture feature to capture network traffic going through the ZyWALL/USG's interfaces. Studying these packet captures may help you identify network problems.



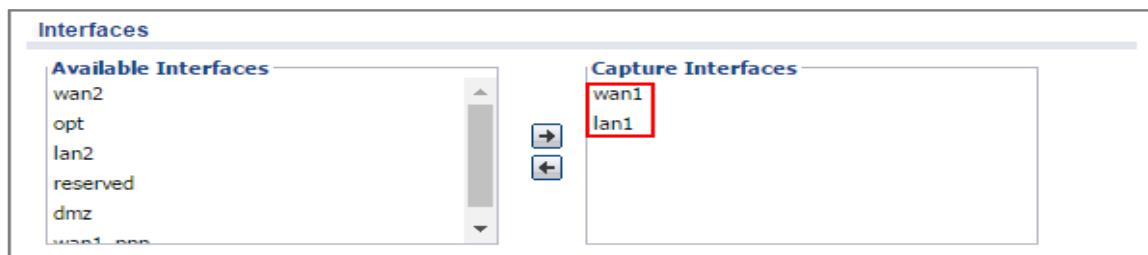
ZyWALL/USG Packet Capture Feature Settings

 Note: New capture files overwrite existing files of the same name. Change the File Suffix field's setting to avoid this. This example was tested using USG110 (Firmware Version: ZLD 4.25).

Set Up the Packet Capture Feature

8 Go to **MAINTENANCE > Diagnostics > Packet Capture > Capture > Interfaces**.

Select interfaces for which to capture packets and click the right arrow button to move them to the **Capture Interfaces** list.

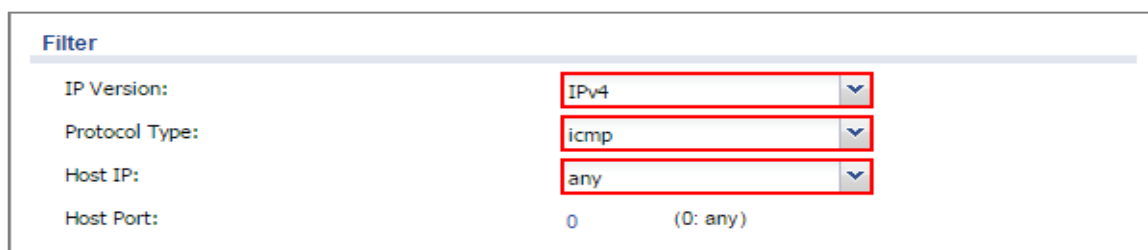


9 Go to **MAINTENANCE > Diagnostics > Packet Capture > Capture > Filter**.

Select **IP Version** (IPv4 or IPv6) for which to capture packets or select **any** to capture packets for all IP versions.

Select the **Protocol Type** of traffic for which to capture packets. Select **any** to capture packets for all types of traffic.

Select a **Host IP** address object for which to capture packets. Select **any** to capture packets for all hosts. Select **User Defined** to be able to enter an IP address.



10 Go to **MAINTENANCE > Diagnostics > Packet Capture > Capture > Misc setting**.

Select **Continuously capture and overwrite old ones** to have the ZyWALL/USG keep capturing traffic and overwriting old packet capture entries when the available storage space runs out. Select **Save data to onboard storage only** or **Save data to USB storage** (If status shows service deactivated, go to **CONFIGURATION > Object > USB Storage**, select Activate USB storage service)

Misc setting

☒ Continuously capture and overwrite old ones

☒ Save data to onboard storage only (available: 65 MB)

☐ Save data to USB storage (available: 895 MB)

Captured Packet Files: MB

 Split threshold: MB

 Duration: (0: unlimited)

 File Suffix:

 Number Of Bytes To Capture (Per Packet): Bytes

11 Click **Capture**.

Interfaces

Available Interfaces

wan2
 opt
 lan2
 reserved
 dmz
 wan1

→

←

Capture Interfaces

lan1
 wan1

Filter

IP Version:

 Protocol Type:

 Host IP:

 Host Port: (0: any)

Misc setting

☐ Continuously capture and overwrite old ones

☒ Save data to onboard storage only (available: 65 MB)

12 Click **Stop** when collection is done.

Interfaces

Available Interfaces

wan2

opt

lan2

reserved

dmz

wan1

Capture Interfaces

lan1

wan1

Filter

IP Version:

IPv4

Protocol Type:

icmp

Host IP:

any

Host Port:

0

(0: any)

Misc setting

☐ Continuously capture and overwrite old ones

☒ Save data to onboard storage only (available: 65 MB)

Capture

Stop

Reset



Check the Capture Files

- 1 Go to **MAINTENANCE > Diagnostics > Packet Capture > Files**, select the .cap file and click **Download**.






Capture

Files

Captured Packet Files

 Remove  Download

| # | File Name | Size | Last Modified |
|---|--------------------------------|------|---------------------|
| 1 | lan1--packet-capture.00000.cap | 924 | 2016-06-27 18:28:17 |
| 2 | lan1--packet-capture.txt | 78 | 2016-06-27 18:28:17 |
| 3 | wan1--packet-capture.00000.cap | 24 | 2016-06-27 18:28:17 |
| 4 | wan1--packet-capture.txt | 76 | 2016-06-27 18:28:17 |

  Page of 1   Show  items

Displaying 1 - 4 of 4

- 2 Open .cap files with Wireshark

lan1--packet-capture.00000.cap [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol |
|-----|----------------------------|--------------|--------------|----------|
| 1 | 2016-06-27 18:37:53.799645 | 192.168.1.33 | 8.8.8.8 | ICMP |
| 2 | 2016-06-27 18:37:53.825728 | 8.8.8.8 | 192.168.1.33 | ICMP |
| 3 | 2016-06-27 18:37:54.800399 | 192.168.1.33 | 8.8.8.8 | ICMP |
| 4 | 2016-06-27 18:37:54.826398 | 8.8.8.8 | 192.168.1.33 | ICMP |
| 5 | 2016-06-27 18:37:55.803515 | 192.168.1.33 | 8.8.8.8 | ICMP |
| 6 | 2016-06-27 18:37:55.829523 | 8.8.8.8 | 192.168.1.33 | ICMP |

File: "C:\Users\ZT01896\Downloads\lan1--... Packets: 6 · Displayed: 6 (100.0%) · Lo... Profile: Default

wan1--packet-capture.00000.cap [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

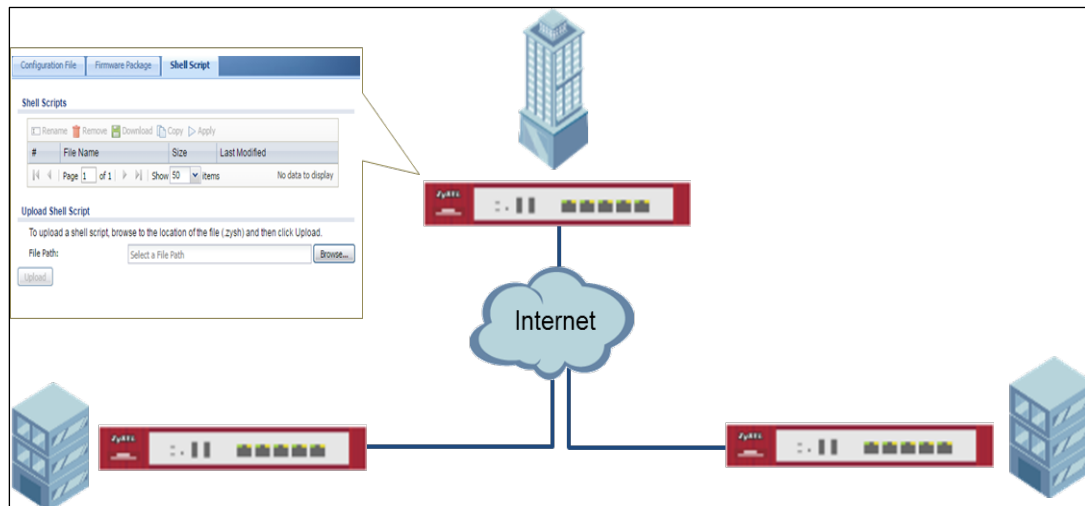
Filter: Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol |
|-----|----------------------------|---------------|---------------|----------|
| 1 | 2016-06-27 18:37:53.799825 | 111.250.188.9 | 8.8.8.8 | ICMP |
| 2 | 2016-06-27 18:37:53.825643 | 8.8.8.8 | 111.250.188.9 | ICMP |
| 3 | 2016-06-27 18:37:54.800473 | 111.250.188.9 | 8.8.8.8 | ICMP |
| 4 | 2016-06-27 18:37:54.826341 | 8.8.8.8 | 111.250.188.9 | ICMP |
| 5 | 2016-06-27 18:37:55.803606 | 111.250.188.9 | 8.8.8.8 | ICMP |
| 6 | 2016-06-27 18:37:55.829421 | 8.8.8.8 | 111.250.188.9 | ICMP |

File: "C:\Users\ZT01896\Downloads\wan1... Packets: 6 · Displayed: 6 (100.0%) · Lo... Profile: Default

How to Automatically Reboot the ZyWALL/USG by Schedule

This example shows how to use shell script and schedule run to reboot device automatically for maintenance purpose.



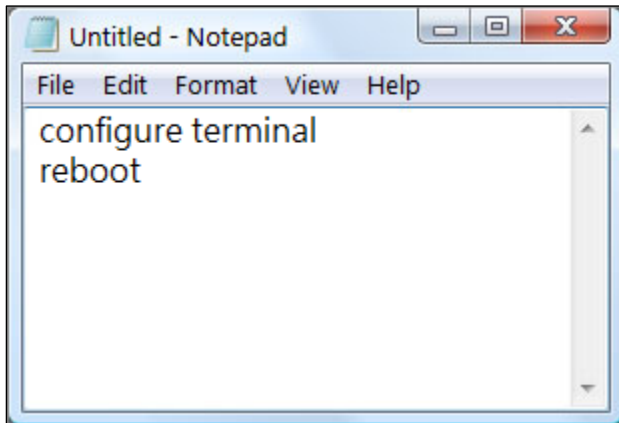
ZyWALL/USG Auto Schedule Reboot Settings

 Note: This example was tested using USG110 (Firmware Version: ZLD 4.25).

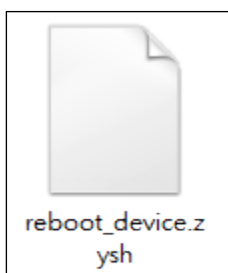
Set Up the Shell Script

- 1 Run Windows Notepad application and input below command:

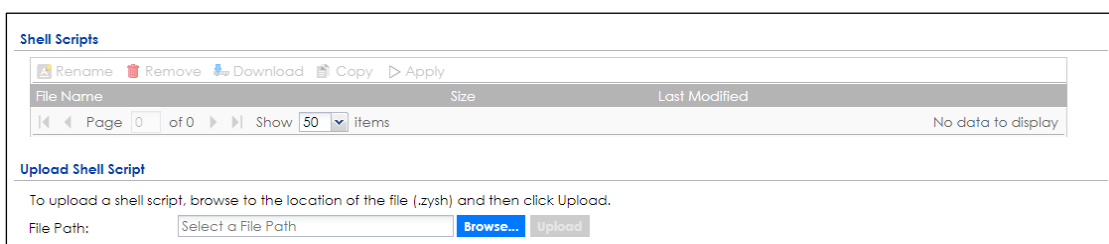
499/774



- 2 Save this file as "reboot_device.zysh"

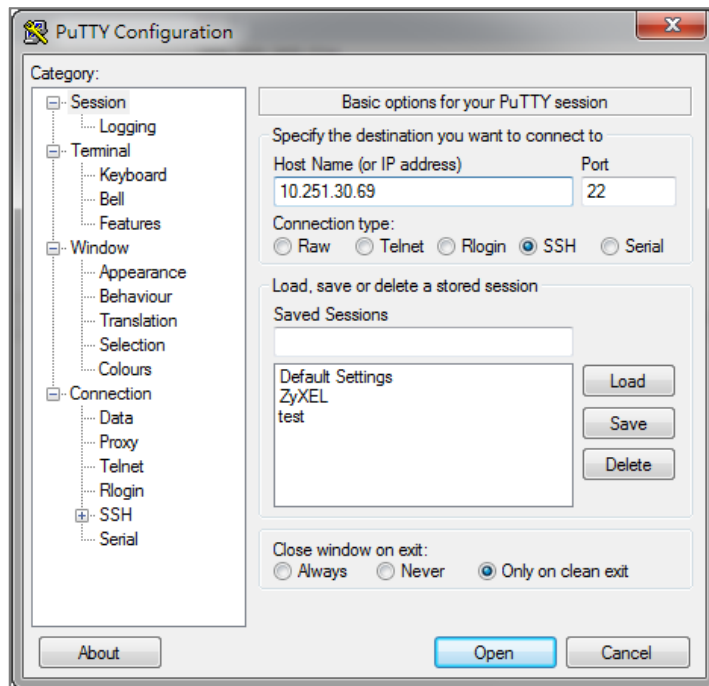


- 3 In the ZyWALL/USG, go to **MAINTENANCE > File Manager > Shell Script**. Click **Browse...** to find the reboot_device.zysh file. Click **Upload** to begin the upload process.



Set Up the Schedule Run

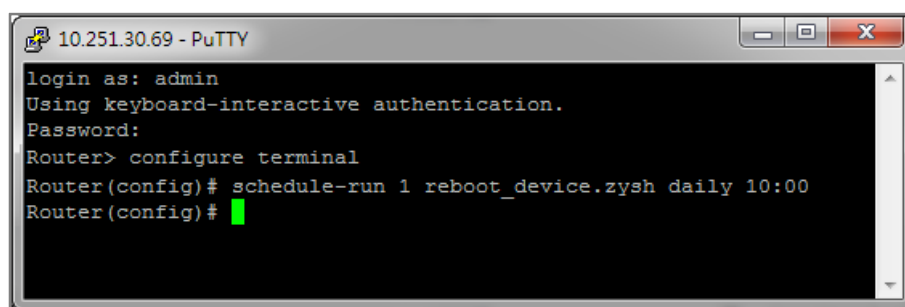
- 1 Login the device via console/telnet/SSH (using PuTTY in this example)



2 Issuing below commands based on three different (daily, weekly and monthly) user scenarios:

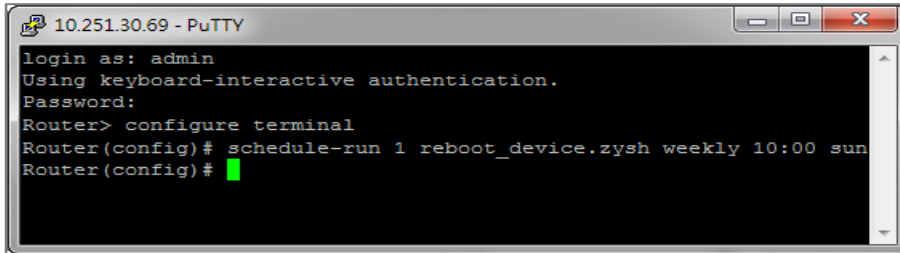
a. Router(config)# schedule-run 1 reboot_device.zysh daily 10:00

(The device will reboot at 10:00 everyday)



b. Router(config)# schedule-run 1 reboot_device.zysh weekly 10:00 sun

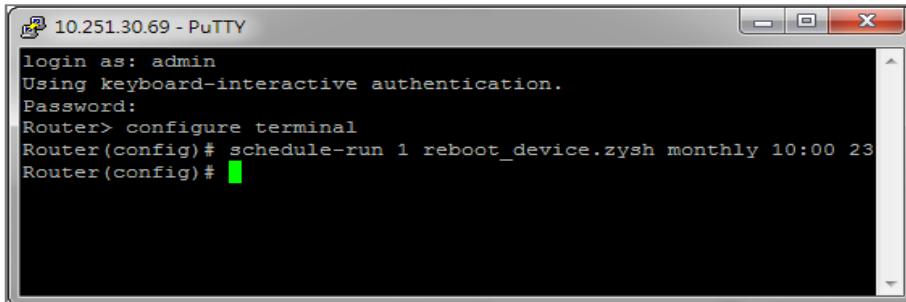
(The device will reboot at 10:00 every Sunday)



```

10.251.30.69 - PuTTY
login as: admin
Using keyboard-interactive authentication.
Password:
Router> configure terminal
Router(config)# schedule-run 1 reboot_device.zysh weekly 10:00 sun
Router(config)#
  
```

- c. Router(config)# schedule-run 1 reboot_device.zysh monthly 10:00 23
(The device will reboot at 10:00 every month on 23th)



```

10.251.30.69 - PuTTY
login as: admin
Using keyboard-interactive authentication.
Password:
Router> configure terminal
Router(config)# schedule-run 1 reboot_device.zysh monthly 10:00 23
Router(config)#
  
```

Check the Reboot Status

- 3 Login the device via console/telnet/SSH, the reboot runs as scheduled

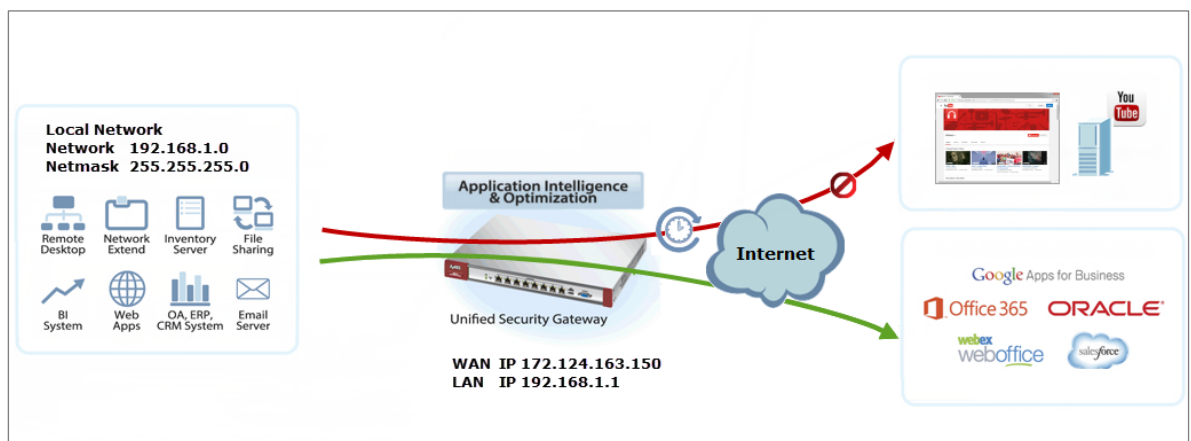
- 4 Go to **Configuration > System > Date/Time**, check **Current Date/Time**.

Figure Configuration > System > Date/Time


| Date/Time | |
|-----------------------|--------------------|
| Current Time and Date | |
| Current Time: | 13:47:47 UTC+08:00 |
| Current Date: | 2017-06-29 |

How To Schedule YouTube Access

This is an example of using the ZyWALL/USG UTM Profile and Security Policy to control access to the network. If an application should not have network access during certain hours, you can use Application Patrol, SSL Inspection and Schedule settings to make sure that these applications cannot access the Internet.



ZyWALL/USG with Scheduled YouTube Access Settings Example

 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the Schedule on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Object > Schedule > Recurring > Add Schedule Recurring Rule**. Configure a **Name** for you to identify the **Schedule Recurring Rule**. Specify the **Day Time** hour and minute when the schedule begins and ends each day. In the **Weekly** schedule, select each day of the week that the recurring schedule is effective.

CONFIGURATION > Object > Schedule > Recurring

Add Schedule Recurring Rule

Configuration

Name:

Day Time

Start Time:

Stop Time:

Weekly

Week Days:

| | | |
|--|---|---|
| <input checked="" type="checkbox"/> Monday | <input checked="" type="checkbox"/> Tuesday | <input checked="" type="checkbox"/> Wednesday |
| <input checked="" type="checkbox"/> Thursday | <input checked="" type="checkbox"/> Friday | <input type="checkbox"/> Saturday |
| <input type="checkbox"/> Sunday | | |

Create the Application Objects on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Object > Application > Add Application Rule**. Configure a **Name** for you to identify the **Application Profile**. Then, click **Add** to create an **Application Object**.

CONFIGURATION > Object > Application > Add Application Rule

In the **Application Object**, select **By Service**, type a keyword and click **Search** to display all signatures containing that keyword. Check all **Query Result** and Click **OK**.

CONFIGURATION > Object > Application > Add Application Rule > Add Application Object

Set Up SSL Inspection on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > UTM Profile > SSL Inspection > Add rule**, configure a **Name** for you to identify the **SSL Inspection** profile.

Then, select the **CA Certificate** to be the certificate used in this profile. Select **Block** to **Action for Connection with SSL v3** and select **Log** type to be **log alert**. Leave other actions as default settings.

CONFIGURATION > UTM Profile > SSL Inspection > Add rule

| General Settings | | | |
|--|-----------------|------|-----------|
| Name: | Youtube_Profile | | |
| Description: | | | |
| CA Certificate: | default | | |
| SSL/TLS version supported minimum: | ssl3 | Log: | log alert |
| Action for connection with unsupported suit: | pass | Log: | no |
| Action for connection with untrusted cert chain: | pass | Log: | log |

Set Up the Security Policy on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Security Policy > Policy Control**, configure a **Name** for you to identify the **Security Policy** profile. For **From** and **To** policies, select the direction of travel of packets to which the policy applies. Select the **Schedule** that defines when the policy applies (Youtube_Schedule in this example).

Scroll down to **UTM Profile**, check **Application Patrol** and select a profile from the list box (Youtube_profile in this example). Then, check **SSL Inspection** and select a profile from the list box (Youtube in this example).

CONFIGURATION > Security Policy > Policy Control

| | | |
|--|---------------------|------------|
| <input checked="" type="checkbox"/> Enable | | |
| Name: | Youtube_Schedule | |
| Description: | | (Optional) |
| From: | LAN1 | |
| To: | any (Excluding zyx) | |
| Source: | any | |
| Destination: | any | |
| Service: | any | |
| User: | any | |
| Schedule: | Youtube_Schedule | |
| Action: | allow | |
| Log matched traffic: | no | |

| UTM Profile | | |
|-------------------------------------|-----------------|-----------------|
| <input type="checkbox"/> | Content Filter: | none |
| <input checked="" type="checkbox"/> | SSL Inspection: | Youtube_Profile |
| | Log: | by profile |
| | Log: | by profile |

Export Certificate from ZyWALL/USG and Import it to Windows 7 Operation System

When SSL inspection is enabled and an access website does not trust the ZyWALL/USG certificate, the browser will display a warning page of security certificate problems.

Go to ZyWALL/USG **CONFIGURATION > Object > Certificate > default > Edit** to export default certificate from ZyWALL/USG with Private Key (zyx123 in this example).

CONFIGURATION > Object > Certificate > default

| My Certificates Setting | | | | | | |
|--|---------|------|------------------------|------------------------|-------------------------|-------------------------|
| <div> + Add ✎ Edit ✖ Remove 🔗 Object References </div> | | | | | | |
| # | Name | Type | Subject | Issuer | Valid From | Valid To |
| 1 | default | SELF | CN=vpn300_B8ECA3A9C... | CN=vpn300_B8ECA3A9C... | 2017-04-25 12:41:25 GMT | 2027-04-23 12:41:25 GMT |
| <div> ⏪ ⏩ Page 1 of 1 ▶ Show 50 Items ⏴ ⏵ </div> | | | | | | |
| | | | | | | Displaying 1 - 1 of 1 |

CONFIGURATION > Object > Certificate > default > Edit > Export Certificate with Private Key

Edit My Certificates

Issuer: CN=vpn300_B8ECA3A9C003
 Signature Algorithm: rsa-pkcs1-sha256
 Valid From: 2017-04-25 12:41:25 GMT
 Valid To: 2027-04-23 12:41:25 GMT
 Key Algorithm: rsaEncryption (2048 bits)
 Subject Alternative Name: vpn300_B8ECA3A9C003
 Key Usage: DigitalSignature, KeyEncipherment, DataEncipherment, KeyCertSi
 Extended Key Usage:
 Basic Constraint: Subject Type=CA, Path Length Constraint=1
 MD5 Fingerprint: 1b:a9:ff:f3:e6:42:44:9c:90:8d:bc:3e:f9:07:af:26
 SHA1 Fingerprint: 1b:dd:6e:b2:c7:89:2e:ea:43:a0:ee:d2:55:3a:ff:15:89:bc:64:70

Certificate in PEM (Base-64) Encoded Format

-----BEGIN X509 CERTIFICATE-----
 MIIDSzCCAjOgAwIBAgIJAP0XXinyW6C/MA0GCSqGSIb3DQEBCwUAMB4xHDAaBgNV
 BAMME3ZwbjMwMF9COEVDQTNBOUMwMDMwHhcNMjcwNDI1MTI0MTI1WhcNMjcw
 NDZz

Password:

Export Certificate Only

Export Certificate with Private Key

OK

Cancel

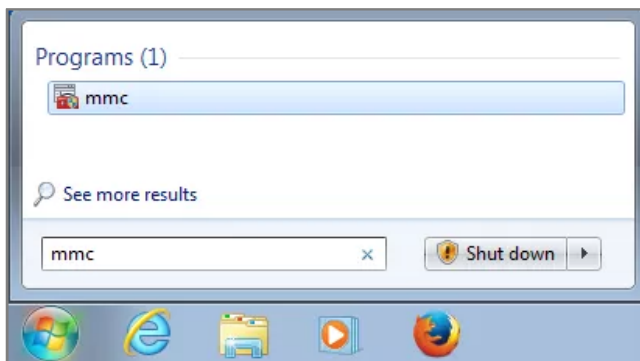
Save default certificate as *.p12 file to Windows 7 Operation System.



default.p12

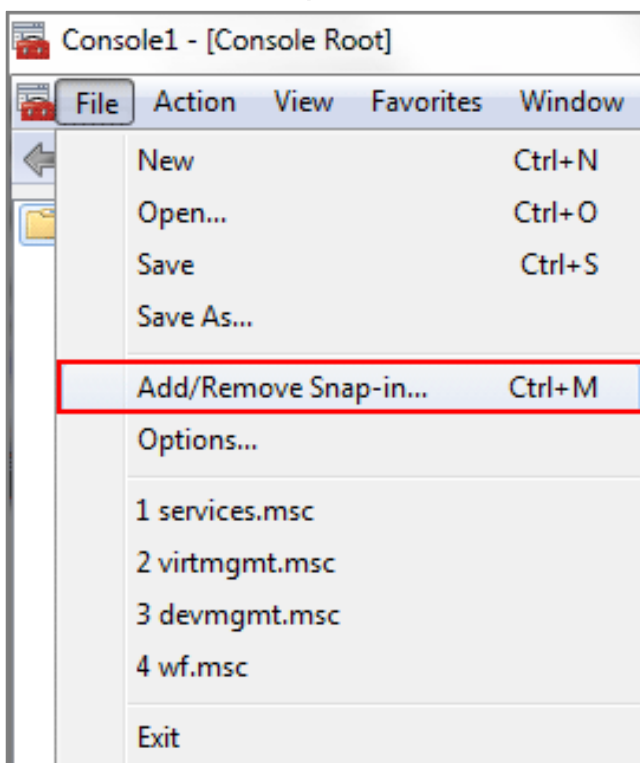
In Windows 7 Operating System **Start Menu > Search Box**, type **mmc** and press **Enter**.

Start Menu > Search Box > mmc



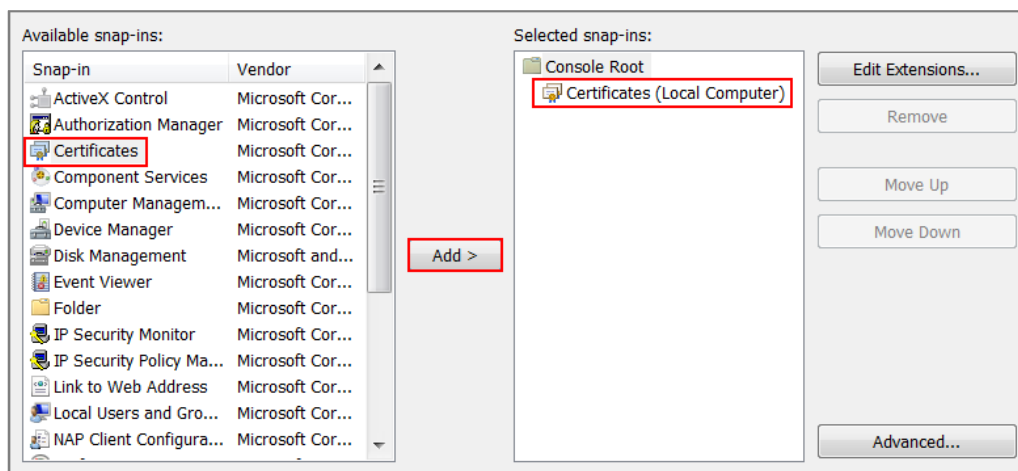
In the mmc console window, click **File > Add/Remove Snap-in...**

File > Add/Remove Snap-in...

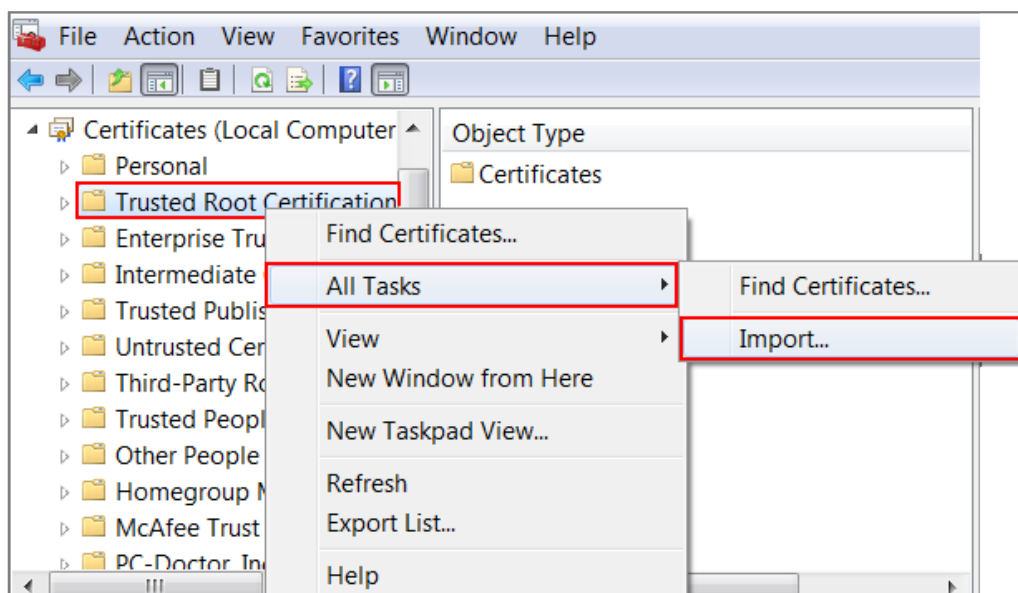


In the **Available snap-ins**, select the **Certificates** and click **Add** button. Select **Computer account > Local Computer**. Then, click **Finished** and **OK** to close the **Snap-ins** window.

Available snap-ins > Certificates > Add



In the mmc console window, open the **Certificates (Local Computer) > Trusted Root Certification Authorities**, right click **Certificate > All Tasks > Import...**



Click **Next**, Then, **Browse...**, and locate the .p12 file you downloaded earlier. Then, click **Next**.

File to Import

Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

- Personal Information Exchange- PKCS #12 (.PFX,.P12)
- Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
- Microsoft Serialized Certificate Store (.SST)

Click **Next**, type **zyx123** in the **Password** field and click **Next** again

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☐ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☒ Include all extended properties.

Select **Place all certificates in the following store** and then click **Browse** and find **Trusted Root Certification Authorities**. Click **Next**, then click **Finish**.

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.


☐ Automatically select the certificate store based on the type of certificate

☒ Place all certificates in the following store

Certificate store:

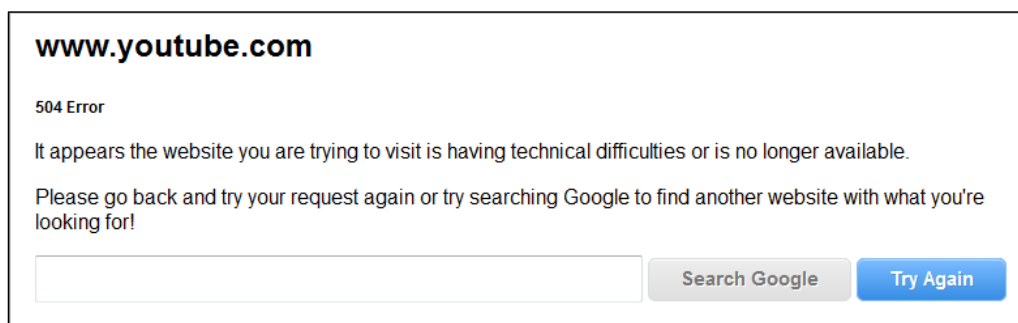
Trusted Root Certification Authorities

Browse...

 Note: Each ZyWALL/USG device has its own self-signed certificate by factory default. When you reset to the default configuration file, the original self-signed certificate is erased, and a new self-signed certificate will be created when the ZyWALL/USG boots the next time.

Test the Result

Type <http://www.youtube.com/> or <https://www.youtube.com/> into the browser.
An error message occurs.



Go to the ZyWALL/USG **Monitor > Log**, you will see [alert] log message such as below.

| Priority | Category | Message | Note |
|----------|--------------------|--|--------------|
| alert | Application Patrol | Rule_id=1 SSI=Y App=[Streaming Media]Youtube:access Action=reject SID=67137542 | ACCESS BLOCK |
| alert | Application Patrol | Rule_id=1 SSI=Y App=[Streaming Media]Youtube:access Action=reject SID=67137542 | ACCESS BLOCK |

What Could Go Wrong?

If you are not be able to configure any **Application Patrol** policies or it's not working, there are two possible reasons:

You have not subscribed for the **Application Patrol** service.

You have subscribed for the **Application Patrol** service but the license is expired.

You can click the link from the **CONFIGURATION > Licensing > Registration** screen of your ZyXEL device's Web Configurator or click the myZyXEL.com 2.0 icon from

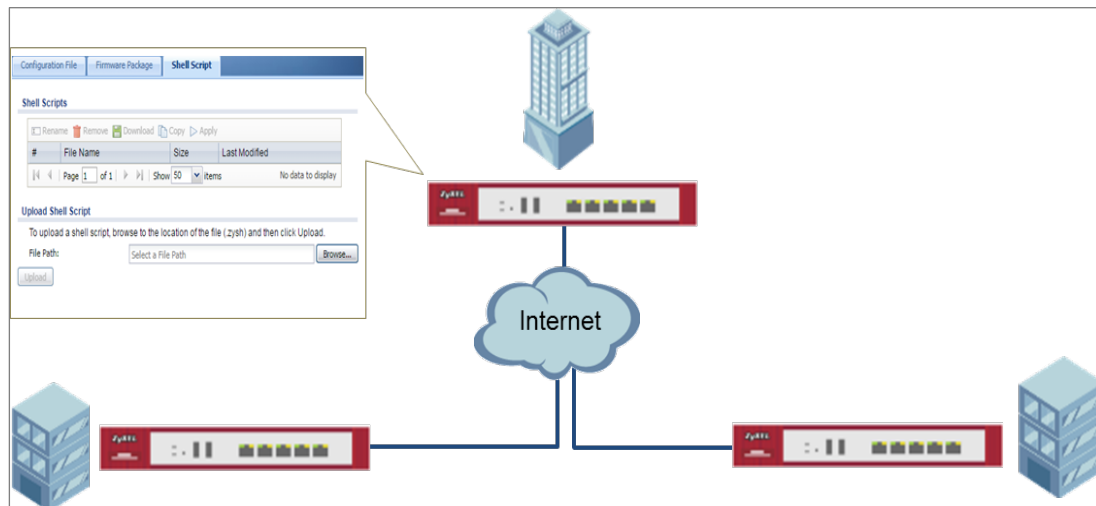
the portal page (<https://portal.myzyxel.com/>) to register or extend your

Application Patrol license.


After you apply the **Application Patrol** service, the running session will continue till it's finished.

How to continuously run a ZySH script

This example shows how to use shell script and continuously run a ZySH script automatically for maintenance purpose.

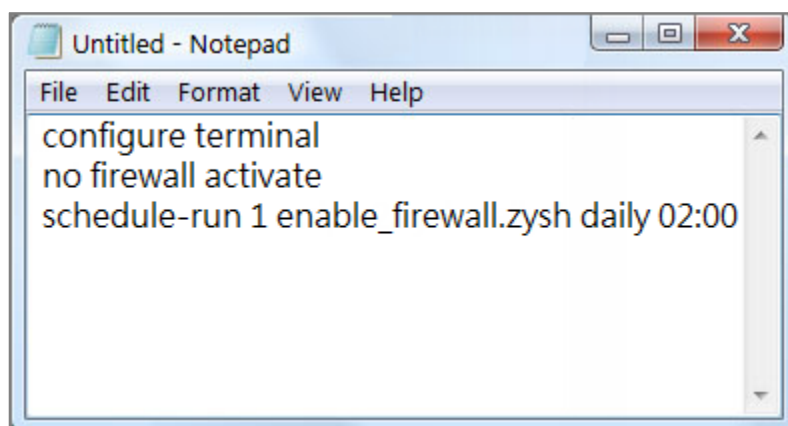


ZyWALL/USG continuously run a ZySH script Settings

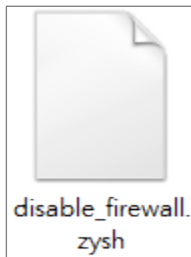
 Note: This example was tested using USG110 (Firmware Version: ZLD 4.25).

Set Up the Shell Script

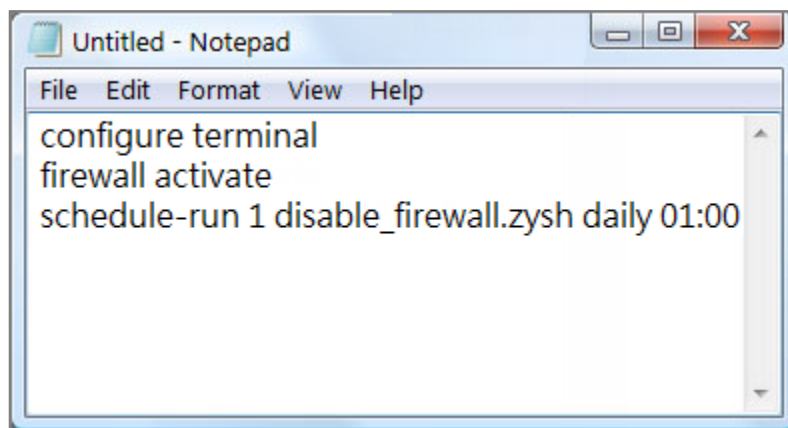
- 1 Run Windows Notepad application and input below command:



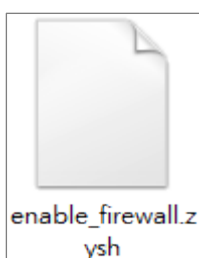
- 2 Save this file as "disable_firewall.zysh"



- 3 Run Windows Notepad application and input below command:



- 4 Save this file as "enable_firewall.zysh"



- 5 In the ZyWALL/USG, go to **MAINTENANCE > File Manager > Shell Script**. Click **Browse...** to find the disable_firewall.zysh and enable_firewall.zysh file. Click **Upload** to begin the upload process.

Shell Scripts

[Rename](#)
[Remove](#)
[Download](#)
[Copy](#)
[Apply](#)

| File Name | Size | Last Modified |
|-----------------------|------|---------------------|
| enable_firewall.zysh | 3 | 2017-06-29 14:48:25 |
| disable_firewall.zysh | 3 | 2017-06-29 14:48:13 |

Page 1 of 1
Show 50 Items
Displaying 1 - 2 of 2

Upload Shell Script

To upload a shell script, browse to the location of the file (.zysh) and then click Upload.

File Path:
[Browse...](#)
[Upload](#)

Set Up the Schedule Run

6 Issuing below commands:

Router> configure terminal

Router(config)# schedule-run 1 disable_firewall.zysh daily 15:15

```

10.214.30.87:22 - Tera Term VT
File Edit Setup Control Window Help
Router(config)# schedule-run 2 disable_firewall.zysh daily 15:15
Router(config)# write
Router(config)# reboot
    
```

Check the Result

1 In the ZyWALL/USG, go to **DASHBOARD**.

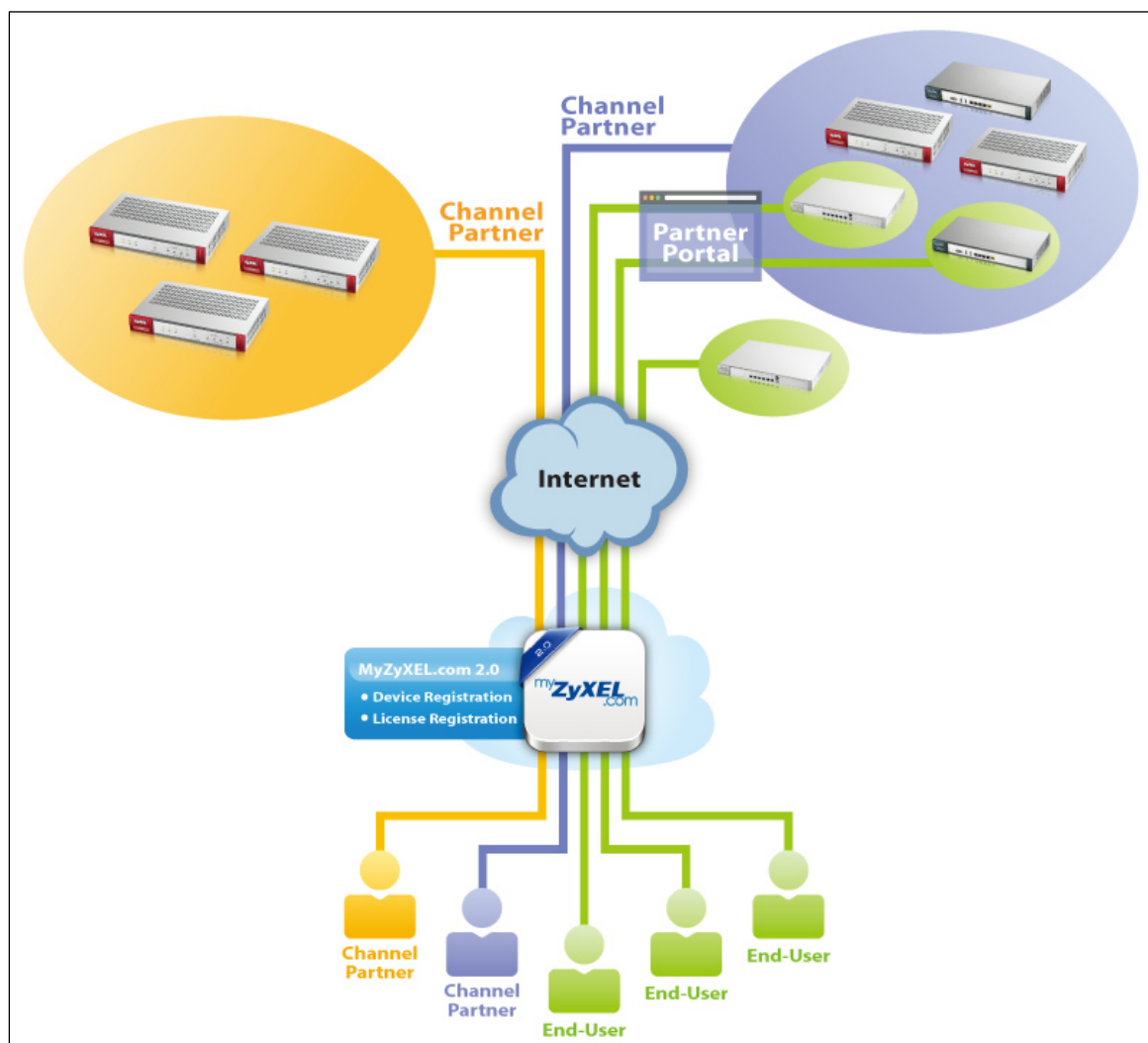
DASHBOARD

| | |
|---------------|---------------------------------|
| System Uptime | Current Date/Time |
| 00:02:48 | 2017-06-29 / 15:15:26 UTC+08:00 |

How To Register Your Device and Services at myZyXEL.com

myZyXEL.com is ZyXEL's online services center where you can register your ZyXEL device and manage subscription services available for the device. To update signature files or use a subscription service, you have to register the device and activate the corresponding service at myZyXEL.com.

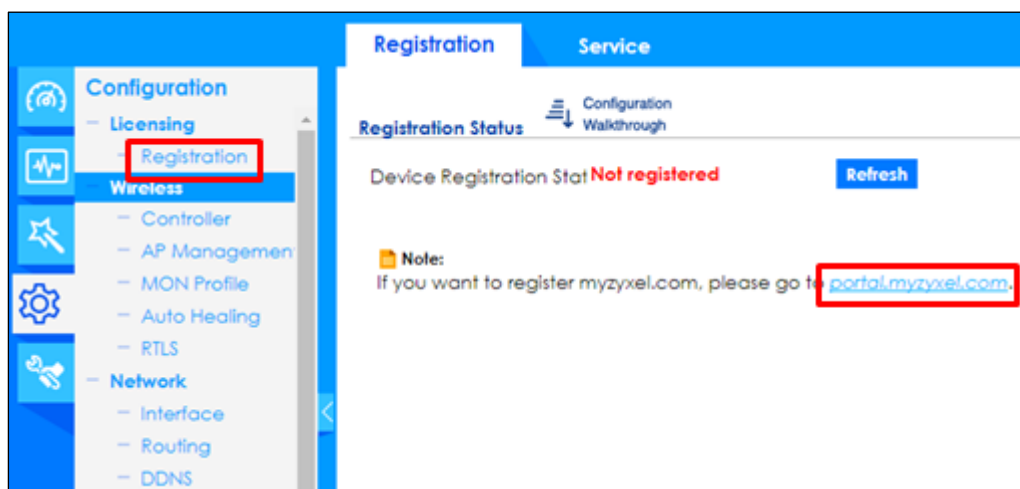
MyZyXEL.com 2.0 Management Architecture



Account Creation

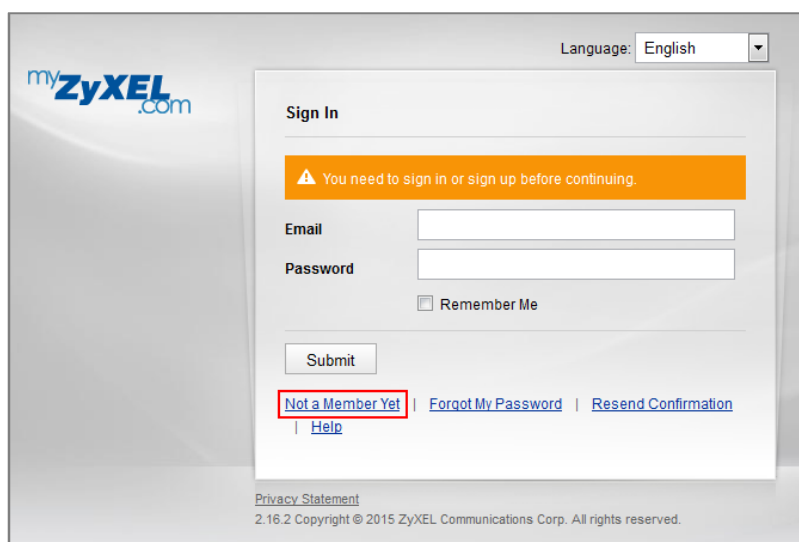
After you click the link from the **Registration** screen of your ZyXEL device's Web Configurator or click **the myZyXEL.com 2.0** icon from the portal page (<https://portal.myzyxel.com/>), the **Sign In** screen displays.

CONFIGURATION > Licensing > Registration



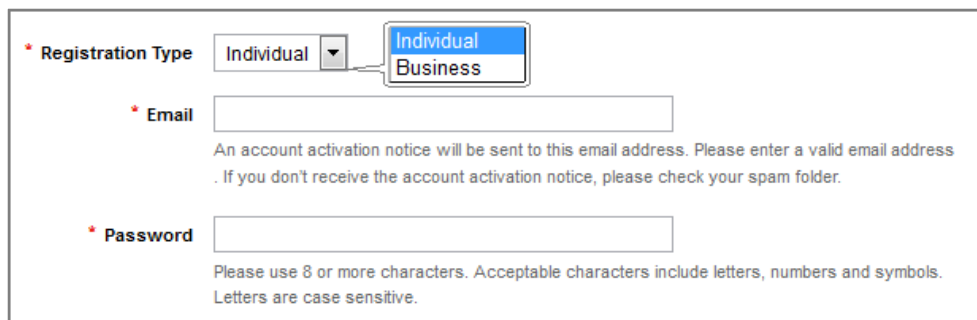
Click **Not a Member Yet** to open the **Sign Up** screen where you can create an account.


myZyXEL.com > Not a Member Yet



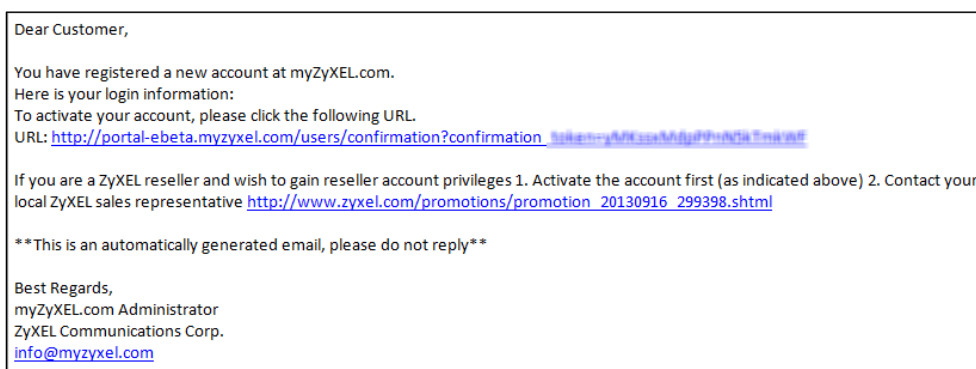
Select Registration Type to create an Individual account or a Business account. Individual account is for non-commercial, end user of ZyXEL products. Business account is for commercial users; VAT # is required (the requirement varies in selection of different countries)

myZyXEL.com > Not a Member Yet > Sign-up



 **Note:** The business account can be changed into a channel partner account by an administrator. With a channel partner account, you can register multiple devices and/or services at a time and check service status reports. Contact your sales representative to have a channel partner account.

After you click **Submit**, myZyXEL.com 2.0 will send you an account activation notification e-mail. Click the URL link from the e-mail to activate your account and log into myZyXEL.com 2.0.



After E-mail activate, sign in myZyXEL.com 2.0 to register or manage your devices and services. If you are a business account, please go to account page and press the **Reseller Request** button.



Device Registration

Click **Device Registration** in the navigation panel to open the screen. Use this screen to register your device with myZyXEL.com.

Enter the device's (first) **MAC Address** and **Serial Number**, which can be found on the sticker on the back of the device. Click **Submit**.

If you access myZyXEL.com from the **Registration** screen of your ZyXEL device's Web Configurator, the device **MAC Address** and **Serial Number** displays automatically.

myZyXEL.com

- Dashboard
- Device Management
- Service Management
- Maintenance Management
 - License Check
- Device Registration**
- Service Registration

Device Registration

Product Select: Device

* MAC Address:
i.e. 20:13:10:00:00:A0

* Serial Number:

Name:
Enter a name for this device (optional).

Reseller:

Enter the email address, VAT number or company name of the reseller selling you the device.

Service Registration (In the Case of Standard License)

Click **Service Registration** in the navigation panel to open the screen. Fill in the **License Key** as shown on **E-iCard License**.

myZyXEL.com

- Dashboard
- Device Management
- Service Management
- Maintenance Management
 - License Check
- Device Registration
- Service Registration**

Service Registration

* License Key:

Go to the **Service Management** page and click the **Link** button. Select the device then click the **Activate** button to initiate the services license. You will get a **Service Activation Notice** Email when you activate a new service.

| Service Management | | | | | |
|--------------------------|----------------------------|----------|------------------------------------|----------------------|--------------------------|
| Product Select | Device | Search | Please enter license key to search | | |
| License Key | Name | Type | Amount/Time | Linked Device | Status |
| S-CCF001-7B2655063E2A... | Content Filter_Commmtouch | Standard | 731 / 731 days | Link | Available |
| | Kaspersky Anti-Virus_Trial | Trial | 30 / 30 days | 00:00:AA:80:38:15 | Activate |
| | Anti-Spam_Trial | Trial | 30 / 30 days | 00:00:AA:80:38:15 | Activate |
| | IDP_Trial | Trial | 253 / 253 days | 00:00:AA:80:38:15 | Activate |

Device Management (In the Case of Registering Bundled Licenses)

Go to **Device Management** and click on the **MAC Address** hyper link of your device. In the **Linked Services** page, click the **Activate** button to initiate the services license. You will get a **Service Activation Notice** Email when you activate a new service.

| Device Management | | | | | |
|-------------------|-----------------------------------|--|-------------------|--------------------------------|----------------------|
| Product Select | Device | Search | MAC Address | Please choose a type to search | |
| Model | MAC Address | Linked Services | Registration Time | Status | Link to CF Report |
| ZyWALL 110 | 00:00:AA:80:38:15 | <ul style="list-style-type: none"> IDP Anti-Spam Kaspersky Anti-Virus Content Filter | 2014-08-07 12:44 | Active | Link |

| Linked Services | | | | |
|-------------------------------|---------------------------|--------------------------------|----------|--------------------------|
| Name | Remaining Amount / Period | Total Licensed Amount / Period | Trial | Status |
| IDP_Standard | 397 days | 397 days | Standard | Activate |
| Anti-Spam_Standard | 397 days | 397 days | Standard | Activate |
| Kaspersky Anti-Virus_Standard | 397 days | 397 days | Standard | Activate |
| Content Filter_Standard | 397 days | 397 days | Standard | Activate |

Refresh Service

After service activated, please go to the ZyWALL/USG **CONFIGURATION >**

Licensing > Registration > Service and click the **Service License Refresh** button to update the **Status**.

| License Status | | | | | | |
|---|---------------------------------|----------|-------------------|-----------------|-------|--|
| # | Service | Status | Registration Type | Expiration Date | Count | |
| 1 | IDP/AppPatrol Signature Service | Licensed | Standard | 2016-7-2 | N/A | |
| 2 | Anti-Virus Signature Service | Licensed | Standard | 2016-7-2 | N/A | |
| 3 | Anti-Spam Service | Licensed | Standard | 2016-7-2 | N/A | |
| 4 | Content Filter Service | Licensed | Standard | 2016-7-2 | N/A | |
| 5 | SSL VPN Service | Licensed | | | 255 | |
| 6 | Managed AP Service | Default | Standard | | 2 | |
| Page 1 of 1 Show 50 items Displaying 1 - 6 of 6 | | | | | | |
| License Refresh | | | | | | |
| <div>Service License Refresh</div> | | | | | | |

What Could Go Wrong?

If you can't activate your device's service license, please check if you entered a correct license key. Or your login session connecting to the device's Web GUI or to myZyXEL.com might have been timed out. Please try to login again.

If the device fails to register and connect to myzyxel.com, please ensure that the WAN interface IP address can public access to Internet is working properly.

If you forget your password of myzyxel.com account, please click the "Forgot My Password" link on the login screen and enter your email address. MyZyXEL.com 2.0 will send an email to you with a link to change your password.



www.zyxel.com

Dear Customer,

You have requested to reset your myZyXEL.com password. Please click the following link to change your password.
https://portal.myzyxel.com/users/password/edit?reset_password_token=1504041935296-CeQm43

****This is an automatically generated email, please do not reply****

Best Regards,
myZyXEL.com Administrator
ZyXEL Communications Corp.
info@myzyxel.com

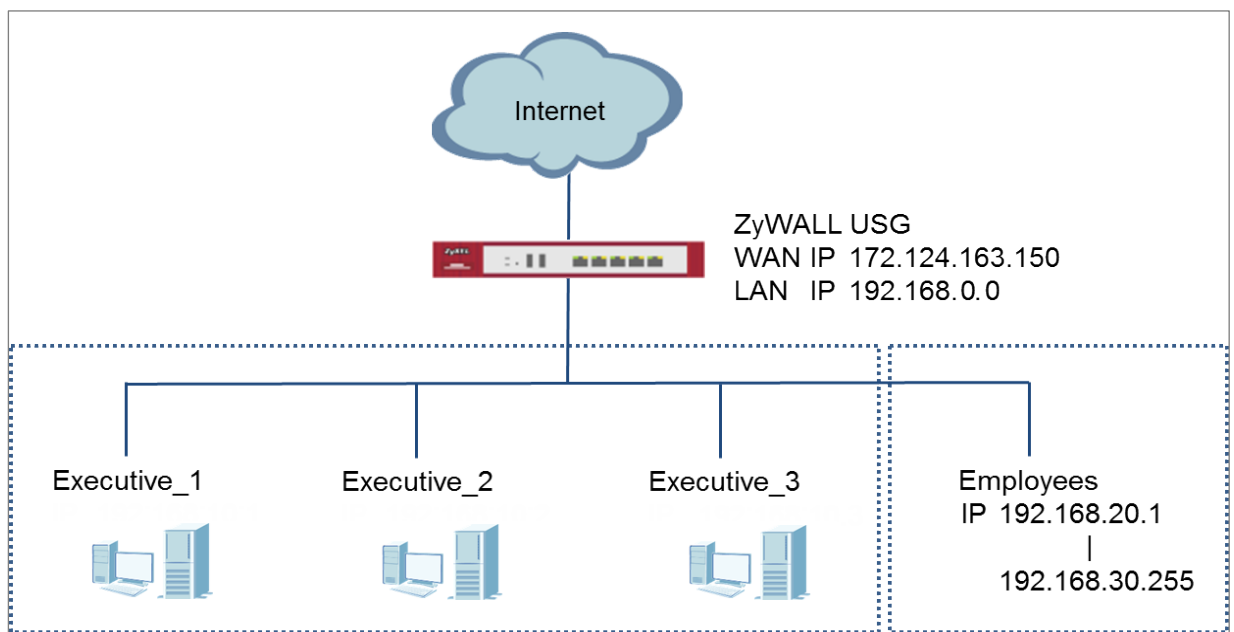
If you forget your registered email address on myZyXEL.com, please go to the link below and submit a request to ZyXEL support team for further support:


http://www.zyxel.com/form/Support_Feedback.shtml

How To Exempt Specific Users From Security Control

This is an example of using a ZyWALL/USG Security Policy to exempt three corporate executives from security control, while controlling Internet access for other employees' accounts.

Exempt Specific Users from Security Control Example

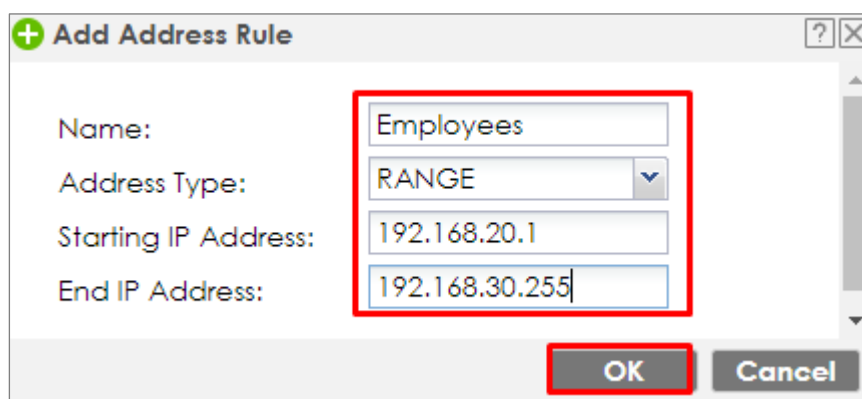


 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the Security Policy on the ZyWALL/USG for Employees

In the ZyWALL/USG, go to **CONFIGURATION > Object > Address > Add Address Rule** to create address range for employees.

CONFIGURATION > Object > Address > Add Address Rule



Set up **Security Policy** for employees, go to **CONFIGURATION > Security Policy > Policy Control > Add corresponding**, configure a **Name** for you to identify the employees' **Security Policy** profile.

For **From** and **To** policies, select the direction of travel of packets to which the policy applies. Select **Source** to be the **Employees** to apply the policy to all traffic coming from them. In order to view the test result later on, set **Log matched traffic** to be **log**.

Scroll down to **UTM Profile**, select the general policy that allows employees to access the Internet. (Using built-in Office profile in this example blocks the non-productive services, such as Advertisement & Pop-Ups, Gambling and Peer to Peer services...etc.).

CONFIGURATION > Security Policy > Policy Control > Add corresponding > Employees_Security

| | |
|---|---------------------|
| <input checked="" type="checkbox"/> Enable | |
| Name: | Employees_Security |
| Description: | (Optional) |
| From: | LAN |
| To: | any (Excluding ZyV) |
| Source: | Employees |
| Destination: | any |
| Service: | any |
| User: | any |
| Schedule: | none |
| Action: | allow |
| Log matched traffic: | log |

| UTM Profile | |
|---|----------------|
| <input checked="" type="checkbox"/> Content Filter: | Office_profile |
| <input type="checkbox"/> SSL Inspection: | none |

Set Up the Security Policy on the ZyWALL/USG for Executives

In the ZyWALL/USG, go to **CONFIGURATION > Object > User/Group > Add A User** to create **User Name/Password** for each executive.

CONFIGURATION > Object > User/Group > Add A User

| User Configuration | |
|--------------------|-------------|
| User Name : | Executive_1 |
| User Type: | user |
| Password: | |
| Retype: | |
| Description: | Local User |

| User Configuration | |
|--------------------|-------------|
| User Name : | Executive_2 |
| User Type: | user |
| Password: | |
| Retype: | |
| Description: | Local User |

| User Configuration | |
|--------------------|-------------|
| User Name : | Executive_3 |
| User Type: | user |
| Password: | |
| Retype: | |
| Description: | Local User |

Then, go to **CONFIGURATION > Object > User/Group > Group > Add Group** to create a **Group Members' Name** and move the just created executives user object to **Member**.

CONFIGURATION > Object > Address Group > Add Address Group Rule

Configuration

Name:

Description: (Optional)

Member List

| Available | | Member |
|----------------|--------|--------|
| === Object === | | |
| Executive_1 | ➔ ➜ | |
| Executive_2 | | |
| Executive_3 | | |
| ad-users | | |
| ldap-users | | |
| radius-users | | |

Set up **Security Policy** for executives, go to **CONFIGURATION > Security Policy > Policy Control > Add corresponding**, configure a **Name** for you to identify the executives' **Security Policy** profile.

For **From** and **To** policies, select the direction of travel of packets to which the policy applies. Select **User** to be the **Executives** to apply the policy to all traffic coming from them.

In order to view the test result later on, set **Log matched traffic** to be **log**.

Leave all **UTM Profiles** disabled.

CONFIGURATION > Security Policy > Policy Control > Add corresponding > Employees_Security

☒ Enable

| | | |
|----------------------|--------------------|------------|
| Name: | Executive_Security | |
| Description: | | (Optional) |
| From: | LAN | |
| To: | any (Excluding ZyV | |
| Source: | any | |
| Destination: | any | |
| Service: | any | |
| User: | Executive | |
| Schedule: | none | |
| Action: | allow | |
| Log matched traffic: | log | |

UTM Profile

Test the Result

Connect to the Internet from two computers: one from executive_1 and one from an employee address (192.168.30.9).

Go to the ZyWALL/USG **Monitor > Log**, you will see [notice] log message such as below. In this example result, a connection from executive_1 has user login message and always with **ACCESS FORWARD** information. A connection from employee address (192.168.30.9) and some of the services are with **ACCESS BLOCK** information

Monitor > Log

| Priority | Category | Message | Source | Destination | Note |
|----------|-------------------------|--|--------------------|-------------------|----------------------|
| notice | Security Policy Control | priority:1, from LAN to ANY, TCP, service others, ACCEPT | 192.168.1.33:60045 | 172.23.5.208:8080 | ACCESS FORWARD |
| notice | Security Policy Control | priority:1, from LAN to ANY, TCP, service others, ACCEPT | 192.168.1.33:60044 | 59.124.183.66:443 | ACCESS FORWARD |
| notice | User | User Executive_1(MAC=F0:DE:F1:B7:FB:7E) from http/https has logged in Device | 192.168.1.33 | 59.124.183.150 | Account: Executive_1 |

| Priority | Category | Message | Source | Destination | Note |
|----------|-------------------------|---|--------------------|-------------------|----------------|
| notice | Security Policy Control | priority:2, from LAN to ANY, TCP, service others, ACCEPT | 192.168.30.9:50928 | 74.125.23.189:443 | ACCESS FORWARD |
| info | Application Patrol | Rule_id=2 SSI=N App=[Social Network]Google-plus:authority Action=reject SID=402692097 | 192.168.30.9:50926 | 74.125.23.113:443 | ACCESS BLOCK |
| info | Application Patrol | Rule_id=2 SSI=N App=[Social Network]Facebook:authority Action=reject SID=402653953 | 192.168.30.9:51041 | 66.220.158.19:443 | ACCESS BLOCK |

What Could Go Wrong?

If you are not be able to configure any **UTM** policies or it's not working, there are two possible reasons:

You have not subscribed for the **UTM** service.

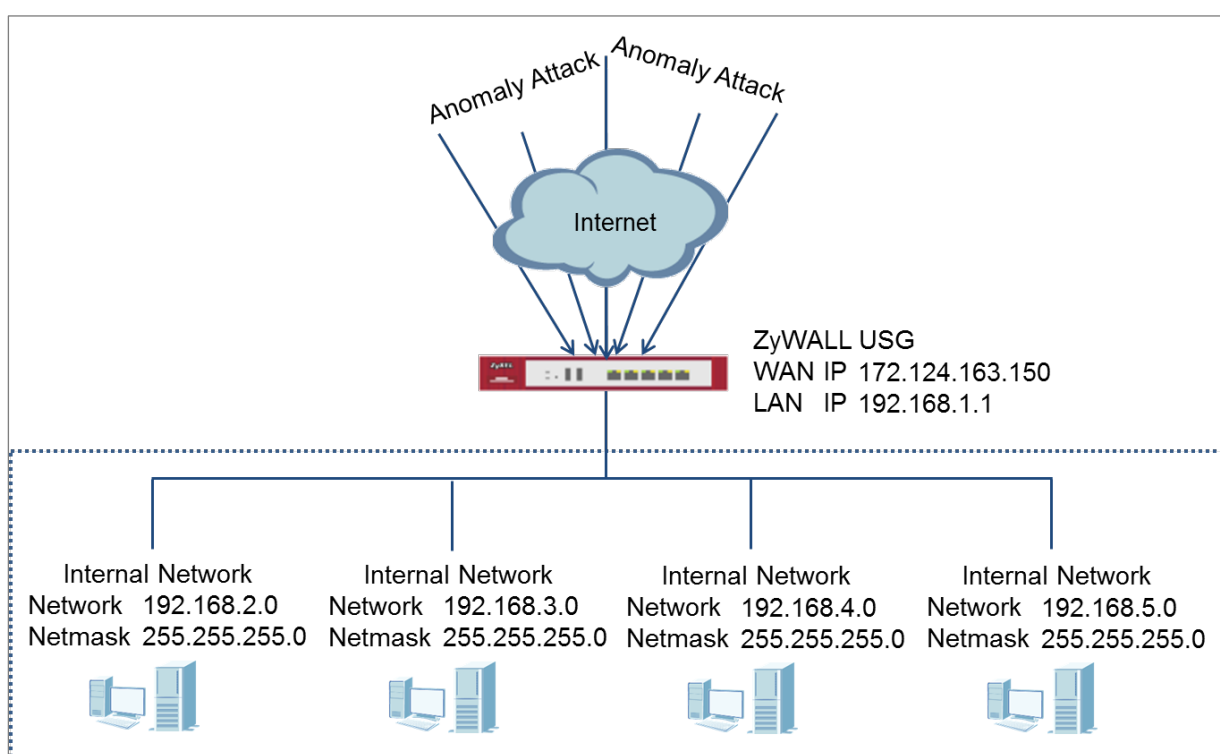
You have subscribed for the **UTM** service but the license is expired.


You can click the link from the **CONFIGURATION > Licensing > Registration** screen of your ZyXEL device's Web Configurator or click the myZyXEL.com 2.0 icon from the portal page (<https://portal.myzyxel.com/>) to register or extend your **UTM** license.

How To Detect and Prevent TCP Port Scanning with ADP

This is an example of using a ZyWALL/USG ADP (Anomaly Detection and Prevention) Profile to protect against anomalies based on violations of protocol standards (RFCs – Requests for Comments) and abnormal traffic flows such as port scans.

ZyWALL/USG with ADP Profile Setting Example

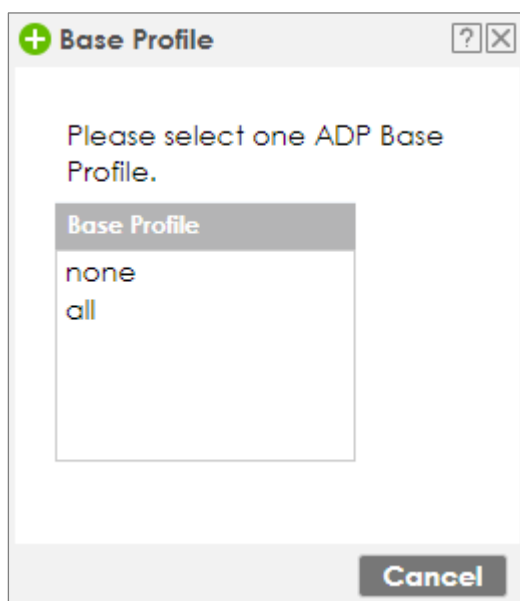


 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the ADP Profile on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Security Policy > ADP > Profile**, click the **Add** icon. A pop-up screen will appear allowing you to choose a base profile. Select a base profile to go to the profile details screen.

CONFIGURATION > Security Policy > ADP > Profile > Base Profile



The **Traffic Anomaly** screen will display. A **Name** is automatically generated that you can edit. Enable or disable individual scan or flood types by selecting a row and clicking **Activate** or **Inactivate**.

In the **Scan Detection** section, selecting levels in the **Sensitivity** drop-down menu and set **Block Period** for the duration applies blocking to the source IP address.

In the **Flood Detection** section, set **Block Period** for the duration applies blocking to the destination IP address. Set a **Threshold** number (the number of packets per second that match the flood detection criteria) for your network. Click **OK**.

CONFIGURATION > Security Policy > ADP > Profile > Base Profile > Traffic Anomaly

General

Name: **APF1895**

Description:

Scan Detection

Sensitivity: medium

Block Period: **10** (1-3600 seconds)

☐ Activate
 ☐ Inactivate
 ☐ Log
 ☐ Action

| # | Status | Name | Log | Action |
|---|--------|-----------------------------|-----|--------|
| 1 | | (portscan) IP Protocol Scan | no | none |
| 2 | | (portscan) TCP Portscan | no | none |
| 3 | | (portscan) UDP Portscan | no | none |
| 4 | | (sweep) ICMP Sweep | no | none |
| 5 | | (sweep) IP Protocol Sweep | no | none |
| 6 | | (sweep) TCP Port Sweep | no | none |
| 7 | | (sweep) UDP Port Sweep | no | none |

|< < Page 1 of 1 > >| Show 50 items

Displaying 1 - 7 of 7

Flood Detection

Block Period: **5** (1-3600 seconds)

☐ Edit
 ☐ Activate
 ☐ Inactivate
 ☐ Log
 ☐ Action

| # | Status | Name | Log | Action | Threshold(p... |
|---|--------|--------------------|-----|--------|----------------|
| 1 | | (flood) ICMP Flood | no | none | 1000 |
| 2 | | (flood) IP Flood | no | none | 1000 |
| 3 | | (flood) TCP Flood | no | none | 1000 |
| 4 | | (flood) UDP Flood | no | none | 1000 |

|< < Page 1 of 1 > >| Show 50 items

Displaying 1 - 4 of 4

Click the **Protocol Anomaly** tab. A **Name** is automatically generated that you can edit. Enable or disable individual rules by selecting a row and clicking **Activate** or **Inactivate**. Edit the default log options and actions by selecting a row and making a selection in the **Log** or **Action** drop-down menus. Click **OK**.

CONFIGURATION > Security Policy > ADP > Profile > Base Profile > Protocol Anomaly

General

Name:

Description:

TCP Decoder

☒ Activate
 ☐ Inactivate
 ☒ Log
 ☒ Action

| # | Status | Name | Log | Action |
|---|--------|------------------------------------|-----|--------|
| 1 | | (tcp_decoder) BAD-LENGTH-OPTI... | no | none |
| 2 | | (tcp_decoder) EXPERIMENTAL-OP... | no | none |
| 3 | | (tcp_decoder) OBSOLETE-OPTION... | no | none |
| 4 | | (tcp_decoder) OVERSIZE-OFFSET A... | no | none |
| 5 | | (tcp_decoder) TRUNCATED-OPTIO... | no | none |
| 6 | | (tcp_decoder) TTCP-DETECTED AT... | no | none |
| 7 | | (tcp_decoder) UNDERSIZE-LEN ATT... | no | none |
| 8 | | (tcp_decoder) UNDERSIZE-OFFSET ... | no | none |
| 9 | | (tcp_decoder) tcp-fragment ATTA... | no | none |

Displaying 1 - 9 of 9

UDP Decoder

☒ Activate
 ☐ Inactivate
 ☒ Log
 ☒ Action

| # | Status | Name | Log | Action |
|---|--------|-----------------------------------|-----|--------|
| 1 | | (udp_decoder) OVERSIZE-LEN ATT... | no | none |
| 2 | | (udp_decoder) TRUNCATED-HEAD... | no | none |
| 3 | | (udp_decoder) UNDERSIZE-LEN AT... | no | none |

Displaying 1 - 3 of 3

ICMP Decoder

☒ Activate
 ☐ Inactivate
 ☒ Log
 ☒ Action

| # | Status | Name | Log | Action |
|---|--------|----------------------------------|-----|--------|
| 1 | | (icmp_decoder) TRUNCATED-ADD... | no | none |
| 2 | | (icmp_decoder) TRUNCATED-HEA... | no | none |
| 3 | | (icmp_decoder) TRUNCATED-TIME... | no | none |
| 4 | | (icmp_decoder) icmp-fragment ... | no | none |

Displaying 1 - 4 of 4

IP Decoder

☒ Activate
 ☐ Inactivate
 ☒ Log
 ☒ Action

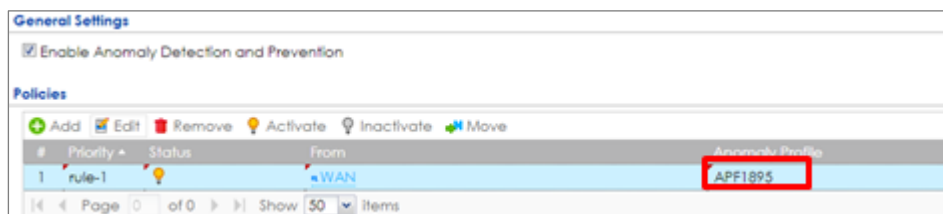
| # | Status | Name | Log | Action |
|---|--------|------------------------------------|-----|--------|
| 1 | | (ip_decoder) BAD-LENGTH-OPTIO... | no | none |
| 2 | | (ip_decoder) IP-land ATTACK | no | none |
| 3 | | (ip_decoder) TRUNCATED-OPTION... | no | none |
| 4 | | (ip_decoder) UNDERSIZE-LEN ATTA... | no | none |
| 5 | | (ip_decoder) ip-spoof ATTACK | no | none |
| 6 | | (ip_decoder) ip-teardrop ATTACK | no | none |

Displaying 1 - 6 of 6

Go to **CONFIGURATION > Security Policy > ADP > General**, select **Enable Anomaly**

Detection and Prevention. Then, select the just created **Anomaly Profile** and click **Apply**.

CONFIGURATION > Security Policy > ADP > General

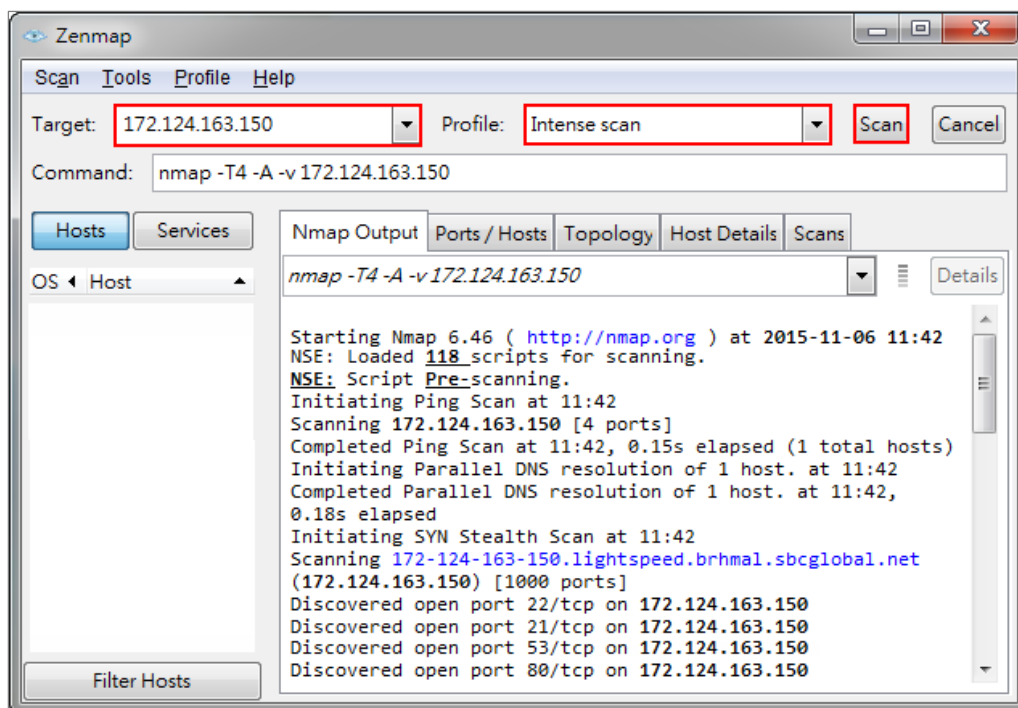


Test the Result

Download Nmap free security scanner for testing the result:

<https://nmap.org/download.html>

Open the Nmap GUI, set the **Target** to be the WAN IP of ZyWALL/USG (172.124.163.150 in this example) and set **Profile** to be **Intense Scan**. Click **Scan**.



Go to the ZyWALL/USG **Monitor > Log**, you will see [warn] log message such as below.

Monitor > Log

| Priority | Category | Message | Source | Destination | Note |
|----------|----------|---|----------------------|-----------------------|--------------|
| warn | ADP | from Any to ZyWALL, [type=Scan-Detection(8910011)] tcp-portscan-syn tcp-portscan-syn Action: Block Severity: medium | 192.168.123.33:40347 | 172.124.163.150:1271 | ACCESS BLOCK |
| warn | ADP | from Any to ZyWALL, [type=Scan-Detection(8910011)] tcp-portscan-syn tcp-portscan-syn Action: Block Severity: medium | 192.168.123.33:40374 | 172.124.163.150:8888 | ACCESS BLOCK |
| warn | ADP | from Any to ZyWALL, [type=Scan-Detection(8910011)] tcp-portscan-syn tcp-portscan-syn Action: Block Severity: medium | 192.168.123.33:40348 | 172.124.163.150:13 | ACCESS BLOCK |
| warn | ADP | from Any to ZyWALL, [type=Scan-Detection(8910011)] tcp-portscan-syn tcp-portscan-syn Action: Block Severity: medium | 192.168.123.33:40347 | 172.124.163.150:15003 | ACCESS BLOCK |

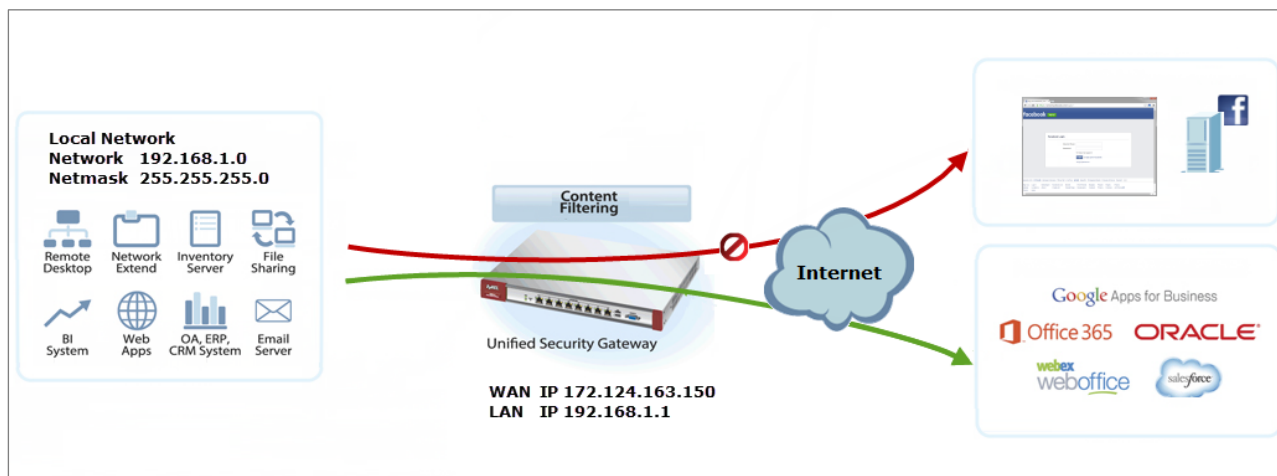
What Could Go Wrong?


You may find that certain rules are triggering too many false positives or false negatives. A false positive is when valid traffic is flagged as an attack. A false negative is when invalid traffic is wrongly allowed to pass through the ZyWALL/USG. As each network is different, false positives and false negatives are common on initial ADP deployment. You could create a new 'monitor profile' that creates logs but all actions are disabled. Observe the logs over time and try to eliminate the causes of the false alarms. When you're satisfied that they have been reduced to an acceptable level, you could then create an 'inline profile' whereby you configure appropriate actions to be taken when a packet matches a detection.

How To Block Facebook

This is an example of using a ZyWALL/USG UTM Profile in a Security Policy to block access to a specific social network service. You can use Content Filter, SSL Inspection and Policy Control to make sure that a certain web page cannot be accessed through both HTTP and HTTPS protocols.

ZyWALL/USG with Block Facebook Settings Example

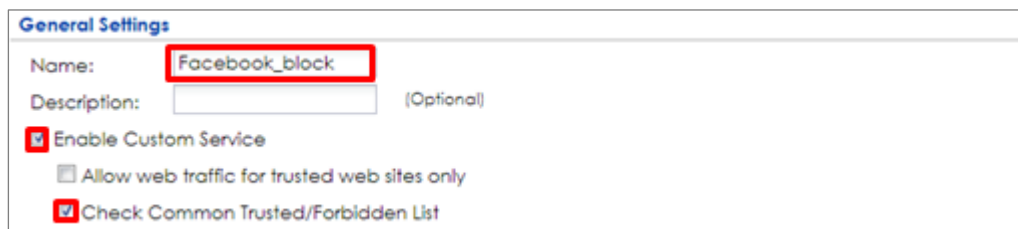


 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the Content Filter on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > UTM Profile > Content Filter > Profile Management > Add Filter File > Custom Service**. Configure a **Name** for you to identify the **Content Filter Profile** and select **Enable Custom Service**.

CONFIGURATION > UTM Profile > Content Filter > Profile > Profile Management > Add Filter File > Custom Service > General Settings



General Settings

Name: **Facebook_block**

Description: (Optional)

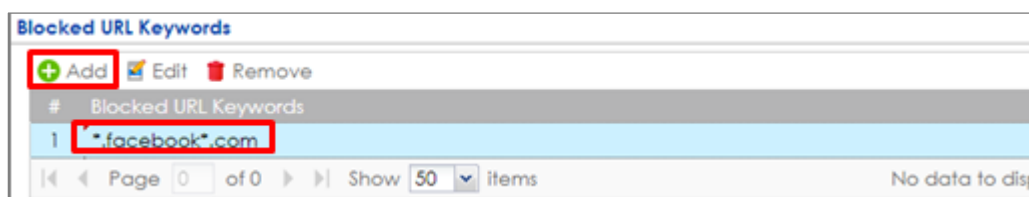
☒ Enable Custom Service

☐ Allow web traffic for trusted web sites only

☒ Check Common Trusted/Forbidden List

Scroll down to the **Blocked URL Keywords** section, click **Add** and use "*" as a wildcard to match any string in trusted/forbidden web sites and blocked URL keywords (*.facebook*.com in this example). Click **OK**.

CONFIGURATION > UTM Profile > Content Filter > Profile > Profile Management > Add Filter File > Custom Service > Blocked URL Keywords



Blocked URL Keywords

Add Edit Remove

| # | Blocked URL Keywords |
|---|------------------------|
| 1 | *.facebook*.com |

Page 0 of 0 Show 50 items No data to display

Set Up the SSL Inspection on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > UTM Profile > SSL Inspection > Add rule**, configure a **Name** for you to identify the **SSL Inspection** profile.

Then, select the **CA Certificate** to be the certificate used in this profile. Select

Block to **Action for Connection with SSL v3** and select **Log** type to be **log alert**.

Leave other actions as default settings.

CONFIGURATION > UTM Profile > SSL Inspection > Add rule

| General Settings | | | |
|--|----------------|------|-----|
| Name: | Facebook_Block | | |
| Description: | | | |
| CA Certificate: | default | | |
| SSL/TLS version supported minimum: | ssl3 | Log: | no |
| Action for connection with unsupported suit: | pass | Log: | no |
| Action for connection with untrusted cert chain: | pass | Log: | log |

Set Up the Security Policy on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Security Policy > Policy Control**, configure a **Name** for you to identify the **Security Policy** profile. For **From** and **To** policies, select the direction of travel of packets to which the policy applies. Select the **Schedule** that defines when the policy applies (Facebook_Block in this example).

Scroll down to **UTM Profile**, select **Content Filter** and select a profile from the list box (Facebook_Block in this example). Then, select **SSL Inspection** and select a profile from the list box (Facebook_Block in this example).

CONFIGURATION > Security Policy > Policy Control

| | |
|--|---------------------|
| <input checked="" type="checkbox"/> Enable | |
| Name: | Facebook_Block |
| Description: | (Optional) |
| From: | LAN |
| To: | any (Excluding ZyV) |
| Source: | any |
| Destination: | any |
| Service: | any |
| User: | any |
| Schedule: | none |
| Action: | allow |
| Log matched traffic: | no |

| UTM Profile | |
|---|----------------|
| <input checked="" type="checkbox"/> Content Filter: | Facebook_Block |
| <input checked="" type="checkbox"/> SSL Inspection: | Facebook_Block |

Export Certificate from ZyWALL/USG and Import it to Windows 7 Operation System

When SSL inspection is enabled and an access website does not trust the ZyWALL/USG certificate, the browser will display a warning page of security certificate problems.

Go to ZyWALL/USG **CONFIGURATION > Object > Certificate > default > Edit** to export default certificate from ZyWALL/USG with Private Key (zyx123 in this example).

CONFIGURATION > Object > Certificate > default

| My Certificates Setting | | | | | | |
|--|---------|------|------------------------|------------------------|-------------------------|-------------------------|
| <div> + Add ✎ Edit ✖ Remove 🔗 Object References </div> | | | | | | |
| # | Name | Type | Subject | Issuer | Valid From | Valid To |
| 1 | default | SELF | CN=vpn300_B8ECA3A9C... | CN=vpn300_B8ECA3A9C... | 2017-04-25 12:41:25 GMT | 2027-04-23 12:41:25 GMT |
| <div> ⏪ ⏩ Page 1 of 1 ▶▶ Show 50 items Displaying 1 - 1 of 1 </div> | | | | | | |

CONFIGURATION > Object > Certificate > default > Edit > Export Certificate with Private Key

✎

Edit My Certificates

?

✕

Issuer:

CN=vpn300_B8ECA3A9C003

Signature Algorithm:

rsa-pkcs1-sha256

Valid From:

2017-04-25 12:41:25 GMT

Valid To:

2027-04-23 12:41:25 GMT

Key Algorithm:

rsaEncryption (2048 bits)

Subject Alternative Name:

vpn300_B8ECA3A9C003

Key Usage:

DigitalSignature, KeyEncipherment, DataEncipherment, KeyCertSi

Extended Key Usage:

Basic Constraint:

Subject Type=CA, Path Length Constraint=1

MD5 Fingerprint:

1b:a9:ff:f3:e6:42:44:9c:90:8d:bc:3e:f9:07:af:26

SHA1 Fingerprint:

1b:dd:6e:b2:c7:89:2e:ea:43:a0:ee:d2:55:3a:ff:15:89:bc:64:70

Certificate in PEM (Base-64) Encoded Format

-----BEGIN X509 CERTIFICATE-----

MIIDSzCCAjOgAwIBAgIJAP0XXinyW6C/MA0GC5qGSIlb3DQEBChwUAMB4xHDAaBgNV

BAMME3ZwbjMwMF9COEVDQTNBOUMwMDMwHhcNMTCwNDI1MTI0MTI1WhcNMjcw

NDIz

Password:

••••

Export Certificate Only

Export Certificate with Private Key

OK

Cancel

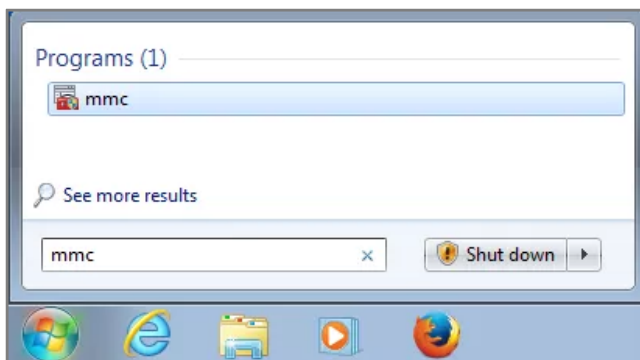
Save default certificate as *.p12 file to Windows 7 Operation System.



default.p12

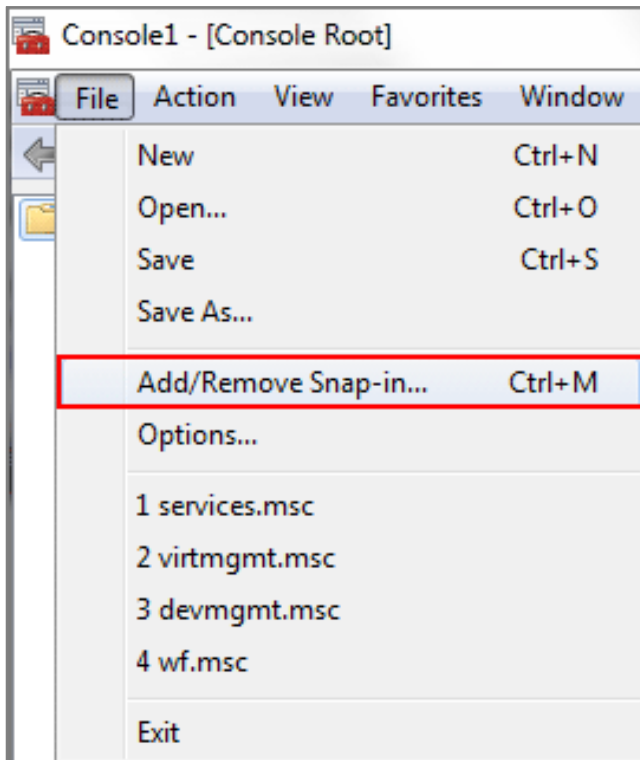
In Windows 7 Operating System **Start Menu > Search Box**, type **mmc** and press **Enter**.

Start Menu > Search Box > mmc



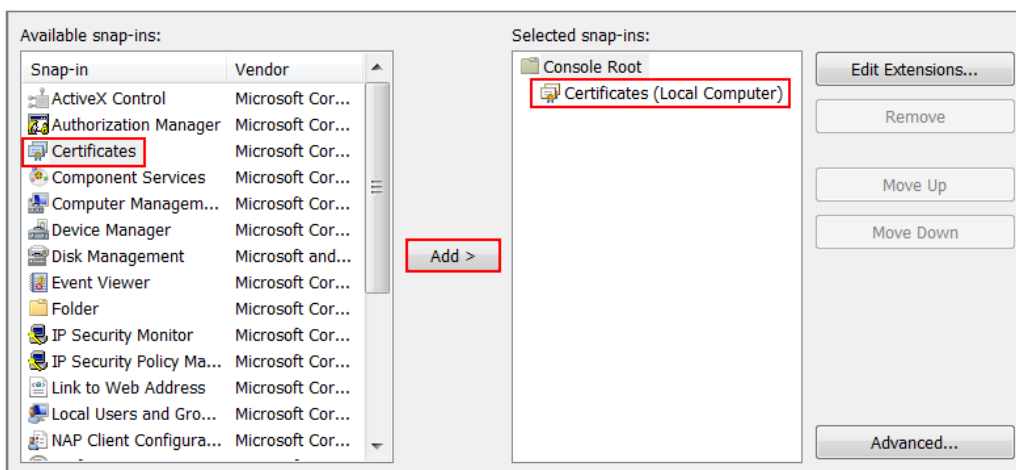
In the mmc console window, click **File > Add/Remove Snap-in...**

File > Add/Remove Snap-in...

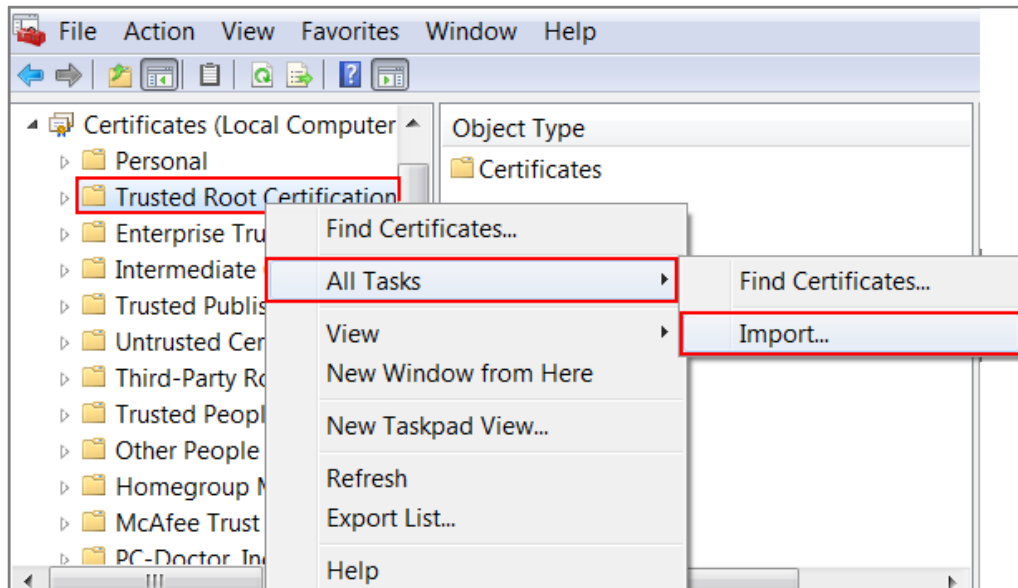


In the **Available snap-ins**, select the **Certificates** and click **Add** button. Select **Computer account > Local Computer**. Then, click **Finished** and **OK** to close the **Snap-ins** window.

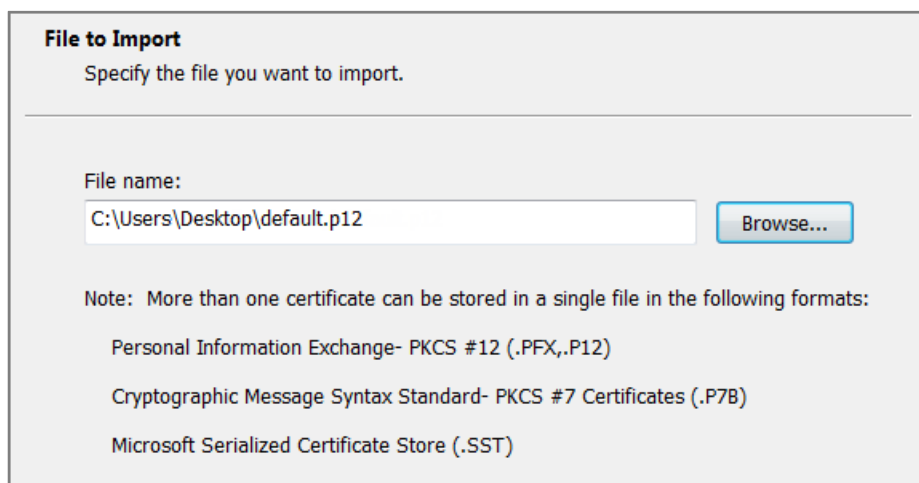
Available snap-ins > Certificates > Add



In the mmc console window, open the **Certificates (Local Computer) > Trusted Root Certification Authorities**, right click **Certificate > All Tasks > Import...**



Click **Next**. Then, **Browse...**, and locate the .p12 file you downloaded earlier. Then, click **Next**.



Click **Next**, type **zyx123** in the **Password** field and click **Next** again

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

•••••

☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☐ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☒ Include all extended properties.

Select **Place all certificates in the following store** and then click **Browse** and find **Trusted Root Certification Authorities**. Click **Next**, then click **Finish**.

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.


☐ Automatically select the certificate store based on the type of certificate

☒ Place all certificates in the following store

Certificate store:

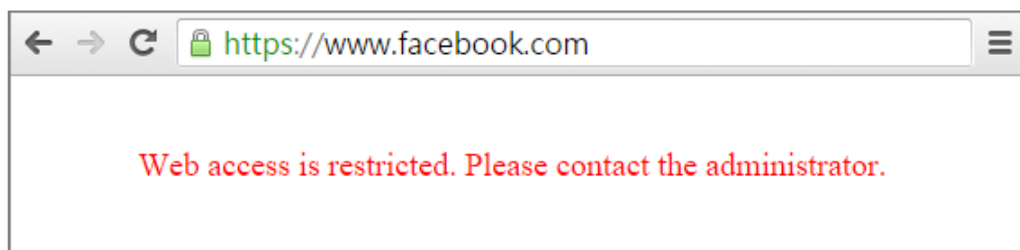
Trusted Root Certification Authorities

Browse...

 **Note:** Each ZyWALL/USG device has its own self-signed certificate by factory default. When you reset to default configuration file, the original self-signed certificate is erased, and a new self-signed certificate will be created when the ZyWALL/USG boots the next time.

Test the Result

Type <http://www.facebook.com/> or <https://www.facebook.com/> into the browser, the error message occurs.



Go to the ZyWALL/USG **Monitor > Log**, you will see [alert] log message such as below.

Monitor > Log

| Priority | Category | Message | Note |
|----------|-------------------|---|-----------|
| alert | Blocked web sites | d2ebu295n9axq5.webhst.com: Keyword blocking, Rule_id=1, SSI=N | WEB BLOCK |
| alert | Blocked web sites | d2ebu295n9axq5.webhst.com: Keyword blocking, Rule_id=1, SSI=N | WEB BLOCK |

What Could Go Wrong?

If you are not be able to configure any **Content Filter** policies or it's not working, there are two possible reasons:

You have not subscribed for the **Content Filter** service.

You have subscribed for the **Content Filter** service but the license is expired.

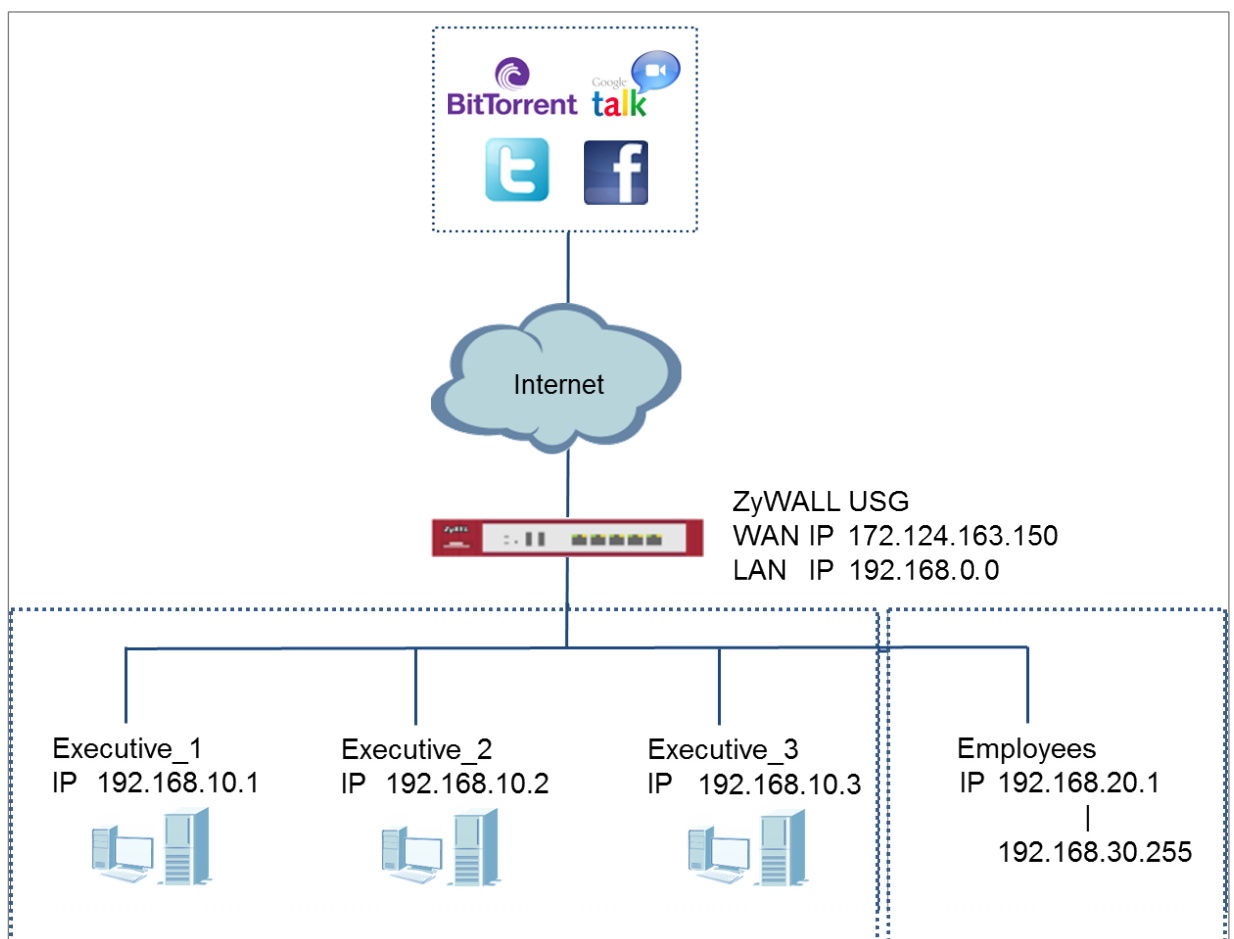
You can click the link from the **CONFIGURATION > Licensing > Registration** screen of your ZyXEL device's Web Configurator or click the myZyXEL.com 2.0 icon from the portal page (<https://portal.myzyxel.com/>) to register or extend your **Content Filter** license.

How To Exempt Specific Users From a Blocked Website

This is an example of using a ZyWALL/USG Security Policy to exempt three corporate executives from a blocked Website, while controlling Internet access for other employees' accounts.

With executives connect to a blocked Website using PCs with static IP addresses, you could set up address group to allow their traffic.

ZyWALL/USG with Exempt Specific Users From a Blocked Website Example

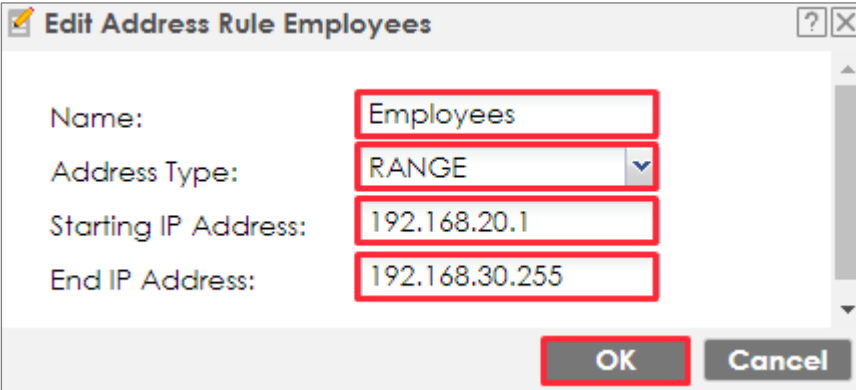


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the Security Policy on the ZyWALL/USG for Employees

In the ZyWALL/USG, go to **CONFIGURATION > Object > Address > Add Address Rule** to create address range for employees.

CONFIGURATION > Object > Address > Add Address Rule



Edit Address Rule Employees

Name: Employees

Address Type: RANGE

Starting IP Address: 192.168.20.1

End IP Address: 192.168.30.255

OK Cancel

Set up **Security Policy** for employees, go to **CONFIGURATION > Security Policy > Policy Control > Add corresponding**, configure a **Name** for you to identify the employees' **Security Policy** profile.

For **From** and **To** policies, select the direction of travel of packets to which the policy applies. Select **Source** to be the **Employees** to apply the policy to all traffic coming from them.

Scroll down to **UTM Profile**, select the general policy that allows employees to access the Internet. (Using built-in Office profile in this example blocks the non-productive services, such as Advertisement & Pop-Ups, Gambling and Peer to Peer services...etc.).

CONFIGURATION > Security Policy > Policy Control > Add corresponding > Employees_Security

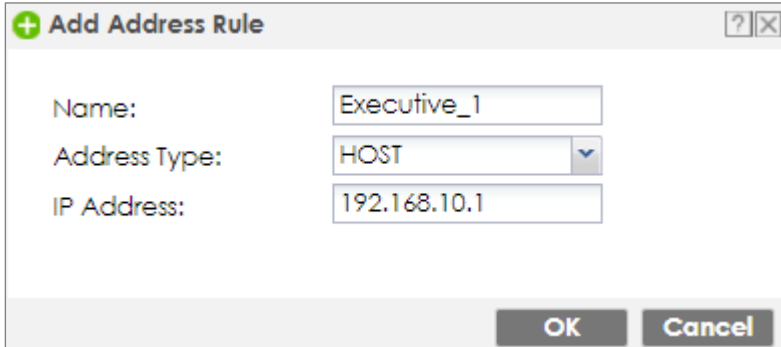
| | |
|--|--------------------|
| <input checked="" type="checkbox"/> Enable | |
| Name: | Employees Security |
| Description: | (Optional) |
| From: | LAN |
| To: | any (Excluding ZyV |
| Source: | Employees |
| Destination: | any |
| Service: | any |
| User: | any |
| Schedule: | none |
| Action: | allow |
| Log matched traffic: | log |

| UTM Profile | |
|---|----------------|
| <input checked="" type="checkbox"/> Content Filter: | Office profile |
| <input type="checkbox"/> SSL Inspection: | none |

Set Up the Security Policy on the ZyWALL/USG for Executives

In the ZyWALL/USG, go to **CONFIGURATION > Object > Address > Add Address Rule** to create address for each executives.

CONFIGURATION > Object > Address > Add Address Rule



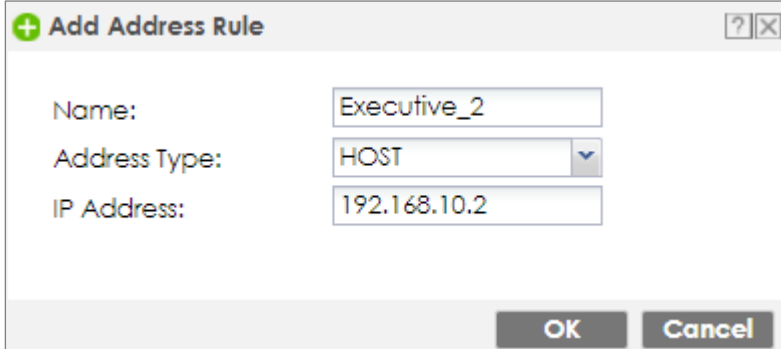
+ Add Address Rule [?] [X]

Name:

Address Type: ▼

IP Address:

OK Cancel



+ Add Address Rule [?] [X]

Name:

Address Type: ▼

IP Address:

OK Cancel



+ Add Address Rule [?] [X]

Name:

Address Type: ▼

IP Address:

OK Cancel

Then, go to **CONFIGURATION > Object > Address Group > Add Address Group Rule** to create a **Group Members' Name** and move the just created executives

address object to **Member**.

CONFIGURATION > Object > Address Group > Add Address Group Rule

Configuration

Name:

Description: (Optional)

Member List

| Available | | Member |
|----------------|---|--------|
| === Object === | | |
| ad-users | | |
| ldap-users | | |
| radius-users | | |
| Executive_1 | <input checked="" type="button" value="→"/> | |
| Executive_2 | <input type="button" value="←"/> | |
| Executive_3 | | |

Set up **Security Policy** for executives, go to **CONFIGURATION > Security Policy > Policy Control > Add corresponding**, configure a **Name** for you to identify the executives' **Security Policy** profile.

For **From** and **To** policies, select the direction of travel of packets to which the policy applies. Select **Source** to be the **Executives** to apply the policy to all traffic coming from them. In order to view the results later, to have the ZyWALL/USG generate **Log matched traffic (log)**.

Leave all UTM Profiles disabled.

CONFIGURATION > Security Policy > Policy Control > Add corresponding > Executives_Security

| | | |
|--|--------------------|------------|
| <input checked="" type="checkbox"/> Enable | | |
| Name: | Executive_Security | |
| Description: | | (Optional) |
| From: | LAN | |
| To: | any (Excluding ZyV | |
| Source: | any | |
| Destination: | any | |
| Service: | any | |
| User: | Executive | |
| Schedule: | none | |
| Action: | allow | |
| Log matched traffic: | log | |

Test the Result

Connect to the Internet from two computers: one from executive_2 address (192.168.10.2) and one from an employee address (192.168.20.1) and both access to <https://hangouts.google.com/>.

Go to the ZyWALL/USG **Monitor > Log**, you will see [notice] and [info] log message such as below. In this example result, connections from executive_2 address (192.168.10.2) use **Security Policy** priority: 1. Connections from employee address (192.168.20.1) use **Security Policy** priority: 2 and **UTM Profile** Rule_id=2.

| Priority | Category | Message | Source | Destination | Note |
|----------|-------------------------|--|--------------------|---------------------|----------------|
| notice | Security Policy Control | priority:1, from LAN to ANY, TCP, service others, ACCEPT | 192.168.10.2:52549 | 172.23.6.115:5088 | ACCESS FORWARD |
| notice | Security Policy Control | priority:1, from LAN to ANY, TCP, service others, ACCEPT | 192.168.10.2:54956 | 64.233.189.125:5222 | ACCESS FORWARD |

| Priority | Category | Message | Source | Destination | Note |
|----------|-------------------------|---|--------------------|---------------------|----------------|
| info | Application Patrol | Rule_id=2 SSI=N App=[Instant messaging]Google Talk:authority Action=reject SID=2305 | 192.168.20.1:53690 | 64.233.189.125:5222 | ACCESS BLOCK |
| notice | Security Policy Control | priority:2, from LAN to ANY, TCP, service others, ACCEPT | 192.168.20.1:53690 | 64.233.189.125:5222 | ACCESS FORWARD |
| info | Application Patrol | Rule_id=2 SSI=N App=[Social Network]Google-plus:authority Action=reject SID=402692097 | 192.168.20.1:53688 | 74.125.203.102:443 | ACCESS BLOCK |

What Could Go Wrong?

If you are not be able to configure any **UTM** policies or it's not working, there are two possible reasons:

You have not subscribed for the **UTM** service.

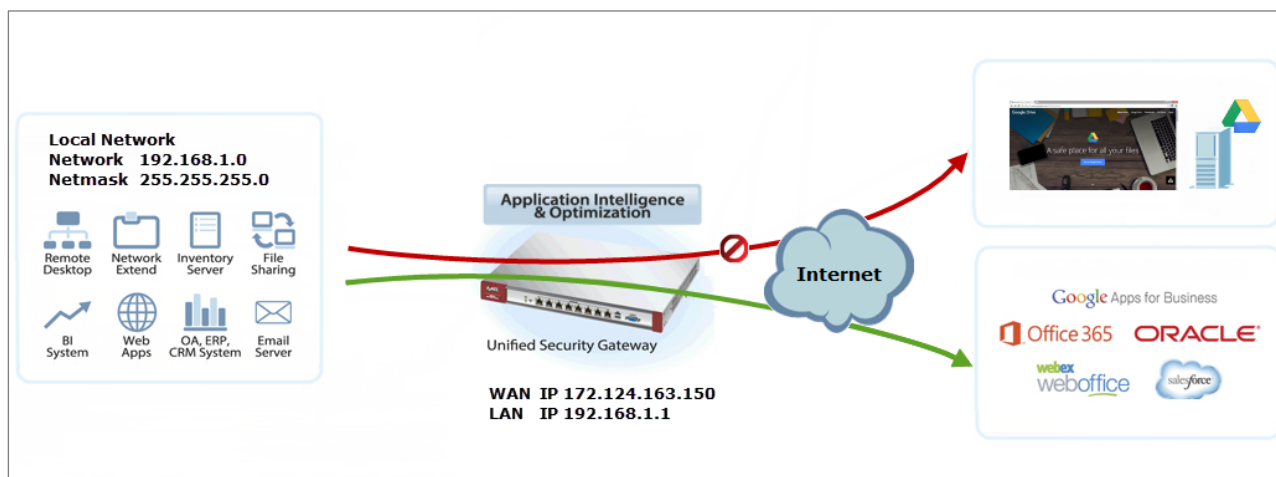
You have subscribed for the **UTM** service but the license is expired.


You can click the link from the **CONFIGURATION > Licensing > Registration** screen of your ZyXEL device's Web Configurator or click the myZyXEL.com 2.0 icon from the portal page (<https://portal.myzyxel.com/>) to register or extend your **UTM** license.

How To Control Access To Google Drive

This is an example of using a ZyWALL/USG UTM Profile in a Security Policy to block access to a specific file transfer service. You can use Application Patrol and Policy Control to make sure that a certain file transfer service cannot be accessed through both HTTP and HTTPS protocols.

ZyWALL/USG with Control Access To Google Drive Settings Example



 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the SSL Inspection on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > UTM Profile > SSL Inspection > Add rule**, configure a **Name** for you to identify the **SSL Inspection** profile.

Then, select the **CA Certificate** to be the certificate used in this profile. Select **Block** to **Action for Connection with SSL v3** and select **Log** type to be **log alert**. Leave other actions as default settings.

CONFIGURATION > UTM Profile > SSL Inspection > Add rule

| General Settings | | | |
|--|---------------------|------|-----------|
| Name: | Google Drive Contr. | | |
| Description: | | | |
| CA Certificate: | default | | |
| SSL/TLS version supported minimum: | ssl3 | Log: | log alert |
| Action for connection with unsupported suit: | pass | Log: | no |
| Action for connection with untrusted cert chain: | pass | Log: | log |

Set Up the Security Policy on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Security Policy > Policy Control**, configure a **Name** for you to identify the **Security Policy** profile. For **From** and **To** policies, select the direction of travel of packets to which the policy applies.

Scroll down to **UTM Profile**, select **Content Filter** and select a profile from the list box (Facebook_Block in this example). Then, select **SSL Inspection** and select a profile from the list box (Facebook_Block in this example).

CONFIGURATION > Security Policy > Policy Control

| | |
|--|--------------------|
| <input checked="" type="checkbox"/> Enable | |
| Name: | Google_Drive_Contr |
| Description: | (Optional) |
| From: | LAN |
| To: | any (Excluding ZyV |
| Source: | any |
| Destination: | any |
| Service: | any |
| User: | any |
| Schedule: | none |
| Action: | allow |
| Log matched traffic: | no |

| | |
|---|------------------|
| UTM Profile | |
| <input type="checkbox"/> Content Filter: | none |
| <input checked="" type="checkbox"/> SSL Inspection: | Google_Drive_Cor |


Export Certificate from ZyWALL/USG and Import it to Windows 7

Operation System

When SSL inspection is enabled and an access website does not trust the ZyWALL/USG certificate, the browser will display a warning page of security certificate problems.

Go to ZyWALL/USG **CONFIGURATION > Object > Certificate > default > Edit** to export default certificate from ZyWALL/USG with Private Key (zyx123 in this example).

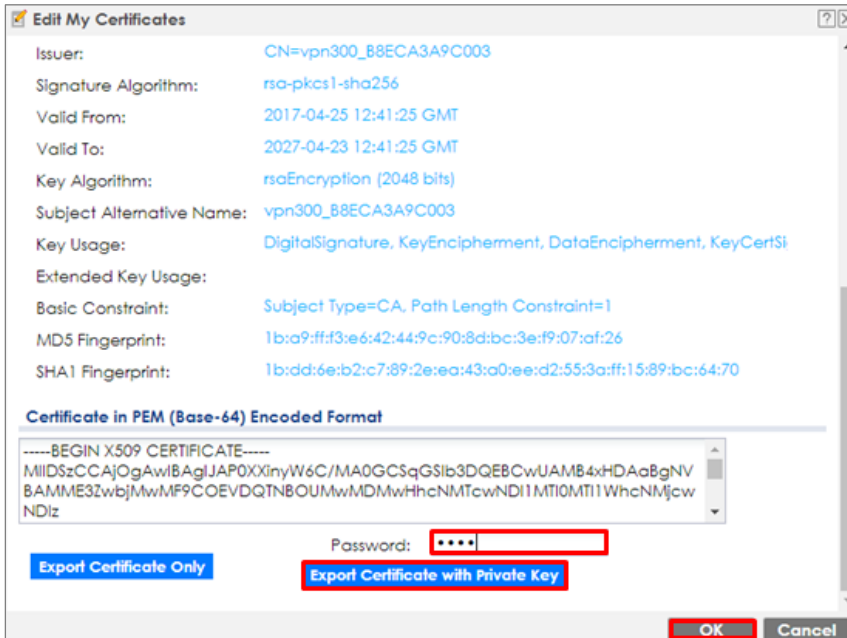
CONFIGURATION > Object > Certificate > default



| # | Name | Type | Subject | Issuer | Valid From | Valid To |
|---|---------|------|------------------------|------------------------|-------------------------|-------------------------|
| 1 | default | SELF | CN=vpn300_B8ECA3A9C... | CN=vpn300_B8ECA3A9C... | 2017-04-25 12:41:25 GMT | 2027-04-23 12:41:25 GMT |

Page 1 of 1 | Show 50 Items | Displaying 1 - 1 of 1

CONFIGURATION > Object > Certificate > default > Edit > Export Certificate with Private Key



Edit My Certificates

Issuer: CN=vpn300_B8ECA3A9C003

Signature Algorithm: rsa-pkcs1-sha256

Valid From: 2017-04-25 12:41:25 GMT

Valid To: 2027-04-23 12:41:25 GMT

Key Algorithm: rsaEncryption (2048 bits)

Subject Alternative Name: vpn300_B8ECA3A9C003

Key Usage: DigitalSignature, KeyEncipherment, DataEncipherment, KeyCertSi

Extended Key Usage:

Basic Constraint: Subject Type=CA, Path Length Constraint=1

MD5 Fingerprint: 1b:a9:ff:f3:e6:42:44:9c:90:8d:bc:3e:f9:07:af:26

SHA1 Fingerprint: 1b:dd:6e:b2:c7:89:2e:ea:43:a0:ee:d2:55:3a:ff:15:89:bc:64:70

Certificate in PEM (Base-64) Encoded Format

```
-----BEGIN X.509 CERTIFICATE-----
MIIDSzCCAJOgAwIBAgIJAP0XXinyW6C/MA0GCSqGSIb3DQEBCwUAMB4xHDAaBgNV
BAMME3ZwbjMwMF9COEVDQTNBOUMwMDMwHhcNMTCwNDI1MTI0MTI1WhcNMjcw
NDIz
```

Password: [Redacted]

Export Certificate Only **Export Certificate with Private Key**

OK **Cancel**

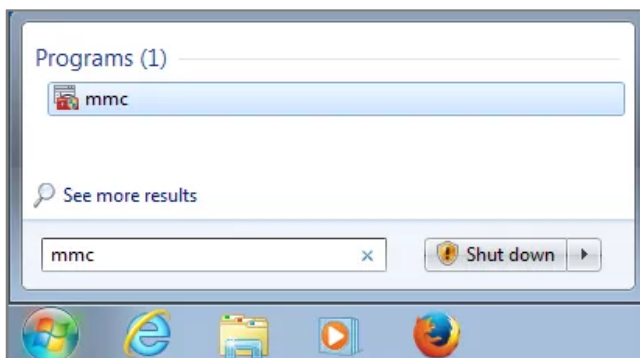
Save default certificate as *.p12 file to Windows 7 Operation System.



default.p12

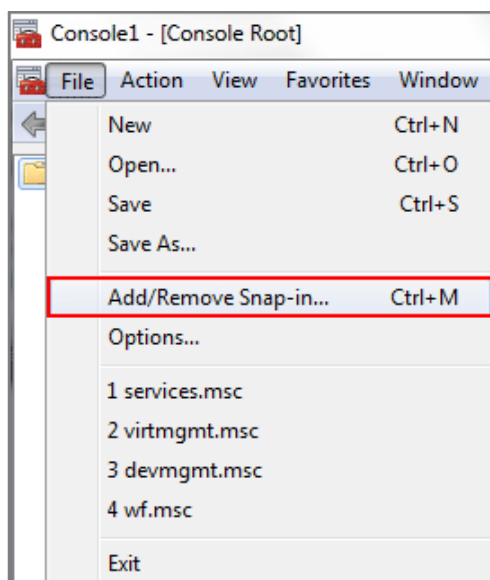
In Windows 7 Operating System **Start Menu > Search Box**, type **mmc** and press **Enter**.

Start Menu > Search Box > mmc



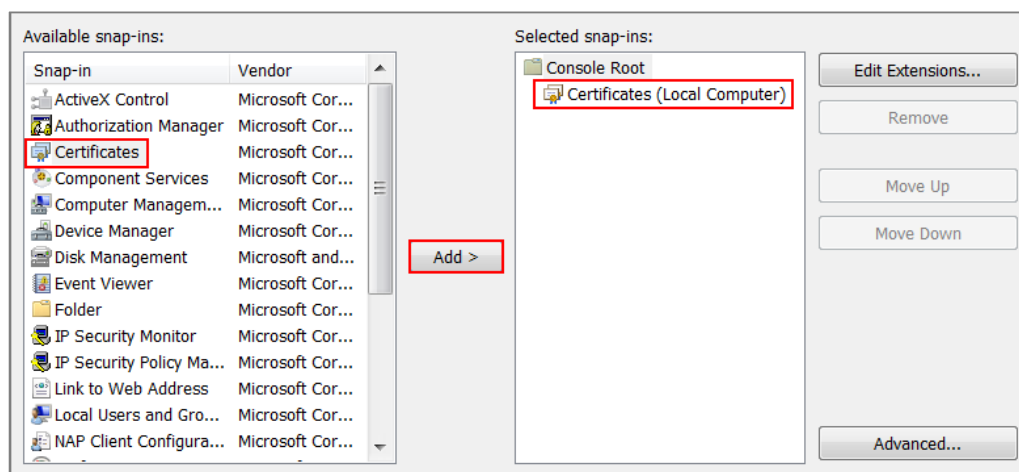
In the mmc console window, click **File > Add/Remove Snap-in...**

File > Add/Remove Snap-in...

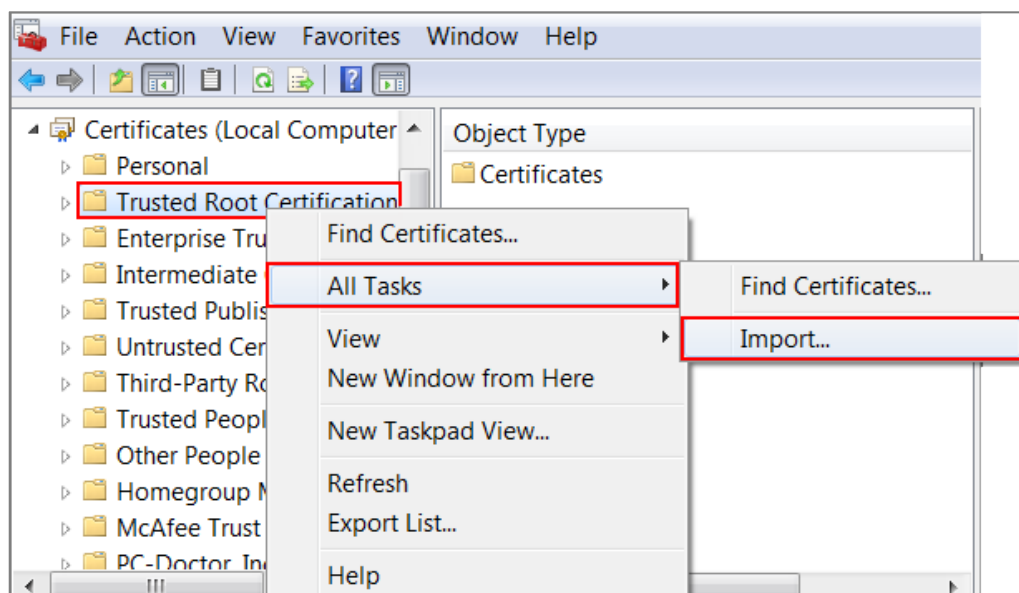


In the **Available snap-ins**, select the **Certificates** and click **Add** button. Select **Computer account > Local Computer**. Then, click **Finished** and **OK** to close the **Snap-ins** window.

Available snap-ins > Certificates > Add



In the mmc console window, open the **Certificates (Local Computer) > Trusted Root Certification Authorities**, right click **Certificate > All Tasks > Import...**



Click **Next**. Then, **Browse...**, and locate the .p12 file you downloaded earlier. Then, click **Next**.

File to Import

Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

- Personal Information Exchange- PKCS #12 (.PFX,.P12)
- Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
- Microsoft Serialized Certificate Store (.SST)

Click **Next**, type **zyx123** in the **Password** field and click **Next** again

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☐ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☒ Include all extended properties.

Select **Place all certificates in the following store** and then click **Browse** and find **Trusted Root Certification Authorities**. Click **Next**, then click **Finish**.

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.


☐ Automatically select the certificate store based on the type of certificate

☒ Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

Browse...

 Note: Each ZyWALL/USG device has its own self-signed certificate by factory default. When you reset to default configuration file, the original self-signed certificate is erased, and a new self-signed certificate will be created when the ZyWALL/USG boots the next time.

Test the Result

Type <http://drive.google.com/> or <https://drive.google.com/> into the browser, the error message occurs.

google.drive

502 Error

It appears the website you are trying to visit is having technical difficulties or is no longer available.

Please go back and try your request again or try searching Google to find another website with what you're looking for!

Go to the ZyWALL/USG **Monitor > Log**, you will see [alert] log message such as below.

Monitor > Log

| Priority | Category | Message | Note |
|----------|--------------------|---|--------------|
| alert | Application Patrol | Rule_id=1 SSI=Y App=[File Transfer]Google-drive:access Action=reject SID=50335494 | ACCESS BLOCK |
| alert | Application Patrol | Rule_id=1 SSI=Y App=[File Transfer]Google-drive:access Action=reject SID=50335494 | ACCESS BLOCK |

What Could Go Wrong?

If you are not be able to configure any **Application Patrol** policies or it's not working, there are two possible reasons:

You have not subscribed for the **Application Patrol** service.

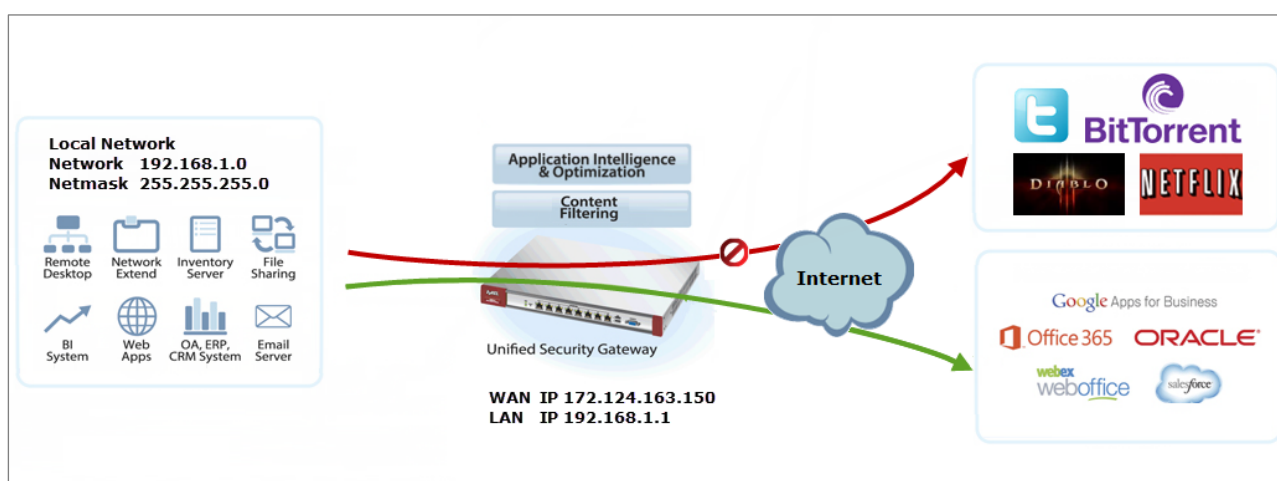
You have subscribed for the **Application Patrol** service but the license is expired.


You can click the link from the **CONFIGURATION > Licensing > Registration** screen of your ZyXEL device's Web Configurator or click the myZyXEL.com 2.0 icon from the portal page (<https://portal.myzyxel.com/>) to register or extend your **Application Patrol** license.

How To Block HTTPS Websites Using Content Filtering and SSL Inspection

This is an example of using a ZyWALL/USG Content Filtering, SSL Inspection and Security Policy to block access to malicious or not business-related websites.

ZyWALL/USG with Block HTTPS Websites Using Content Filtering and SSL Inspection Settings Example



 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the Content Filter on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > UTM Profile> Content Filter > Profile Management > Add Filter File > Category Service**. Configure a **Name** for you to identify the **Content Filter Profile** and select **Enable Custom Service**.

CONFIGURATION > UTM Profile> Content Filter > Profile > Profile Management > Add > Category Service > General Settings

General Settings

License Status: Licensed

License Type: Standard

Name: Office_Profile

Description: (Optional)

☐ Enable SafeSearch

☒ Enable Content Filter Category Service

☐ Log all web pages

Action for Unsafe Web Pages: Block ☐ Log

Action for Managed Web Pages: Block ☐ Log

Action for Unrated Web Pages: Warn ☐ Log

Action When Category Server Is Unavailable: Warn ☐ Log

Scroll down to the **Security Threat (unsafe)** section and select all categories of web pages that are known to pose a threat to your computers.

CONFIGURATION > UTM Profile> Content Filter > Profile > Profile Management > Add Filter File > Category Service > Security Threat (unsafe)

Security Threat (unsafe)

☒ Anonymizers ☒ Botnets ☒ Compromised

☒ Malware ☒ Network Errors ☒ Parked Domains

☒ Phishing & Fraud ☒ Spam Sites

Scroll down to the **Managed Categories** section and select the categories that are not business-related. Click **OK**.

CONFIGURATION > UTM Profile> Content Filter > Profile > Profile Management > Add Filter File > Category Service > Managed Categories

| Managed Categories | | |
|---|--|--|
| <input checked="" type="checkbox"/> Advertisements & Pop-Ups | <input checked="" type="checkbox"/> Alcohol/Tobacco | <input type="checkbox"/> Arts |
| <input type="checkbox"/> Business | <input type="checkbox"/> Transportation | <input type="checkbox"/> Chat |
| <input type="checkbox"/> Forums & Newsgroups | <input type="checkbox"/> Computers & Technology | <input checked="" type="checkbox"/> Criminal Activity |
| <input checked="" type="checkbox"/> Dating & Personals | <input type="checkbox"/> Download Sites | <input type="checkbox"/> Education |
| <input type="checkbox"/> Entertainment | <input type="checkbox"/> Finance | <input checked="" type="checkbox"/> Gambling |
| <input checked="" type="checkbox"/> Games | <input type="checkbox"/> Government | <input checked="" type="checkbox"/> Hate & Intolerance |
| <input type="checkbox"/> Health & Medicine | <input checked="" type="checkbox"/> Illegal Drugs | <input type="checkbox"/> Job Search |
| <input checked="" type="checkbox"/> Streaming Media & Downloads | <input type="checkbox"/> News | <input type="checkbox"/> Non-profits & NGOs |
| <input checked="" type="checkbox"/> Nudity | <input type="checkbox"/> Personal Sites | <input type="checkbox"/> Politics |
| <input checked="" type="checkbox"/> Pornography/Sexually Explicit | <input type="checkbox"/> Real Estate | <input type="checkbox"/> Religion |
| <input type="checkbox"/> Restaurants & Dining | <input type="checkbox"/> Search Engines/Portals | <input type="checkbox"/> Shopping |
| <input checked="" type="checkbox"/> Social Networking | <input type="checkbox"/> Sports | <input type="checkbox"/> Translators |
| <input type="checkbox"/> Travel | <input checked="" type="checkbox"/> Violence | <input checked="" type="checkbox"/> Weapons |
| <input type="checkbox"/> Web-based Email | <input type="checkbox"/> General | <input type="checkbox"/> Leisure & Recreation |
| <input checked="" type="checkbox"/> Cults | <input type="checkbox"/> Fashion & Beauty | <input type="checkbox"/> Greeting Cards |
| <input checked="" type="checkbox"/> Hacking | <input checked="" type="checkbox"/> Illegal Software | <input type="checkbox"/> Image Sharing |
| <input type="checkbox"/> Information Security | <input type="checkbox"/> Instant Messaging | <input checked="" type="checkbox"/> Peer to Peer |
| <input type="checkbox"/> Private IP Addresses | <input checked="" type="checkbox"/> School Cheating | <input checked="" type="checkbox"/> Sex Education |
| <input checked="" type="checkbox"/> Tasteless | <input checked="" type="checkbox"/> Child Abuse Images | |

If you are not sure which category a web page belongs to, you can enter a web site URL in the text box of **Test Web Site Category**.

CONFIGURATION > UTM Profile> Content Filter > Profile > Profile Management > Add Filter File > Category Service > Test Web Site Category

| Test Web Site Category | |
|--|--|
| URL to test: | <input type="text" value="https://www.youtube.com"/> |
| <input type="button" value="Test Against Content Filter Category Server"/> | |

Set Up SSL Inspection on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > UTM Profile > SSL Inspection > Add rule**, and configure a **Name** for you to identify the **SSL Inspection** profile.

Then, select the **CA Certificate** to be the certificate used in this profile. Select to **pass** or **block** SSLv2/unsupported suit/untrusted cert chain traffic that matches

traffic bound to this policy here.

Select desired **Log** type whether to have the ZyWALL/USG generate a log (log), log and alert (log alert) or neither (no) by default when traffic matches this policy.

CONFIGURATION > UTM Profile > SSL Inspection > Add rule

| General Settings | | | |
|--|---|------|----------------------------------|
| Name: | <input type="text" value="Office_Control"/> | | |
| Description: | <input type="text"/> | | |
| CA Certificate: | <input type="text" value="default"/> | | |
| SSL/TLS version supported minimum: | <input type="text" value="ssl3"/> | Log: | <input type="text" value="no"/> |
| Action for connection with unsupported suit: | <input type="text" value="pass"/> | Log: | <input type="text" value="no"/> |
| Action for connection with untrusted cert chain: | <input type="text" value="pass"/> | Log: | <input type="text" value="log"/> |

Set Up the Security Policy on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Security Policy > Policy Control**, configure a **Name** for you to identify the **Security Policy** profile. For **From** and **To** policies, select the direction of travel of packets to which the policy applies.

Scroll down to **UTM Profile**, select **Content Filter** and select a profile from the list box (Office_profile in this example). Then, select **SSL Inspection** and select a profile from the list box (Office_Control in this example).

CONFIGURATION > Security Policy > Policy Control

| | | |
|--|--------------------|------------|
| <input checked="" type="checkbox"/> Enable | | |
| Name: | Office_Control | |
| Description: | | (Optional) |
| From: | LAN | |
| To: | any (Excluding ZyV | |
| Source: | any | |
| Destination: | any | |
| Service: | any | |
| User: | any | |
| Schedule: | none | |
| Action: | allow | |
| Log matched traffic: | no | |

| UTM Profile | | |
|-------------------------------------|-----------------|----------------|
| <input checked="" type="checkbox"/> | Content Filter: | Office_profile |
| <input checked="" type="checkbox"/> | SSL Inspection: | Office_Control |

Export Certificate from ZyWALL/USG and Import it to Windows 7 Operation System

When SSL inspection is enabled and an access website does not trust the ZyWALL/USG certificate, the browser will display a warning page of security certificate problems.

Go to ZyWALL/USG **CONFIGURATION > Object > Certificate > default > Edit** to export default certificate from ZyWALL/USG with Private Key (zyx123 in this example).

CONFIGURATION > Object > Certificate > default

| My Certificates Setting | | | | | | | |
|---|---------|------|------------------------|------------------------|-------------------------|-------------------------|--|
| Add Edit Remove Object References | | | | | | | |
| # | Name | Type | Subject | Issuer | Valid From | Valid To | |
| 1 | default | SELF | CN=vpn300_B8ECA3A9C... | CN=vpn300_B8ECA3A9C... | 2017-04-25 12:41:25 GMT | 2027-04-23 12:41:25 GMT | |
| Page 1 of 1 Show 50 Items Displaying 1 - 1 of 1 | | | | | | | |

CONFIGURATION > Object > Certificate > default > Edit > Export Certificate with Private Key

Edit My Certificates

Issuer: CN=vpn300_B8ECA3A9C003
 Signature Algorithm: rsa-pkcs1-sha256
 Valid From: 2017-04-25 12:41:25 GMT
 Valid To: 2027-04-23 12:41:25 GMT
 Key Algorithm: rsaEncryption (2048 bits)
 Subject Alternative Name: vpn300_B8ECA3A9C003
 Key Usage: DigitalSignature, KeyEncipherment, DataEncipherment, KeyCertSi
 Extended Key Usage:
 Basic Constraint: Subject Type=CA, Path Length Constraint=1
 MD5 Fingerprint: 1b:a9:ff:f3:e6:42:44:9c:90:8d:bc:3e:f9:07:af:26
 SHA1 Fingerprint: 1b:dd:6e:b2:c7:89:2e:ea:43:a0:ee:d2:55:3a:ff:15:89:bc:64:70

Certificate in PEM (Base-64) Encoded Format


```
-----BEGIN X509 CERTIFICATE-----
MIIDSzCCAjOgAwIBAgIJAP0XXinyW6C/MA0GCSqGSIb3DQEBCwUAMB4xHDAaBgNV
BAUME3Zwbj/MwMF9COEVDQTNBOUMwMDMwHhcNMjcwNDI1MTI0MTI1WhcNMjcw
NDIz
```

Password:

Export Certificate Only
 Export Certificate with Private Key

OK Cancel

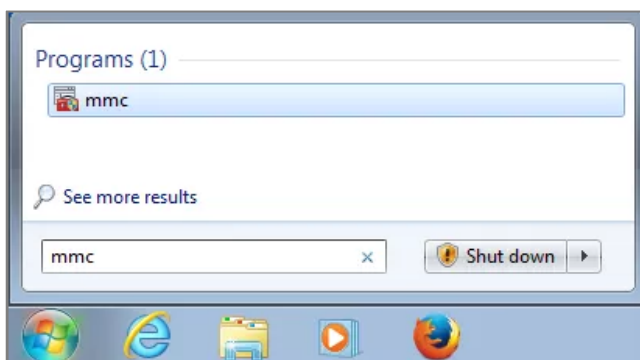
Save default certificate as *.p12 file to Windows 7 Operation System.



default.p12

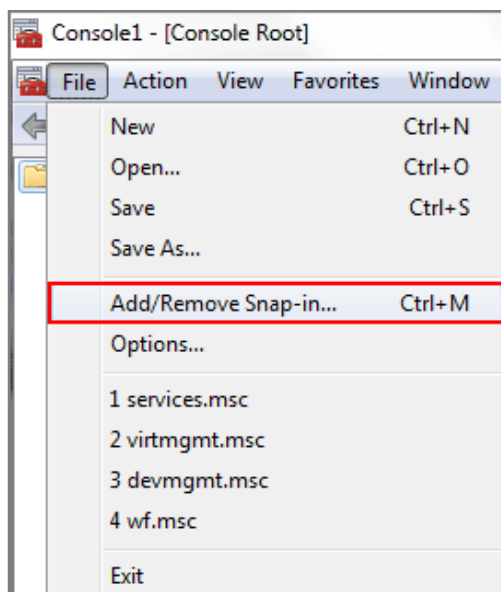
In Windows 7 Operating System **Start Menu > Search Box**, type **mmc** and press **Enter**.

Start Menu > Search Box > mmc



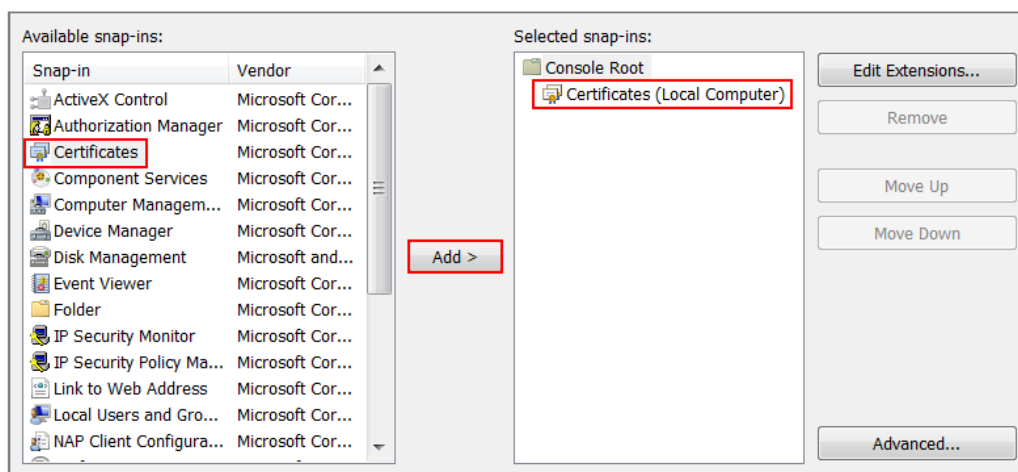
In the mmc console window, click **File > Add/Remove Snap-in...**

File > Add/Remove Snap-in...

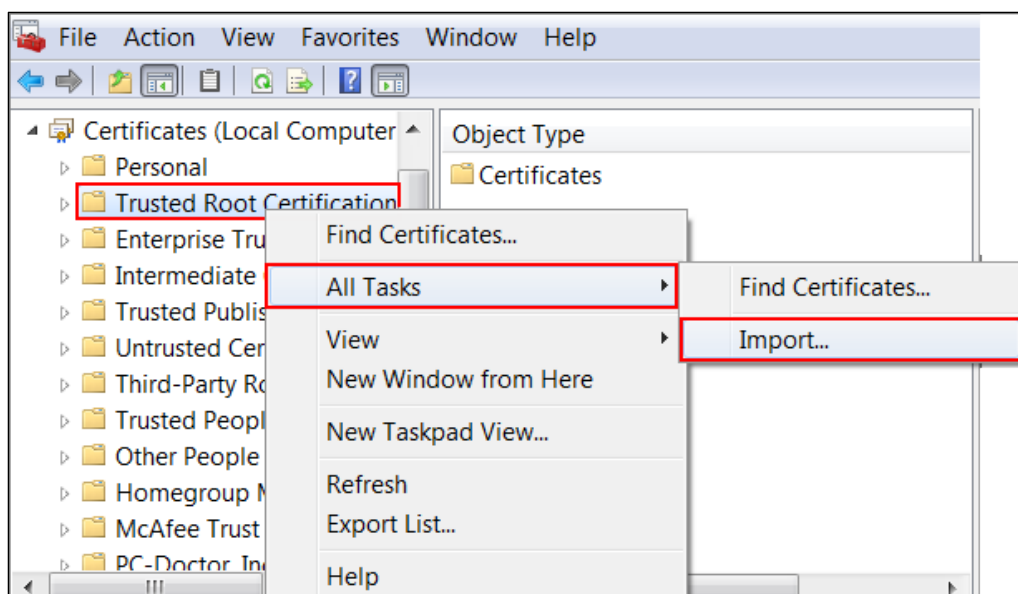


In the **Available snap-ins**, select the **Certificates** and click **Add** button. Select **Computer account > Local Computer**. Then, click **Finished** and **OK** to close the **Snap-ins** window.

Available snap-ins > Certificates > Add



In the mmc console window, open the **Certificates (Local Computer) > Trusted Root Certification Authorities**, right click **Certificate > All Tasks > Import...**



Click **Next**. Then, **Browse...**, and locate the .p12 file you downloaded earlier. Then, click **Next**.

File to Import
Specify the file you want to import.

File name:

C:\Users\Desktop\default.p12

Browse...

Note: More than one certificate can be stored in a single file in the following formats:

- Personal Information Exchange- PKCS #12 (.PFX,.P12)
- Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
- Microsoft Serialized Certificate Store (.SST)

Click **Next**, type **zyx123** in the **Password** field and click **Next** again

Password
To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

••••••

☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☐ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☒ Include all extended properties.

Select **Place all certificates in the following store** and then click **Browse** and find **Trusted Root Certification Authorities**. Click **Next**, then click **Finish**.

Certificate Store

Certificate stores are system areas where certificates are kept.


Windows can automatically select a certificate store, or you can specify a location for the certificate.

☐ Automatically select the certificate store based on the type of certificate

☒ Place all certificates in the following store

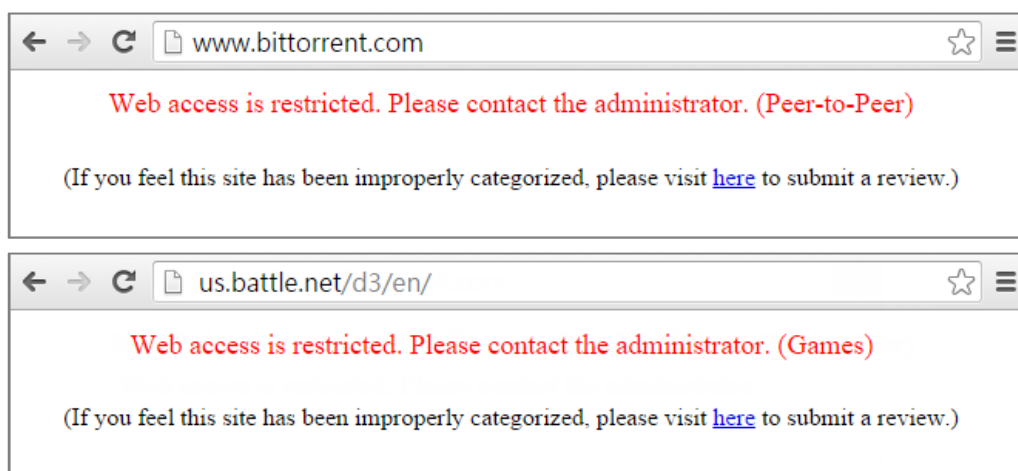
Certificate store:

Trusted Root Certification Authorities
Browse...

 **Note:** Each ZyWALL/USG device has its own self-signed certificate by factory default. When you reset to default configuration file, the original self-signed certificate is erased, and a new self-signed certificate will be created when the ZyWALL/USG boots the next time.

Test the Result

Type <http://www.bittorrent.com/> or <http://us.battle.net/d3/en/> into the browser.
The error message occurs.



Go to the ZyWALL/USG **Monitor > Log** to see [alert] log message such as below.

Monitor > Log

| Priority | Category | Message | Note |
|----------|-------------------|---|-----------|
| alert | Blocked web sites | www.bittorrent.com : Peer-to-Peer, Rule_id=1, SSI=N | WEB BLOCK |
| alert | Blocked web sites | us.battle.net : Games, Rule_id=1, SSI=N | WEB BLOCK |

What Could Go Wrong?

If you are not be able to configure any **Content Filter** policies or it's not working, there are two possible reasons:

You have not subscribed for the **Content Filter** service.

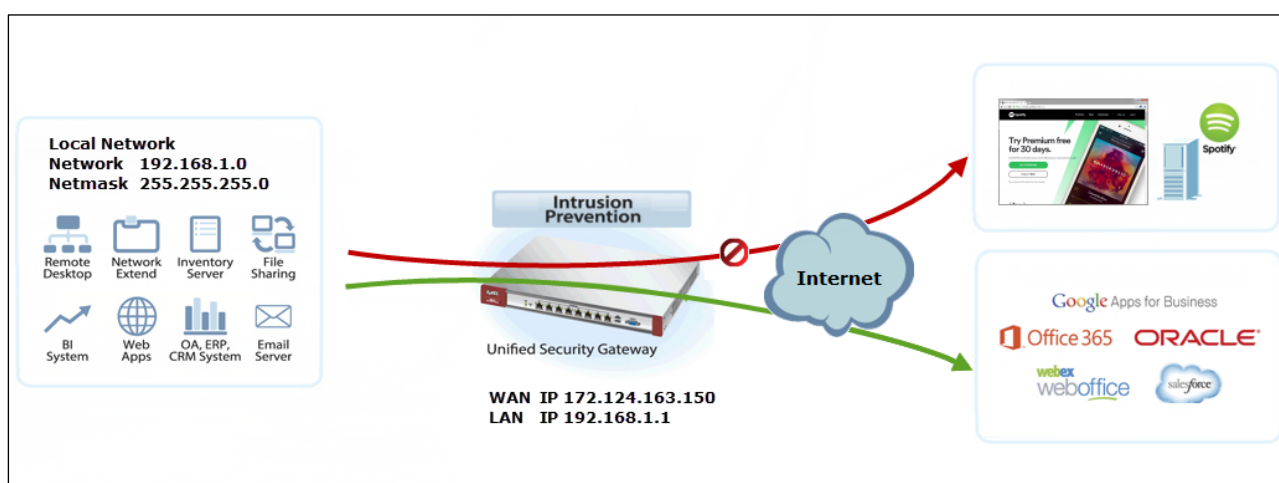
You have subscribed for the **Content Filter** service but the license is expired.


You can click the link from the **CONFIGURATION > Licensing > Registration** screen of your ZyXEL device's Web Configurator or click the myZyXEL.com 2.0 icon from the portal page (<https://portal.myzyxel.com/>) to register or extend your **Content Filter** license.

How To Block the Spotify Music Streaming Service

This is an example of using a ZyWALL/USG IDP Profile to block DNS query packet. When the Spotify software launches, it will send a DNS query for Spotify's public server. In this example, you can create a custom IDP to block DNS query packet if this packet includes the Spotify signature.

ZyWALL/USG with Block the Spotify Service Example



 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up IDP Profile on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > UTM Profile > IDP > Custom Signatures > Add Custom Signatures**, configure a **Name** for you to identify the IDP Profile. Select **medium** as the **Severity** level. Select all **Platform**. Select **Policy Type** to be **Access-Control** here to limit access network resources such as servers.

CONFIGURATION > Security Policy > IDP > Custom Signatures > Add Custom Signatures > Setup & Information

Setup

Name: Spotify

Signature ID: 9986234

Information

Severity: medium

Platform:

- ☒ Windows
- ☒ Linux
- ☒ FreeBSD
- ☒ Solaris
- ☒ Other-Unix
- ☒ Network-Device
- ☒ MAC
- ☒ iOS
- ☒ Android
- ☒ Windows-Mobile
- ☒ Symbian
- ☒ Others

Policy Type: Access-Control

Scroll down to the **Payload Options** section, the type Spotify's software signature: |73||70||6F||74||69||66||79| into the **Content** field. Click **OK**.

CONFIGURATION > Security Policy > IDP > Custom Signatures > Add Custom Signatures > Payload Options

Payload Options

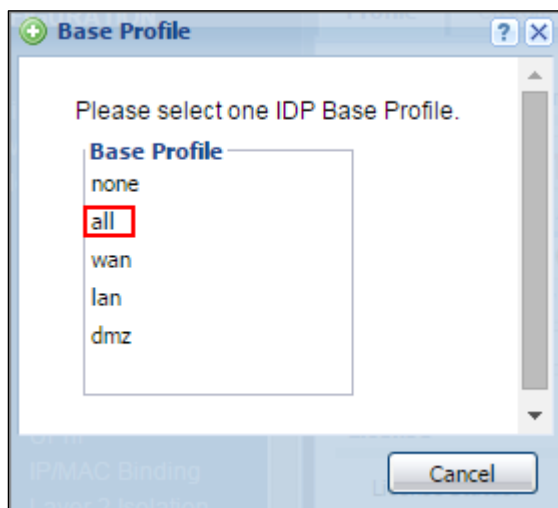
Payload Size: [] Bytes

Buttons: Add, Edit, Remove

| # | Offset | Content | Case-insensitive | Decode as URI |
|---|--------|----------------------------|------------------|---------------|
| 1 | 0 | 73 70 6F 74 69 66 79 | no | no |

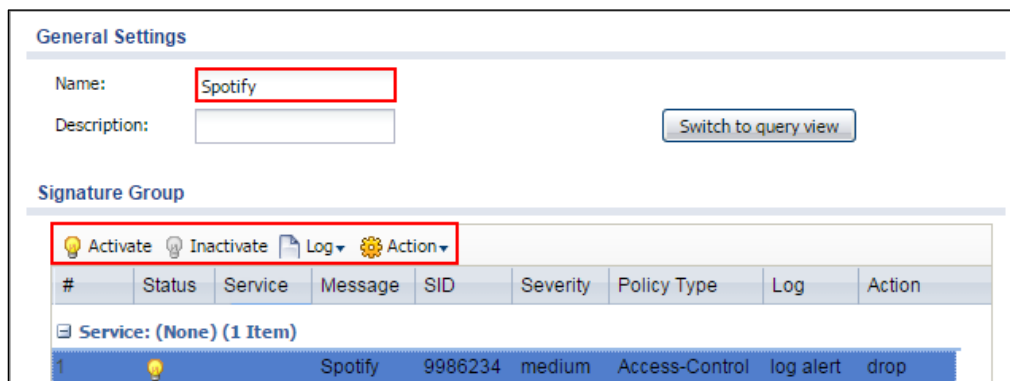
In the ZyWALL/USG, go to **CONFIGURATION > UTM Profile > IDP > Profile > Base Profile**. A pop-up screen will appear and select a **Base Profile** to go to the profile details screen.

CONFIGURATION > UTM Profile > IDP > Profile > Base Profile



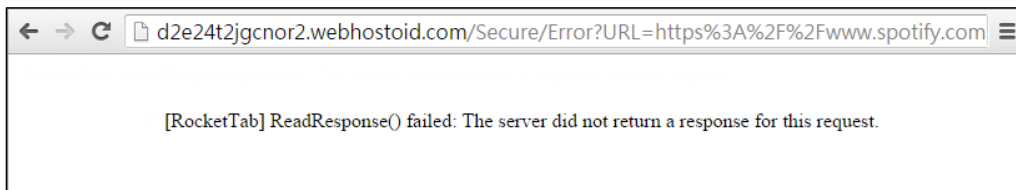
Configure a **Name** for you to identify the **IDP** Profile. **Activate** the newly created IDP Profile and select **Action** to be **drop**. Select **Log** type to be **log alert** in order to view the result later.

CONFIGURATION > UTM Profile > IDP > Profile > Base Profile > Add Profile



Test the Result

Type <http://www.spotify.com/> or <https://www.spotify.com/> into the browser, the error message occurs.



Go to the ZyWALL/USG **Monitor > Log**, you will see [crit] log message such as below.

Monitor > Log

| Priority | Category | Message | Note |
|----------|----------|---|--------------|
| crit | IDP | Rule_id=1 SSL=Y [type=custom-signature(9986234)] Spotify Action: Drop Packet Severity: medium | ACCESS BLOCK |

What Could Go Wrong?

If you are not be able to configure any **IDP** policies or it's not working, there are two possible reasons:

You have not subscribed for the **IDP** service.

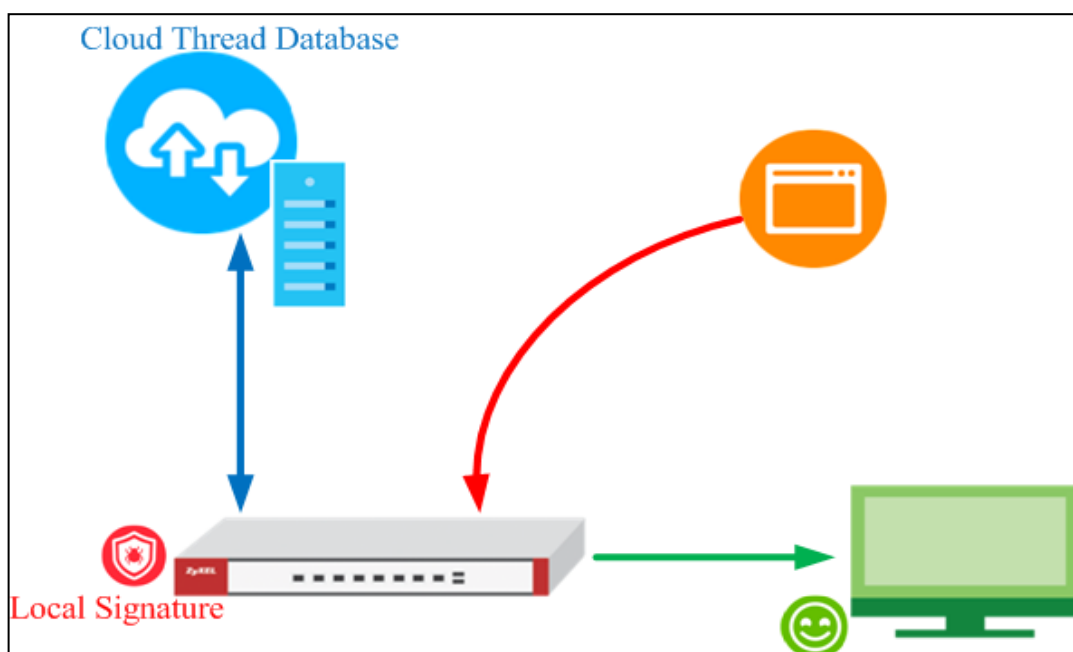
You have subscribed for the **IDP** service but the license is expired.

You can click the link from the **CONFIGURATION > Licensing > Registration** screen of your ZyXEL device's Web Configurator or click the myZyXEL.com 2.0 icon from the portal page (<https://portal.myzyxel.com/>) to register or extend your

Application Patrol license.

How does Anti-Malware work

There are many virus exist on the internet. And it may auto-downloaded on unexpected situation when you surfing between websites. The Anti-Malware is a good choose to protecting your computer to downloads unsafe application or files.



After you enabled Anti-Malware function, it will enabled “**Cloud Threat Database**” and “**Anti-Malware Signature**” in the same time.

The **Cloud Threat Database** is means your downloaded files will decompressed by device first, and then check files with cloud data base server if it exist unsafe file or not.

The **Anti-Malware Signature** is means your downloaded files will checked by local signatures that exist on device itself. It is helpful when your device unable access to internet at that moment.

 **Note:** In the default setting, the **Cloud Threat Database** is enabled and with higher priority when scanning the files.

Enable Anti-Malware function to protecting your traffic

Go to **CONFIGURATION > Security Service > Anti-Malware** > Tick in **enable** checkbox to enable Anti-Malware function.

Configuration > Security Service > Anti-Malware > Tick in **enable** checkbox

Anti-Malware **Signature**

General Settings

☒ Enable

☒ Scan and detect EICAR test virus

Actions When Matched

☒ Destroy infected file

Log:

☒ Check White List

+ Add Edit Remove Activate Inactivate

| Status | # | File Pattern |
|--------------------|---|--------------|
| No data to display | | |

☒ Check Black List

+ Add Edit Remove Activate Inactivate

| Status | # | File Pattern |
|--------------------|---|--------------|
| No data to display | | |

File decompression

☒ Enable file decompression (ZIP and RAR)

☐ Destroy compressed files that could not be decompressed

Signature Information

Anti-Malware

Current Version: 3.0.1.20180327.0

Signature Number: 404077

Released Date: 2018-03-27 01:32:19 (UTC+00:00)

Cloud Threat Database

Current Version: 1.0.0.20180226.0

Signature Number: 20001

Released Date: 2018-02-25 18:15:02 (UTC+00:00)

[Update Signatures](#)

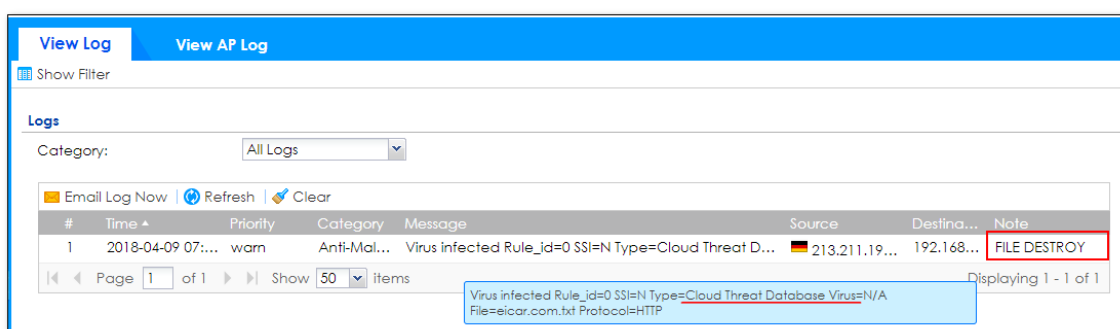
Apply **Reset**

Note: The Anti-Malware license is required. So you must enabled Anti-Malware function on your myzyxel.com account.

Test the result

After you enabled Anti-Malware function and your PC downloaded the virus file from internet. Your device will detect it and drop the file directly.

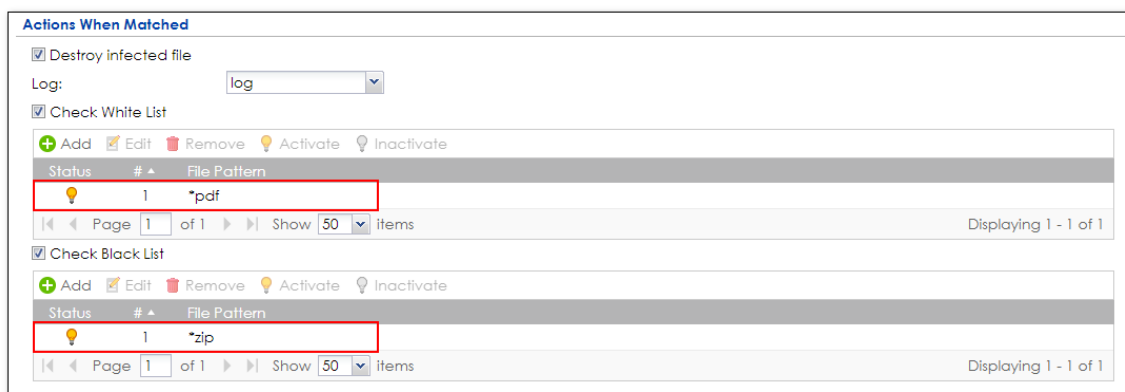
Then your file is unable opened or replaced by "0".



Additional configuration

White List: You can use wildcard to allowing specific type files.

Black List: You can use wildcard to drop specific type files.



Logs

Category:

Email Log Now Refresh Clear

| # | Time | Priority | Categ... | Message | Source | Destination | Note |
|---|--------------|----------|-----------|--|-------------|--------------|------|
| 2 | 2018-04-0... | info | Anti-M... | FTP, NWA1123-ACv2_5.20(ABEL.4)C0_2.pdf matched the <u>White-List *.pdf</u> | 66.85.12... | 192.168.1... | |
| 1 | 2018-04-0... | info | Anti-M... | HTTP, eicar_com.zip matched the <u>Black-List *.zip</u> | 213.211.... | 192.168.1... | |

Page 1 of 1 Show 50 items Displaying 1 - 2 of 2

What can go wrong

- 1 The Anti-Malware service license is required
- 2 The Anti-Malware is able decompress the file. But it is not support multi-layer zip files.
- 3 In the default setting, could thread databse is enabled. You can use the CLI command to activate/deactivate cloud base service. It means the scanning priority will be changed.
 - a. **Router(config)# debug anti-virus ctdb activate**
 - b. **Router(config)# debug anti-virus ctdb deactivate**


How to Configure an Email Security Policy with Mail Scan and DNSBL

This is an example of using ATP Series' UTM Profile to mark or discard spam (unsolicited commercial or junk e-mail). Use the Email Security white list to identify legitimate e-mail. Use the Email Security black list to identify spam e-mail. The ATP Series can also check e-mail against a DNS Black List (DNSBL) of IP addresses of servers that are suspected of being used by spammers.

ATP Series with Email Security Profile to mark or discard spam e-mail
Example



Figure 1 Using Email Security to Detect Spam

 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using ATP200 (Firmware Version: ZLD 4.32).

Set Up the Email Security on ATP Series

In the ATP Series, go to **CONFIGURATION > Security Service > Email Security**; Enable this feature on General Settings page. Select **Check IP Reputation (SMTP only)** to have the ATP Series scan for spam e-mail by IP Reputation. Select **Check Mail Content** to identify Spam Email by content, such as malicious content. Select **Check Virus Outbreak** to scan viruses attached in emails. On advance section, leave Query Timeout Settings to be the default settings.

Select from the list of available **Scan Options** and desired Log type whether to have the ATP Series generate a log (**log**), log and alert (**log alert**) or neither (**no**) by default when traffic matches this policy. Click **Apply** to save the configuration

CONFIGURATION > Security Service > Email Security

☒ Enable

☒ Check White List
☒ Check Black List
☒ Check IP Reputation (SMTP only)
☒ Check Mail Content
☒ Check Virus Outbreak
☒ Check Mail Phishing
☒ Check DNSBL

Black List Spam Tag: (Optional)
 Mail Content Spam Tag: (Optional)
 Virus Outbreak Tag: (Optional)
 Mail Phishing Tag: (Optional)
 DNSBL Spam Tag: (Optional)

DNSBL Domain List

+ Add Edit Remove Activate Inactivate

| Status | # | DNSBL Domain |
|---|---|--------------|
| << < Page 0 of 0 > > Show 50 items No data to display | | |

Action

Actions For Spam Mail ⓘ

SMTP:

POP3:

Log: ⓘ

Action taken when mail session threshold is reached

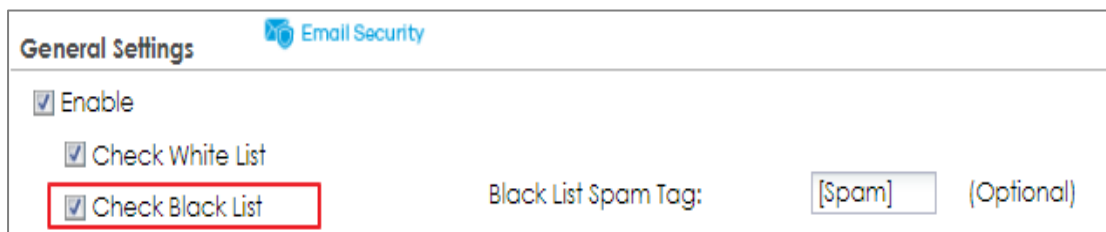
☒ Forward Session


1. Register the device to myZyxel.com.
2. Activate Application Security.

| # | Service | Status | Service Type | Expiration Date | Count | Action |
|---|--------------------------|-----------|--------------|-----------------|-------|-----------------------|
| 1 | Web Security | Activated | Standard | 2019-5-13 | N/A | Renew |
| 2 | Application Security | Activated | Standard | 2019-5-13 | N/A | Renew |
| 3 | Malware Blocker | Activated | Standard | 2019-5-13 | N/A | Renew |
| 4 | Intrusion Prevention | Activated | Standard | 2019-5-13 | N/A | Renew |
| 5 | Geo Enforcer | Activated | Standard | 2019-5-13 | N/A | Renew |
| 6 | Sandboxing | Activated | Standard | 2019-5-13 | N/A | Renew |
| 7 | SecuReporter | Activated | Standard | 2019-5-13 | N/A | Renew |
| 8 | Managed AP Service | Activated | Standard | 2019-5-13 | 8 | Renew |
| 9 | Firmware Upgrade Service | Activated | | | N/A | |

<< < Page 1 of 1 > > Show 50 items Displaying 1 - 9 of 9

3. Go to **CONFIGURATION > Security Service> Email Security>Enable Check Black List** to have the ATP Series treat e-mail that matches (an active) black list entry as spam.



General Settings  Email Security

☒ Enable

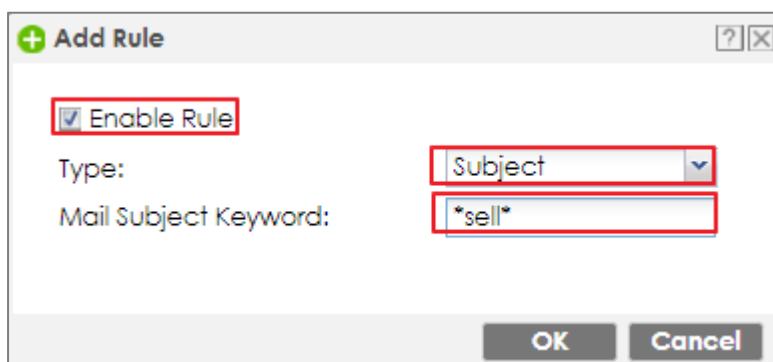
☒ Check White List



☒ Check Black List

Black List Spam Tag: (Optional)

4. Continue to **Rule Summary on Black/White List**, click the **Add** icon. A pop-up screen will appear allowing you to configure **Content (Subject, IP/IPv6 Address, E-Mail Address and Mail Header)**, Use wildcards (*) to configure **Mail Subject Keyword**. (*sell* in this example). Click **OK** to return to the **General** screen.

CONFIGURATION > Security Service> Black/White List



+ Add Rule  

☒ Enable Rule

Type:

Mail Subject Keyword:

OK **Cancel**

5. In the ATP Series, go to **CONFIGURATION > Security Service> Email Security>Enable Check DNSBL**

Press **Add** and enter the **DNSBL Domain** for a DNSBL service (zen.spamhaus.org in this example). Click **Apply**.

☒ Check DNSBL

DNSBL Spam Tag: (Optional)

DNSBL Domain List

[+ Add](#) [Edit](#) [Remove](#) [Activate](#) [Inactivate](#)

| Status | # | DNSBL Domain |
|--------|---|------------------|
| | | zen.spamhaus.org |

Page 0 of 0 Show 50 items No data to display

Test the result

1. Send the mail subject with "sell".

Send

From: zyxelsupport@zyxel.com.tw

To: zyxelsupport@zyxel.com.tw;

Cc:

Bcc:

Subject: Now on sell!!!

Anti-Spam test

2. You will receive the mail subject with [Spam] tag.

From: zyxelsupport <zyxelsupport@zyxel.com.tw>

To: zyxelsupport@zyxel.com.tw

Cc:

Subject: [Spam][Spam]Now on sell!!!

Anti-Spam test

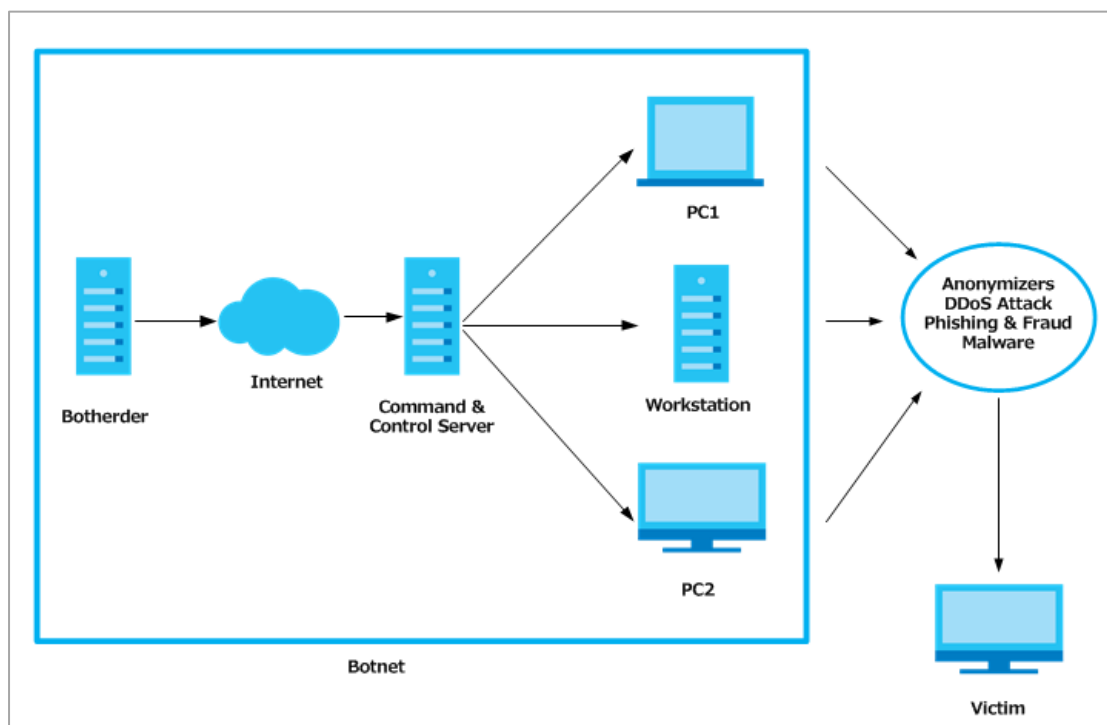
What can go wrong

1. If Email Security is not working, there are two possible reasons:
 - You have not subscribed for the **Email Security** service.
 - You have subscribed for the **Email Security** service but the license (**Application Security**) is expired.
2. You can click the link from the **CONFIGURATION > Licensing > Registration** screen of your ZyXEL device's Web Configurator or click the myZyXEL.com 2.0 icon from the portal page (<https://portal.myzyxel.com/>) to register or extend your **Application Security** license.

How to Configure Botnet Filter on ATP series?

Botnets are organized groups of infected computers. Those infected PCs will try to connect to the command-and-control server and ask for commands. When the attacker sends command to the command-and-control server, it will relay those commands to the clients (infected computers) and perform attacks on particular targets.

The following steps will walk you through an example of how to configure Botnet Filter (IP blocking and URL blocking) on the ATP.



Prerequisites before setting up Botnet Filter function

1. License status check
2. Update the Botnet Filter signature

License activation

Before setting up the Botnet Filter function, users need to make sure their licenses are purchased and activated.

To check the license activation status:

Go to configuration > Licensing > Registration > Service and check on the “Application Security” service which includes the Botnet Filtering function.

Registration

Service

Service Status

| # | Service | Status | Service Type | Expiration Date | Count | Action |
|---|--------------------------|-----------|--------------|-----------------|-------|-----------------------|
| 1 | Web Security | Activated | Standard | 2019-5-13 | N/A | Renew |
| 2 | Application Security | Activated | Standard | 2019-5-13 | N/A | Renew |
| 3 | Malware Blocker | Activated | Standard | 2019-5-13 | N/A | Renew |
| 4 | Intrusion Prevention | Activated | Standard | 2019-5-13 | N/A | Renew |
| 5 | Geo Enforcer | Activated | Standard | 2019-5-13 | N/A | Renew |
| 6 | Sandboxing | Activated | Standard | 2019-5-13 | N/A | Renew |
| 7 | SecuReporter | Activated | Standard | 2019-5-13 | N/A | Renew |
| 8 | Managed AP Service | Activated | Standard | 2019-5-13 | 8 | Renew |
| 9 | Firmware Upgrade Service | Activated | | | N/A | |

Page 1 of 1

Show 50 Items

Displaying 1 - 9 of 9


Update Botnet Filter Signatures









To make sure the device has the most updated signature, we suggest users to update their Botnet Filter signature before using this function.

To update the Botnet Filter signature:

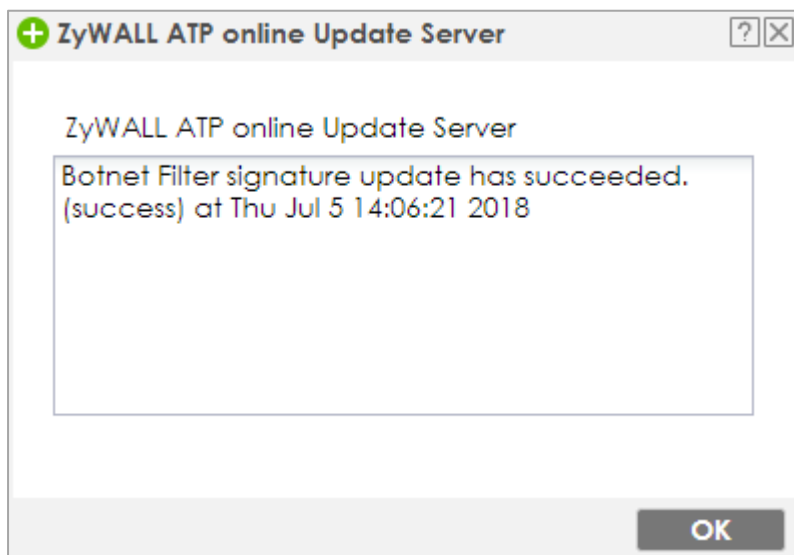
Go to **Configuration > Security Service > Botnet Filter**. Then click **“Update Signatures”**

| Signature Information | |
|-----------------------------------|---------------------|
| Current Version: | 1.0.1.20180703.0 |
| Signature Number: | 200000 |
| Released Date: | 2018-07-03 10:07:39 |
| Update Signatures | |

Then the device will redirect users to the “**Service Status**” page. Click on the cloud icon  and the device will start signature downloading process

| Signature | | | | | |
|----------------|------------------------|------------------|---------------------------------|---------------------|---|
| Service Status | | | | | |
| Feature | Type | Current Version | Released Date | Last Sync | Action |
| Anti-Malware | Anti-Malware Signature | 2.0.1.20180627.0 | 2018-06-27 09:31:58 (UTC+08:00) | 2018-07-04 23:55:01 |   |
| | Cloud Threat Databa... | 1.0.0.20180704.0 | 2018-07-04 02:15:03 (UTC+08:00) | | |
| App-Patrol | App-Patrol | 1.0.0.20180517.0 | 2018-05-17 09:45:17 (UTC+08:00) | 2018-06-20 04:52:18 |   |
| IDP | IDP | 4.0.1.20180626.0 | 2018-06-26 13:10:00 (UTC+08:00) | 2018-07-01 00:27:01 |   |
| Botnet Filter | Botnet Filter | 1.0.1.20180703.0 | 2018-07-03 10:07:39 (UTC+08:00) | 2018-07-05 02:59:01 |   |

Once the signature updating process was done. The GUI will pop up the following message to notify users.

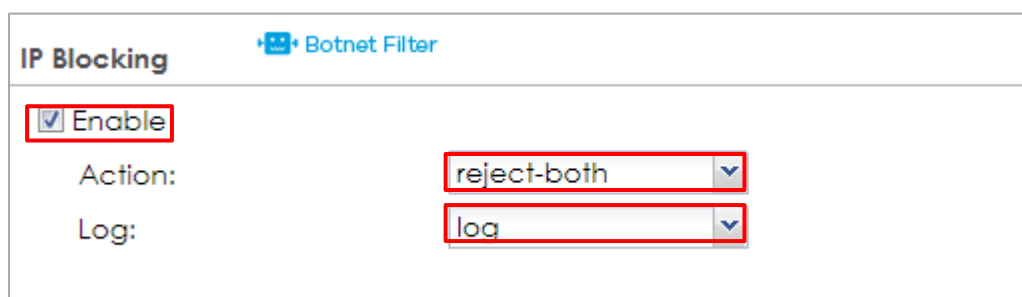


Now the Botnet Filtering function is ready to go.

Set Up the IP Blocking on the ATP series

Go to **Configuration > Security Service > Botnet Filter**.

Select the **Enable IP Blocking** check box. There're some actions can be selected "reject-both", user can decide if they'd like to "forward", "reject-sender" or "reject-receiver" the blocked IP . In addition, users can select if they want to log the related events or not.



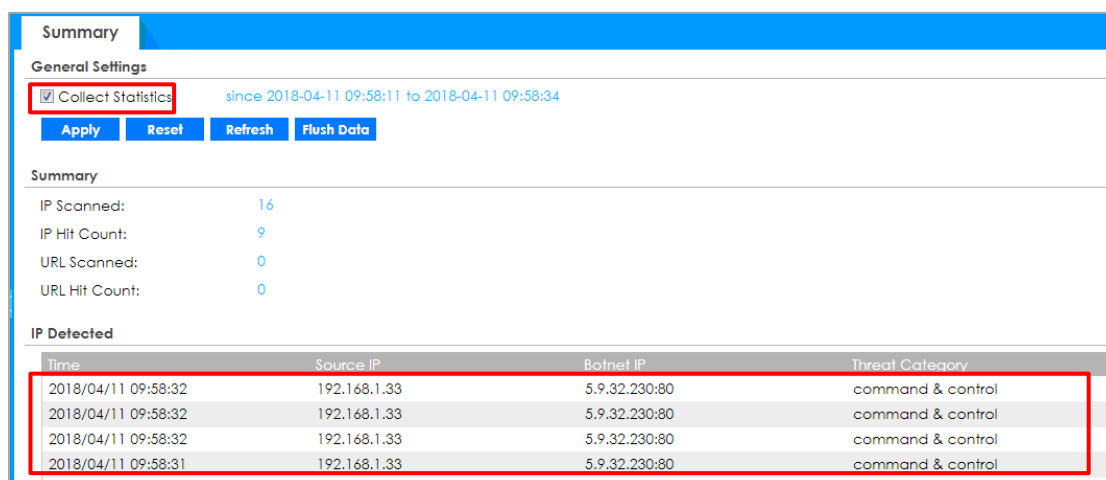
The screenshot shows the 'Botnet Filter' configuration page. Under the 'IP Blocking' section, the 'Enable' checkbox is checked. The 'Action' dropdown menu is set to 'reject-both', and the 'Log' dropdown menu is set to 'log'. Red boxes highlight the 'Enable' checkbox, the 'Action' dropdown, and the 'Log' dropdown.

Test the Result

User access IP: 5.9.32.230

Go to **Monitor > Security Statistics > Botnet Filter** to check summary.

IP: 5.9.32.230 is blocked due to command & control.



The screenshot shows the 'Summary' page of the Botnet Filter. The 'General Settings' section has the 'Collect Statistics' checkbox checked. The 'Summary' section shows statistics for IP Scanned (16), IP Hit Count (9), URL Scanned (0), and URL Hit Count (0). The 'IP Detected' section contains a table with the following data:

| Time | Source IP | Botnet IP | Threat Category |
|---------------------|--------------|---------------|-------------------|
| 2018/04/11 09:58:32 | 192.168.1.33 | 5.9.32.230:80 | command & control |
| 2018/04/11 09:58:32 | 192.168.1.33 | 5.9.32.230:80 | command & control |
| 2018/04/11 09:58:32 | 192.168.1.33 | 5.9.32.230:80 | command & control |
| 2018/04/11 09:58:31 | 192.168.1.33 | 5.9.32.230:80 | command & control |

Red boxes highlight the 'Collect Statistics' checkbox and the 'IP Detected' table.

Set up the URL Blocking on the ATP series

Go to **Configuration > Security Service > Botnet Filter**.

Select the **Enable URL Blocking** check box, check the categories that need to be blocked. Users can only check those categories as their requirement. Choose the Action the device will take (In this example we select "block" to block certain URLs) and if they want to Log those events on the device.

URL Blocking

☒ Enable

☒ Anonymizers
 ☒ Botnet C&C
 ☒ Compromised

☒ Malware
 ☒ Phishing & Fraud
 ☒ Spam Sites

Action:

Log:

Message to display when a site is blocked

Denied Access Message:

Redirect URL:

Test the Result

Browse the Phishing website URL from the host browser. Users will be redirected to an error page in the browser that notifies users they are visiting to the "Phishing & Fraud" categorized URL

← → ↻ 🏠 ⓘ websectest.ctmail.com/31_Phishing_and_Fraud.htm

Web access is restricted. Please contact the administrator. (Phishing & Fraud)

(If you feel this site has been improperly categorized, please visit [here](#) to submit a review.)

Go to **Monitor > Security Statistics > Botnet Filter** to check summary where users will see the related threat log was recorded

Summary

General Settings

☒ Collect Statistics since 2018-04-11 10:03:39 to 2018-04-11 10:08:04

Apply
 Reset
 Refresh
 Flush Data

Summary

IP Scanned: 0

IP Hit Count: 0

URL Scanned: 80

URL Hit Count: 2

IP Detected

| Time | Source IP | Botnet IP | Threat Category |
|--|-----------|-----------|-----------------|
| <div> <div> <div> <div>◀</div> <div>◀</div> <div>Page 0 of 0</div> <div>▶</div> <div>▶</div> </div> <div>Show 50 items</div> <div>No data to display</div> </div> </div> | | | |

URL Detected

| Time | Source IP | Botnet URL | Threat Category |
|----------------------|--------------|------------------------------------|------------------|
| Apr 11 10:03:52 2018 | 192.168.1.33 | websectest.ctmail.com/31_Phishi... | Phishing & Fraud |
| Apr 11 10:03:43 2018 | 192.168.1.33 | websectest.ctmail.com/42_Malw... | Malware |

◀

◀

Page 1 of 1

▶

▶

Show 50 items

Displaying 1 - 2 of 2

598/774

How to Use Sandboxing to Detect Unknown Malware

The traditional security service such as Anti-Virus and IDP are signature-based solution, so they have no chance to detect unknown threats. ZyWALL ATP enhances UTM service and integrates Sandbox solution as a second layer of defense to detect and mitigate advanced threats. Zyxel Sandbox is a cloud-based service that can identify previously unknown malware. Each new threat discovered by Sandbox will be converted to known signatures in the cloud threat database of Anti-Malware. The Anti-Malware examines file for threats before deciding to block or pass to Sandbox. If the file has never been inspected by Sandbox, ZyWALL ATP copies this file to the caches and then forwards the file. A copy of the file is sent to Sandbox for analysis and the analysis result is recorded on device's local cache. Once ZyWALL ATP detects the file again, it can identify the file and take the action based on the previous analysis result on local cache. With the cooperation of Anti-Malware, ATP can immediately block threat which previous detected by Sandbox. This example illustrates how to configure Sandboxing on ATP gateway to detect unknown malware.

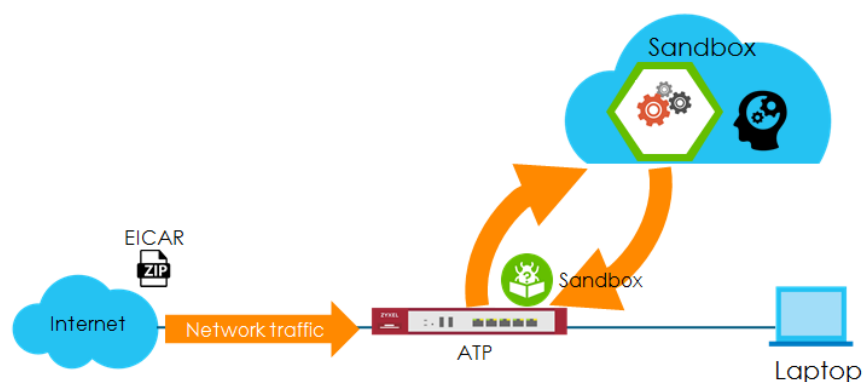



Figure 1 Using Sandboxing to Detect Unknown Malware

 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses. This example was tested using the ATP200 (Firmware Version: ZLD 4.32).

Set Up Sandboxing on ATP

1. Register the device to myZyxel.com.
2. Activate Sandboxing license.

| Service Status | | | | | | |
|---|--------------------------|-----------|--------------|-----------------|-------|-----------------------|
| # | Service | Status | Service Type | Expiration Date | Count | Action |
| 1 | Web Security | Activated | Standard | 2019-4-28 | N/A | Renew |
| 2 | Application Security | Activated | Standard | 2019-4-28 | N/A | Renew |
| 3 | Malware Blocker | Activated | Standard | 2019-4-28 | N/A | Renew |
| 4 | Intrusion Prevention | Activated | Standard | 2019-4-28 | N/A | Renew |
| 5 | Geo Enforcer | Activated | Standard | 2019-4-28 | N/A | Renew |
| 6 | Sandboxing | Activated | Standard | 2019-4-28 | N/A | Renew |
| 7 | SecuReporter | Activated | Standard | 2019-4-28 | N/A | Renew |
| 8 | Managed AP Service | Activated | Standard | 2019-4-28 | 18 | Renew |
| 9 | Firmware Upgrade Service | Activated | | | N/A | |
| Page 1 of 1 Show 50 Items Displaying 1 - 9 of 9 | | | | | | |

3. In the ATP, go to **CONFIGURATION > Security Service > Sandboxing > File Submission Options**, the default supported file types are listed.

File Submission Options

- ☒ Archives(.zip)
- ☒ Executables
- ☒ MS Office Documents
- ☒ Macromedia Flash Data
- ☒ PDF
- ☒ RTF

Use the command to check the status of each file type. If the status is "no", the file type is not scanned by Sandboxing.

Router> show sandbox file-type all

```
Router> show sandbox file-type all
```

| No. | Show_name | Name | Status |
|-----|-----------------------|-----------------------|--------|
| 1 | Archives(.zip) | archives | yes |
| 2 | CHM | chm | no |
| 3 | EICAR | eicar | no |
| 4 | Executables | executables | yes |
| 5 | Macromedia Flash Data | macromedia-flash-data | yes |
| 6 | MS Office Documents | ms-office-document | yes |
| 7 | PDF | pdf | yes |
| 8 | RTF | rtf | yes |
| 9 | Unknow Type | unknow-type | no |

Use the following commands to make Sandboxing access and check a certain file type.

Router> configure terminal

Router(config)# sandbox file-type eicar

Router(config)# write

```
Router> configure terminal
Router(config)# sandbox file-type eicar
Router(config)# write
Router(config)# show sandbox file-type all
```

| No. | Show_name | Name | Status |
|-----|-----------------------|-----------------------|--------|
| 1 | Archives(.zip) | archives | yes |
| 2 | CHM | chm | no |
| 3 | EICAR | eicar | yes |
| 4 | Executables | executables | yes |
| 5 | Macromedia Flash Data | macromedia-flash-data | yes |
| 6 | MS Office Documents | ms-office-document | yes |
| 7 | PDF | pdf | yes |
| 8 | RTF | rtf | yes |
| 9 | Unknow Type | unknow-type | no |

- Go to **CONFIGURATION > Security Service > Sandboxing > General**, enable Sandboxing and select action and log for malicious and suspicious files to monitor the result.

General

☒ Enable Sandboxing

Action For Malicious File: destroy

Log For Malicious File: log alert

Action For Suspicious File: destroy

Log For Suspicious File: log alert

5. Enable Collect Statistics to monitor the scan results and statistics.

MONITOR > Security Statistics > Sandboxing

General Settings

☒ Collect Statistics since 2018-07-03 10:41:08 to 2018-07-03 10:41:08

Apply Reset Refresh Flush Data

Submission Summary

| | |
|------------------|---|
| Total: | 0 |
| Scanning: | 0 |
| Scanned: | 0 |
| Destroyed Files: | 0 |

Scan Result

| | |
|-------------------|---|
| Malicious Files: | 0 |
| Suspicious Files: | 0 |
| Safe Files: | 0 |
| Other: | 0 |

Statistics

| # | File Name | Hash | Type | Occurrence | Update Time |
|--|-----------|------|------|------------|-------------|
| <div> Page 0 of 0 Show 50 items </div> | | | | | |
| No data to display | | | | | |

Test the Result


- 4 Go to <http://www.eicar.org/85-0-Download.html> to download eicar_com.zip file.

www.eicar.org/85-0-Download.html

**BE UP TO DATE
RSS FEED**

Order eicar news and events as rss feed.

[EICAR News](#) [EICAR Events](#)



caused by the scanner which puts the file into quarantine. The test file will be treated just like any other real virus infected file. Read the user's manual of your AV scanner what to do or contact the vendor/manufacturer of your AV scanner.

IMPORTANT NOTE

EICAR cannot be held responsible when these files or your AV scanner in combination with these files cause any damage to your computer. **YOU DOWNLOAD THESE FILES AT YOUR OWN RISK.** Download these files only if you are sufficiently secure in the usage of your AV scanner. EICAR cannot and will not provide any help to remove these files from your computer. Please contact the manufacturer/vendor of your AV scanner to seek such help.

Download area using the standard protocol http

| | | | |
|---------------------------------------|---|--|--|
| eicar.com 68 Bytes | eicar.com.txt 68 Bytes | eicar_com.zip 184 Bytes | eicarcom2.zip 308 Bytes |
|---------------------------------------|---|--|--|

Download area using the secure, SSL enabled protocol https

| | | | |
|---------------------------------------|---|--|--|
| eicar.com 68 Bytes | eicar.com.txt 68 Bytes | eicar_com.zip 184 Bytes | eicarcom2.zip 308 Bytes |
|---------------------------------------|---|--|--|

- When you download eicar_com.zip for the first time, it is considered to be an unknown malware. The file is allowed to pass and a copy of eicar_com.zip will be sent to Sandbox for further scan.

MONITOR > Log > View Log > Sandboxing

View Log

View AP Log

Show Filter

Logs

Category: Sandbox

Email Log Now | Refresh | Clear

| # | Time | Priority | Category | Message | Source | Destination | Note |
|-----|-------------|----------|----------|--|-------------------|----------------|------|
| 1 | 2018-04-... | alert | Sandbox | Malicious File name: eicar_com.zip, md5: 6ce6f4... | 192.168.1.33:1... | 213.211.198... | |
| 2 | 2018-04-... | info | Sandbox | Query File name: eicar_com.zip, md5: 6ce6f415... | 192.168.1.33:1... | 213.211.198... | |
| 134 | 2018-04-... | info | Sandbox | sandbox daemon Start OK... | | | |
| 135 | 2018-04-... | info | Sandbox | dc connector Start OK | | | |

Page 1 of 1 | Show 50 items | Displaying 1 - 4 of 4

The eicar_com.zip file is detected by Sandbox as a malicious file.

MONITOR > Security Statistics > Sandboxing

Summary

General Settings

☒ Collect Statistics

since 2018-04-27 16:55:12 to 2018-04-27 17:04:09

Apply

Reset

Refresh

Flush Data

Submission Summary

Total:

1

Scanning:

0

Scanned:

1

Destroyed File:

0

Scan Result

Malicious File:

1

Suspicious File:

0

Clean File:

0

Other:

0

Statistics

| # | File Name | Hash | Type | Occurence | Update Time |
|---|---------------|----------------------------------|-----------|-----------|---------------------|
| 1 | eicar_com.zip | 6ce6f415d8475545be5ba114f208b0ff | Malicious | 1 | 2018-04-27 17:03:18 |



Note: Disable anti-virus software on your laptop in order to test Sandbox.

- Download eicar_com.zip file again. ZyWALL ATP destroyed the eicar_com.zip file at the second time when you download the file and generate the log.

MONITOR > Log > View Log > Sandboxing

| View Log | | | | | | | |
|--|---------------------|----------|----------|--|-------------------|-------------------|--------------|
| View AP Log | | | | | | | |
| Show Filter | | | | | | | |
| Logs | | | | | | | |
| Category: <input type="text" value="Sandbox"/> | | | | | | | |
| <input type="button" value="Email Log Now"/> <input type="button" value="Refresh"/> <input type="button" value="Clear"/> | | | | | | | |
| # | Time | Priority | Category | Message | Source | Destination | Note |
| 1 | 2018-04-27 17:03:18 | crit | Sandbox | Malicious infected SSL=File=eicar_com.zip, md5: 6ce6f415d8475545be5ba114f208b0ff | 213.211.198.198 | 192.168.1.33:1853 | FILE DESTROY |
| 4 | 2018-04-27 17:03:18 | alert | Sandbox | Malicious File name: eicar_com.zip, md5: 6ce6f415d8475545be5ba114f208b0ff | 192.168.1.33:1845 | 213.211.198.198 | |
| 5 | 2018-04-27 17:03:18 | info | Sandbox | Query File name: eicar_com.zip, md5: 6ce6f415d8475545be5ba114f208b0ff | 192.168.1.33:1845 | 213.211.198.198 | |
| 137 | 2018-04-27 17:03:18 | info | Sandbox | sandbox daemon Start OK... | | | |
| 138 | 2018-04-27 17:03:18 | info | Sandbox | dc connector Start OK | | | |
| Page 1 of 1 Show 50 items | | | | | | | |
| Displaying 1 - 5 of 5 | | | | | | | |

MONITOR > Security Statistics > Sandboxing

Summary

General Settings

☒ Collect Statistics

since 2018-04-27 16:55:11 to 2018-04-27 17:11:14

Apply

Reset

Refresh

Flush Data

Submission Summary

Total:

2

Scanning:

0

Scanned:

2

Destroyed File:

1

Scan Result

Malicious File:

2

Suspicious File:

0

Clean File:

0

Other:

0

Statistics

| # | File Name | Hash | Type | Occurrence | Update Time |
|---|---------------|----------------------------------|-----------|------------|---------------------|
| 1 | eicar_com.zip | 6ce6f415d8475545be5ba114f208b0ff | Malicious | 2 | 2018-04-27 17:08:26 |

◀

◀ Page 1 of 1 ▶▶

Show 50 Items

Displaying 1 - 1 of 1

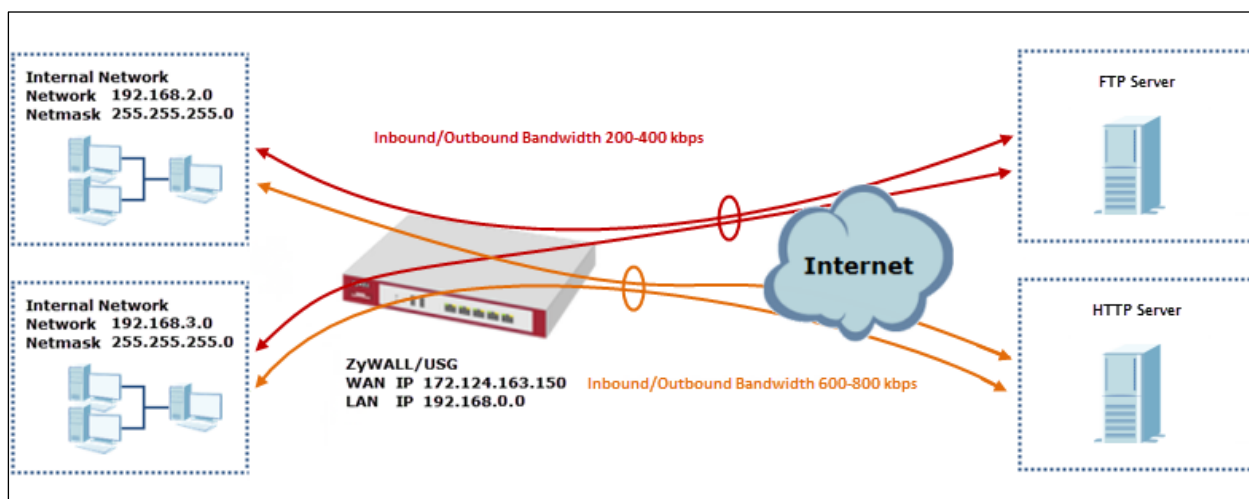
What Can Go Wrong?


- 7 SSL inspection needs to be enabled and applied to the corresponding security policy rule for HTTPS traffic.
- 8 Only Windows (Win XP, Win 7, Win 10) and Mac OSX operating system are supported.
- 9 The local cache of the analysis result will be deleted when the device reboots.

How to Configure Bandwidth Management for FTP and HTTP Traffic

This is an example of using ZyWALL/USG Bandwidth Management (BWM) to control the bandwidth allocation for FTP and HTTP traffic. You can use source interface, destination interface, destination port, schedule, user, source, destination information, DSCP code and service type as criteria to create a sequence of specific conditions to allocate bandwidth for the matching packets. When the BWM is configured, you can limit bandwidth consuming services, such as FTP, while providing consistent HTTP service with bandwidth guarantees.

ZyWALL/USG with Bandwidth Management for HTTP and FTP Traffic Example



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. The total available bandwidth assumption is 1,600 kbps. This example was tested using USG310

Set Up the Bandwidth Management for FTP on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > BWM > Configuration > Add Policy**, select **Enable** and type **FTP Any-to-WAN** as the policy's **Description**.

Leave the **Incoming Interface** to **any** and select the Outgoing Interface to be **wan1**. Select **Service Type** to be the **Service Object** and select **FTP** from the list box.

Set the **Guaranteed Bandwidth Inbound** to 200 (kbps) and set **Priority 5** (low-to-medium). Set the **Maximum** to 400 (kbps). Set the **Guaranteed Bandwidth Outbound** to 200 (kbps) and set **Priority 5**. Set the **Maximum** to 400 (kbps).

In order to view the result later, set the **Log** setting to be **log alert**. Click **OK** to return to the **General** screen.

CONFIGURATION > BWM > Configuration > Add Policy

Configuration

☒ Enable
 Description: FTP Any-to-WAN (Optional)
 BWM Type: ☒ Shared ☐ Per user ☐ Per-Source-IP

Criteria

User: any
 Schedule: none
 Incoming Interface: any
 Outgoing Interface: ge1
 Source: any
 Destination: any
 DSCP Code: any
 Service Type: service-object
 Service Object: FTP

DSCP Marking

DSCP Marking
 Inbound Marking: preserve
 Outbound Marking: preserve

Bandwidth Shaping

| | | |
|----------------------|---|-------------------------------|
| Guaranteed Bandwidth | Inbound: 200 kbps (0 : disabled) | Priority: 5 |
| | <input type="checkbox"/> Maximize Bandwidth Usage | Maximum 400 kbps |
| | Outbound: 200 kbps (0 : disabled) | Priority: 5 |
| | <input type="checkbox"/> Maximize Bandwidth Usage | Maximum 400 kbps |

802.1P Marking

Priority Code: 0 (0-7)
 Interface: none

Related Setting

Log: log alert



Note: In Bandwidth Management, the highest priority is (1) the lowest priority is (7).

Set Up the Bandwidth Management for HTTP on the

ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > BWM > Configuration > Add Policy**, select **Enable** and type **HTTP Any-to-WAN** as the policy's Description (Optional).

Leave the **Incoming Interface** to **any** and select the Outgoing Interface to be **wan1**. Select **Service Type** to be the **Service Object** and select **HTTP** from the list box.

Set the **Guaranteed Bandwidth Inbound** to 600 (kbps) and set higher **Priority 3**. Set the **Maximum** to 800 (kbps). Set the **Guaranteed Bandwidth Outbound Priority 3**.

In order to view the result later, set the **Log** setting to be **log alert**. Click **OK** to return to the **General** screen.

CONFIGURATION > BWM > Configuration > Add Policy

Configuration

☒ Enable

Description: HTTP Any-to-WAN (Optional)

BWM Type:
 ☒ Shared
 ☐ Per user
 ☐ Per-Source-IP

Criteria

User: any

Schedule: none

Incoming Interface: any

Outgoing Interface: ge1

Source: any

Destination: any

DSCP Code: any

Service Type: service-object

Service Object: HTTP

DSCP Marking

DSCP Marking

Inbound Marking: preserve

Outbound Marking: preserve

Bandwidth Shaping

Guaranteed Bandwidth

Inbound: 600 kbps (0 : disabled)

Priority: 3

☐ Maximize Bandwidth Usage

Maximum: 800 kbps

Outbound: 600 kbps (0 : disabled)

Priority: 3

☐ Maximize Bandwidth Usage

Maximum: 800 kbps

802.1P Marking

Priority Code: 0 (0-7)

Interface: none

Related Setting

Log: log alert



Note: In Bandwidth Management, the highest priority is (1) the lowest priority is (7).

Set Up the Bandwidth Management Global Setting on the

ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > BWM > BWM Global Setting**, select **Enable**.

CONFIGURATION > BWM > BWM Global Setting

BWM Global Setting

☒ Enable BWM





Test the Result

Access the Internet to generate FTP traffic and HTTP traffic. In this example, a 123 MB file is downloading from an FTP server. The FTP file should download slowly.

| <div> ← → ↻ <input type="text" value="ftp://ftp.zyxel.com/ZyWALL_1100/firmware/"/> ☆ ≡ </div> | | |
|--|---------|----------------------|
| <h3>Index of /ZyWALL_1100/firmware/</h3> | | |
| Name | Size | Date Modified |
| [parent directory] | | |
| ZyWALL 1100_3.10(AAAC.0)C0.zip | 55.0 MB | 7/11/13, 12:00:00 AM |
| ZyWALL 1100_3.10(AAAC.1)C0.zip | 55.4 MB | 9/26/13, 12:00:00 AM |
| ZyWALL 1100_3.20(AAAC.0)C0.zip | 55.5 MB | 6/9/14, 12:00:00 AM |
| ZyWALL 1100_4.10(AAAC.0)C0.zip | 115 MB | 9/2/14, 12:00:00 AM |
| ZyWALL 1100_4.10(AAAC.2)C0.zip | 115 MB | 3/9/15, 12:00:00 AM |
| ZyWALL 1100_4.11(AAAC.2)C0.zip | 122 MB | 5/4/15, 12:00:00 AM |
| ZyWALL 1100_4.11(AAAC.2)C0_2.pdf | 414 kB | 5/4/15, 12:00:00 AM |
| ZyWALL 1100_4.13(AAAC.0)C0_2.pdf | 494 kB | 8/5/15, 10:00:00 AM |
| ZyWALL 1100_4.13(AAAC.1)C0.zip | 123 MB | 8/28/15, 3:33:00 AM |
| ZyWALL 1100_4.13(AAAC.1)C0_2.pdf | 498 kB | 8/28/15, 3:33:00 AM |

Go to the ZyWALL/USG **Monitor > Log**, you will see [alert] log message such as below.

Monitor > Log

| Priority | Category | Message | Source | Destination |
|----------|----------|-------------------------------|--------------------|---|
| alert | BWM | Mode=port-base Rule=2 matched | 192.168.1.33:51495 |  216.241.54.88:54190 |
| alert | BWM | Mode=port-base Rule=2 matched | 192.168.1.33:51494 |  216.241.54.88:21 |
| alert | BWM | Mode=port-base Rule=2 matched | 192.168.1.33:51493 |  216.241.54.88:13700 |
| alert | BWM | Mode=port-base Rule=2 matched | 192.168.1.33:51492 |  216.241.54.88:21 |

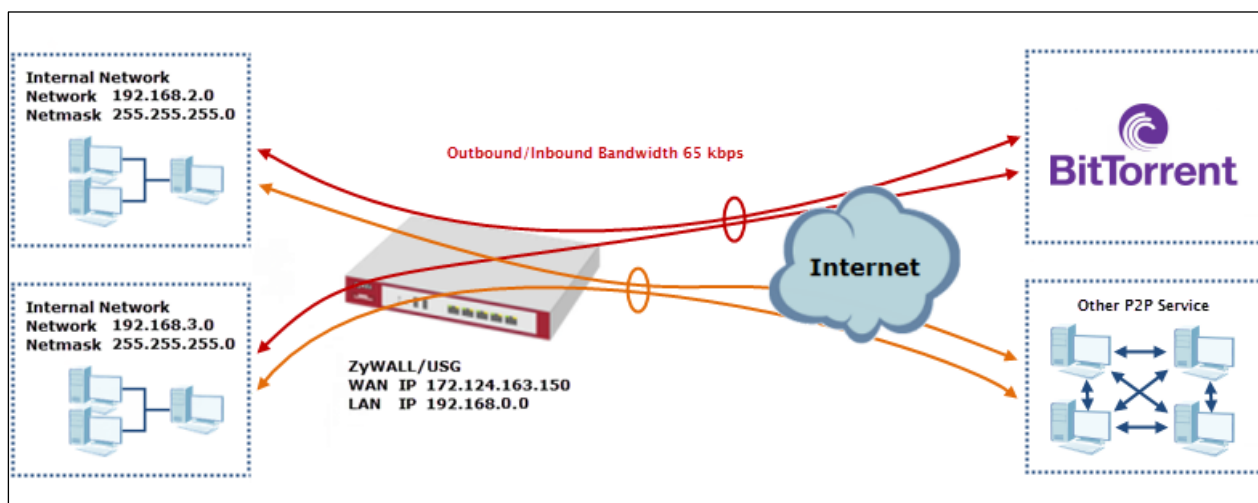
What Could Go Wrong?

If the "outbound" in the guaranteed bandwidth settings apply to traffic going from the connection initiator to the outgoing interface. "Inbound" refers to the reverse direction.

How to Limit BitTorrent or Other Peer-to-Peer Traffic

This is an example of using ZyWALL/USG Bandwidth Management (BWM) to control the bandwidth allocation for peer-to-peer traffic. You can use source interface, destination interface, destination port, schedule, user, source, destination information, DSCP code and service type as criteria to create a sequence of specific conditions to allocate bandwidth for the matching packets. When the BWM is configured, you can limit bandwidth consuming Application traffic, such as Peer-to-Peer (P2P) service.

ZyWALL/USG with Bandwidth Management for Peer-to-Peer Traffic Example



Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. The total available bandwidth assumption is 1,600 kbps. This example was tested using USG310

Set Up the Application Patrol Profile on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Object > Application > Add Application Rule**. Configure a **Name** for you to identify the **Application Profile**. Then, click **Add** to create an **Application Object**.

CONFIGURATION > Object > Application > Add Application Rule

Name: **BitTorrent**

Description: **New Create** (Optional)

Add Remove

| # | Category | Application |
|--------------------|----------|-------------|
| No data to display | | |

Page 1 of 1 | Show 50 items

In the **Application Object**, select **By Service**, type a keyword and click **Search** to display all signatures containing that keyword. Select all **Query Result** and Click **OK**.

CONFIGURATION > Object > Application > Add Application Rule > Add Application Object

Query

Search: **By Service** **BitTorrent** **Search**

Query Result

| # | Category | Application |
|---|----------|------------------------------|
| 1 | P2P | BitTorrent Series (transfer) |
| 2 | P2P | BitTorrent Series (access) |
| 3 | P2P | BitTorrent Series (connect) |

Page 1 of 1 | Show 50 items | Displaying 1 - 3 of 3

Set Up the Bandwidth Management for BitTorrent on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > BWM > Configuration > Add Policy**, select **Enable** and type **BitTorrent Any-to-Any** as the policy's **Description**.

Leave the **Incoming Interface** to **any** and select the Outgoing Interface to be **wan1**. Select **Service Type** to be the **Service Object** and select **BitTorrent** from the list box.


Set the **Guaranteed Bandwidth Inbound** to 65 (kbps) and set **Priority 5** (low-to-medium). Set the **Maximum** to 512(kbps). Set the **Guaranteed Bandwidth Outbound** to 65 (kbps) and set **Priority 5**. Set the **Maximum** to 512 (kbps). Click **OK** to return to the **General** screen.

CONFIGURATION > BWM > Configuration > Add Policy

Configuration

☒ Enable

Description: BitTorrent Any-to-Any (Optional)

BWM Type: ☒ Shared ☐ Per user ☐ Per-Source-IP 

Criteria

User: any

Schedule: none

Incoming Interface: any

Outgoing Interface: any

Source: any

Destination: any

DSCP Code: any

Service Type: ☐ Service Object ☒ Application Object

Application Object: BitTorrent

DSCP Marking

DSCP Marking

Inbound Marking: preserve

Outbound Marking: preserve

Bandwidth Shaping

| | | | | | | |
|----------------------|---|---------------------|---------------------|-----------|------|------|
| Guaranteed Bandwidth | Inbound: | 65 | kbps (0 : disabled) | Priority: | 5 | |
| | <input type="checkbox"/> Maximize Bandwidth Usage | | | Maximum: | 512 | kbps |
| Outbound: | 65 | kbps (0 : disabled) | Priority: | 5 | | |
| | <input type="checkbox"/> Maximize Bandwidth Usage | | Maximum: | 512 | kbps | |

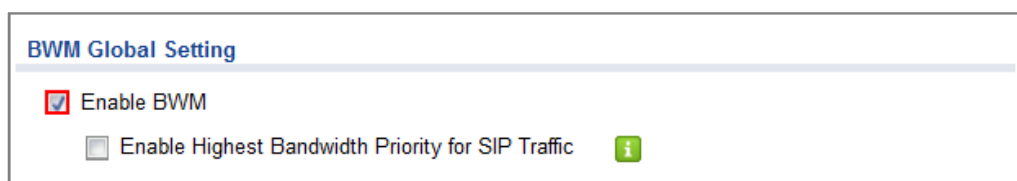


Note: In Bandwidth Management, the highest priority is (1) the lowest priority is (7).

Set Up the Bandwidth Management Global Setting on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > BWM > BWM Global Setting**, select **Enable**.

CONFIGURATION > BWM > BWM Global Setting

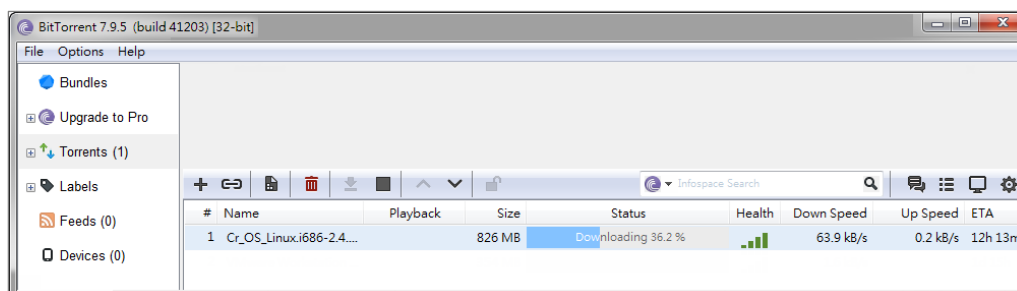


Test the Result

Download BitTorrent application for testing the result:

<http://www.bittorrent.com/downloads>

In this example, an 826 MB file is downloading, the **Down Speed** limited to maximum 65 kB/s.



Go to the ZyWALL/USG **Monitor > Log**, you will see [alert] log message such as below.

Monitor > Log

| Priority | Category | Message | Source | Destination | Protocol |
|----------|----------|-------------------------------|--------------------|----------------------|----------|
| alert | BWM | Mode=port-less Rule=1 matched | 192.168.1.33:53722 | 187.34.56.190:13867 | udp |
| alert | BWM | Mode=port-less Rule=1 matched | 192.168.1.33:53722 | 84.250.209.195:51413 | udp |
| alert | BWM | Mode=port-less Rule=1 matched | 192.168.1.33:53722 | 89.43.62.55:51016 | udp |

What Could Go Wrong?

If the "outbound" in the guaranteed bandwidth settings apply to traffic going from the connection initiator to the outgoing interface. "Inbound" refers to the reverse direction.

Make sure you have registered the **Application Patrol** service on the ZyWALL/USG to use **Application Object** as the **Service Type** in the bandwidth management rules.

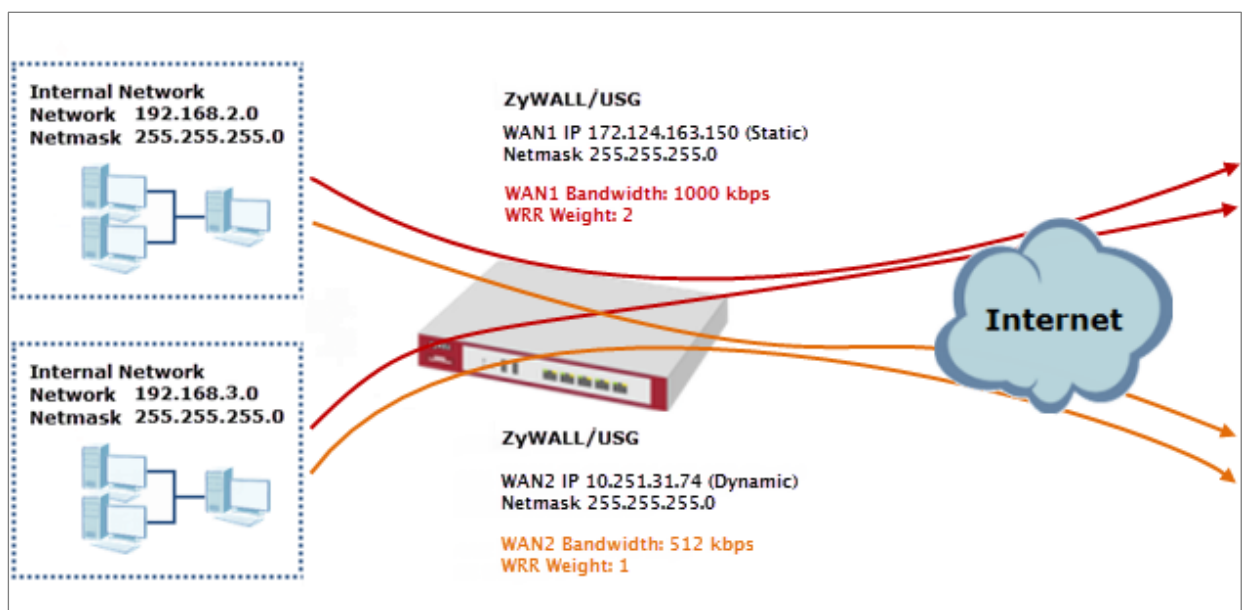
| | |
|---------------------|--|
| Service Type: | <input type="radio"/> Service Object <input checked="" type="radio"/> Application Object |
| Application Object: | <div>BitTorrent</div> |


You can click the link from the **CONFIGURATION > Licensing > Registration** screen of your ZyXEL device's Web Configurator or click the myZyXEL.com 2.0 icon from the portal page (<https://portal.myzyxel.com/>) to register or extend your **Application Patrol** license.

How to Configure a Trunk for WAN Load Balancing with a Static or Dynamic IP Address

This is an example of using ZyWALL/USG Trunk for two WAN connections to the Internet. The available bandwidth for the connections is 1000 kbps (wan1 with static IP address) and 512 Kbps (wan2 with dynamic IP address) respectively. As these connections have different bandwidths, we will use the Weighted Round Robin (WRR) algorithm to send traffic to wan1 and wan2 in a 2:1 ratio.

ZyWALL/USG with WAN Load Balancing Example



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the Available Bandwidth on WAN1 Interfaces on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Interface > Ethernet > WAN1 > Egress Bandwidth** and enter the available bandwidth (1000 kbps) in the **Egress Bandwidth** field. Click **OK**.

CONFIGURATION > Interface > Ethernet > WAN1

| General Settings | |
|-------------------------------------|---------------------------------|
| <input checked="" type="checkbox"/> | Enable Interface |
| Interface Properties | |
| Interface Type: | external i |
| Interface Name: | WAN1 |
| Port: | P1 |
| Zone: | WAN i |
| MAC Address: | B8:EC:A3:A9:C0:0B |
| Description: | <input type="text"/> (Optional) |
| IP Address Assignment | |
| <input type="radio"/> | Get Automatically |
| <input checked="" type="checkbox"/> | Advance |
| <input checked="" type="radio"/> | Use Fixed IP Address |
| IP Address: | 172.124.163.150 |
| Subnet Mask: | 255.255.255.0 |
| Gateway: | <input type="text"/> (Optional) |
| Metric: | 0 (0-15) |
| <input checked="" type="checkbox"/> | Enable IGMP Support |
| <input checked="" type="radio"/> | IGMP Upstream |
| <input type="radio"/> | IGMP Downstream |
| Interface Parameters | |
| Egress Bandwidth: | 1000 Kbps i |

Set Up the Available Bandwidth on WAN2 Interfaces on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Interface > Ethernet > WAN2 > Egress Bandwidth** and enter the available bandwidth (512 kbps) in the **Egress Bandwidth** field. Click **OK**.

CONFIGURATION > Interface > Ethernet > WAN2

General Settings

☒ Enable Interface

Interface Properties

Interface Type: external ⓘ

Interface Name: WAN2

Port: P3

Zone: WAN ⓘ

MAC Address: B8:EC:A3:A9:C0:0D

Description: ⓘ (Optional)

IP Address Assignment

☒ Get Automatically 10.251.31.74

☐ Advance

☐ Use Fixed IP Address

IP Address: ⓘ

Subnet Mask: ⓘ

Gateway: ⓘ (Optional)

Metric: 0 (0-15)

☐ Enable IGMP Support

☒ IGMP Upstream

☐ IGMP Downstream

Interface Parameters

Egress Bandwidth: 512 Kbps ⓘ

Set Up the WAN Trunk on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Interface > Trunk > User Configuration > Add Trunk**. Configure a **Name** for you to identify the Trunk profile and set the **Load Balancing Algorithm** field to be the **Weighted Round Robin**.

Add **WAN1** and enter **2** in the **Weight** column. Add **WAN2** and enter **1** in the **Weight** column. Click **OK** to return to the **Configuration** screen.

CONFIGURATION > Interface > Trunk > User Configuration > Add Trunk

Name:

Load Balancing Algorithm:

| # | Member | Mode | Weight |
|---|--------|--------|--------|
| 1 | WAN1 | Active | 2 |
| 2 | WAN2 | Active | 1 |

Page 1 of 1 Show 50 items Displaying 1 - 2 of 2

In the **Configuration** screen, go to **Default WAN Trunk** section, select **User Configured Trunk** and select the newly created Trunk from the list box. Click **Apply**.

CONFIGURATION > Interface > Trunk > Default WAN Trunk

Default WAN Trunk

☐ Advance

Default Trunk Selection

☐ SYSTEM_DEFAULT_WAN_TRUNK

☒ User Configured Trunk

Test the Result

Browse any website to test the result.

The Weighted Round Robin (WRR) algorithm is best suited for situations where the bandwidths set for the two WAN interfaces are different. An interface with a larger weight (**WAN1**) gets more chances to transmit traffic than an interface with a smaller weight (**WAN2**).

MONITOR > Interface Summary > Interface Statistics

| Interface Statistics | | | | | |
|----------------------|------------|--------|--------|--------|--------|
| Refresh | | | | | |
| Name | Status | TxPkts | RxPkts | Tx B/s | Rx B/s |
| + ge1 | Down | 0 | 0 | 0 | 0 |
| + WAN1 | 1000M/Full | 16501 | 47815 | 0 | 634 |
| + WAN2 | 1000M/Full | 268 | 169 | 0 | 0 |

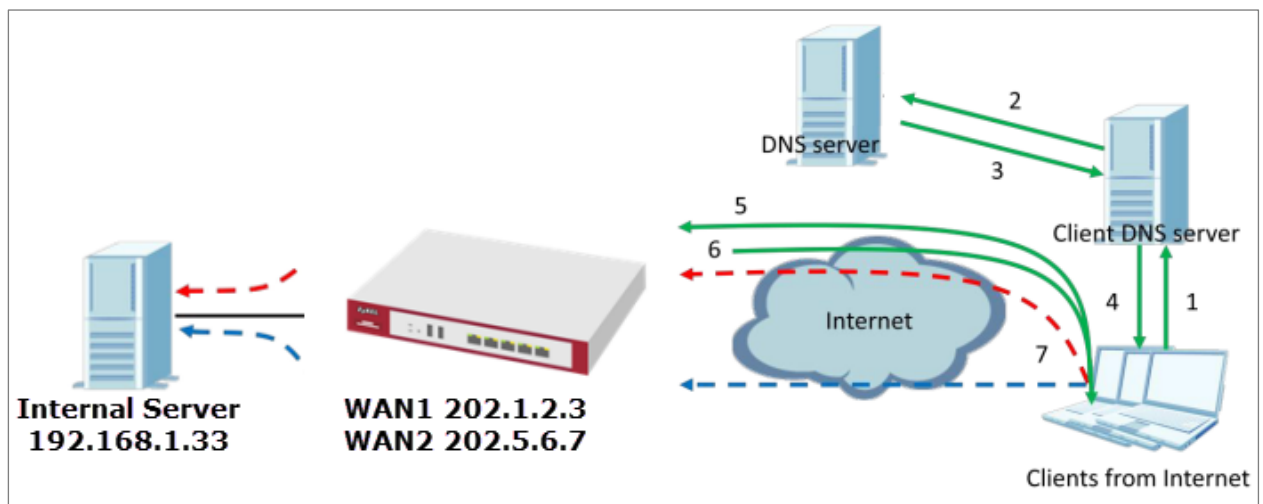
What Could Go Wrong?


If there is no traffic passing through either WAN1 or WAN2 interfaces, check that the **Mode** of both WAN1 & WAN2 should be **Active**. If a trunk is in **Passive** mode, the ZyWALL/USG will use this connection only when all of the connections set to **Active** mode are down.

How to Configure DNS Inbound Load Balancing to balance DNS Queries Among Interfaces

This is an example of using the ZyWALL/USG dynamically responding to DNS query messages with its least loaded interface's IP address. The DNS query senders will then transmit packets to that interface instead of an interface that has a heavy load. This example assumes that your company's domain name is `www.example.com`. You want your ZyWALL/USG's WAN1 (202.1.2.3) and WAN2 (202.5.6.7) to use DNS inbound load balancing to balance traffic loading coming from the Internet.

ZyWALL/USG with DNS Inbound Load Balancing Example



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the DNS Inbound Load Balancing on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > DNS Inbound LB**. Edit the **Query Domain Name**, set the **Load Balancing Algorithm** field to be the **Least Load - Total**. Click **Add** to create a new **Load Balancing Member**.

CONFIGURATION > Network > DNS Inbound LB

General Setting

☐ Enable

DNS Settings

Query Domain Name: zyxel.for-our.info

Time to Live: 0 (0-604800 seconds, 0 is unchanged)

Query From Settings

IP Address: any

Zone: any

Load Balancing Member

Load Balancing Algorithm: Least Load - Total

Failover IP Address: 0.0.0.0 (Optional)

+ Add Edit Remove

| # | IP Address | Monitor Interface |
|---|------------|-------------------|
| Page 0 of 0 Show 50 items No data to display | | |

If you want to configure Security Option Control, please go to [DNS](#)

CONFIGURATION > Network > DNS Inbound LB

Add Load Balancing Member

Load Balancing Member

Member: 1

Monitor Interface: WAN1 DHCP client -- 202.1.2.3/255.255.255.0

IP Address

☒ Same as Monitor Interface 202.1.2.3

☐ Custom 0.0.0.0

OK Cancel

CONFIGURATION > Network > DNS Inbound LB

Add Load Balancing Member

Load Balancing Member

Member: 2

Monitor Interface: WAN2 DHCP client -- 202.5.6.7/255.255.255.0

IP Address

☒ Same as Monitor Interface 202.5.6.7

☐ Custom 0.0.0.0

OK Cancel

Go to the **Global Setting** page to select **Enable DNS Load Balancing**.

CONFIGURATION > Network > DNS Inbound LB

Global Setting

☒ Enable DNS Load Balancing

Set Up the NAT Rule on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > NAT**. Configure the **Virtual**

Server to forward the traffic from WAN to Internal Server (192.168.1.33). Click **OK**.

CONFIGURATION > Network > NAT

| General Settings | |
|---|--|
| <input checked="" type="checkbox"/> Enable Rule | |
| Rule Name: | NAT_WAN1 |
| Port Mapping Type | |
| Classification: | <input checked="" type="radio"/> Virtual Server <input type="radio"/> 1:1 NAT <input type="radio"/> Many 1:1 NAT |
| Mapping Rule | |
| Incoming Interface: | WAN1 |
| Original IP: | User Defined |
| User-Defined Original IP: | 202.1.2.3 (IP Address) |
| Mapped IP: | User Defined |
| User-Defined Mapped IP: | 192.168.1.33 (IP Address) |
| Port Mapping Type: | Port |
| Protocol Type: | any |
| Original Port: | 80 |
| Mapped Port: | 80 |

| General Settings | |
|---|--|
| <input checked="" type="checkbox"/> Enable Rule | |
| Rule Name: | NAT_WAN2 |
| Port Mapping Type | |
| Classification: | <input checked="" type="radio"/> Virtual Server <input type="radio"/> 1:1 NAT <input type="radio"/> Many 1:1 NAT |
| Mapping Rule | |
| Incoming Interface: | WAN2 |
| Original IP: | User Defined |
| User-Defined Original IP: | 202.5.6.7 (IP Address) |
| Mapped IP: | User Defined |
| User-Defined Mapped IP: | 192.168.1.33 (IP Address) |
| Port Mapping Type: | Port |
| Protocol Type: | any |
| Original Port: | 80 |
| Mapped Port: | 80 |

Test the Result

Open the browser and query **http://zyxel.for-our.info/**.

Create a **Security Policy** in order to view the testing result. Set **Destination** to be the Internal Server IP address (192.168.1.33 in this example) and set **Log** type to be the **Log Alert**.

Go to the ZyWALL/USG **Monitor > Log**, you will see [alert] log message such as below. The **Source Interface** is the WAN1 or WAN2 interface which is handling the least amount of outgoing and incoming traffic.

| Prior... | Category | Message | Source | Source I... | Destination | Note |
|----------|---------------------|--|-----------------|-------------|-----------------|-----------------|
| alert | Security Policy ... | priority:1, from ANY to ANY, TCP, service oth... | 202.1.2.4:52268 | WAN2 | 192.168.1.33:80 | ACCESS FORWA... |
| alert | Security Policy ... | priority:1, from ANY to ANY, TCP, service oth... | 202.1.2.4:52267 | WAN2 | 192.168.1.33:80 | ACCESS FORWA... |
| alert | Security Policy ... | priority:1, from ANY to ANY, TCP, service oth... | 202.1.2.4:52266 | WAN1 | 192.168.1.33:80 | ACCESS FORWA... |
| alert | Security Policy ... | priority:1, from ANY to ANY, TCP, service oth... | 202.1.2.4:52265 | WAN1 | 192.168.1.33:80 | ACCESS FORWA... |
| alert | Security Policy ... | priority:1, from ANY to ANY, TCP, service oth... | 202.1.2.4:52260 | WAN1 | 192.168.1.33:80 | ACCESS FORWA... |
| alert | Security Policy ... | priority:1, from ANY to ANY, TCP, service oth... | 202.1.2.4:52259 | WAN1 | 192.168.1.33:80 | ACCESS FORWA... |
| alert | Security Policy ... | priority:1, from ANY to ANY, TCP, service oth... | 202.1.2.4:52258 | WAN2 | 192.168.1.33:80 | ACCESS FORWA... |
| alert | Security Policy ... | priority:1, from ANY to ANY, TCP, service oth... | 202.1.2.4:52257 | WAN2 | 192.168.1.33:80 | ACCESS FORWA... |

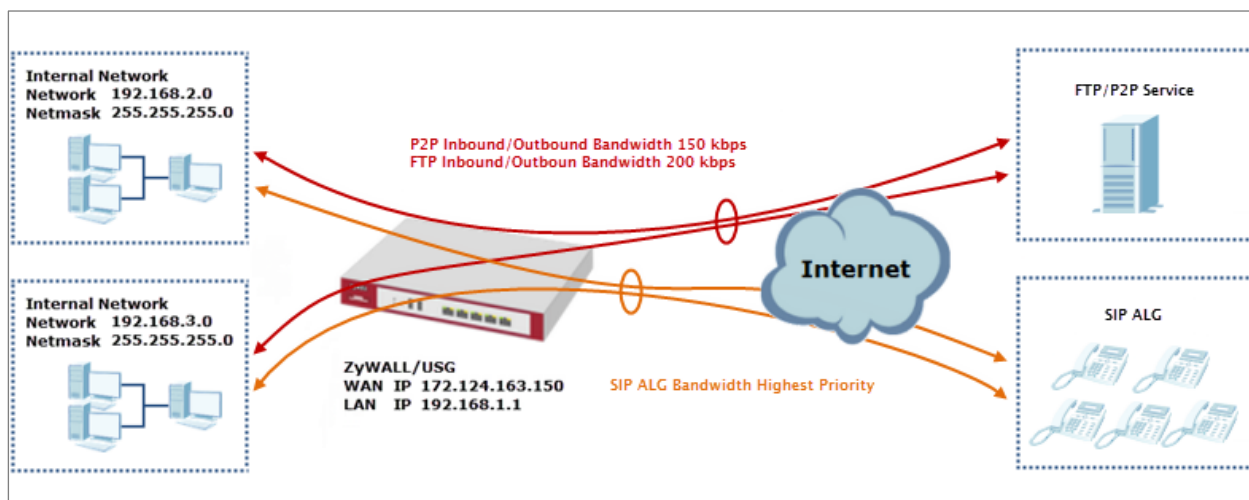
What Could Go Wrong?


If you cannot access the Internal Server, please check that the NAT configuration matches the Internal Server IP address and Port number. If the NAT configuration is correct, please check the system status of your Internal Server is up.

How to Manage Voice Traffic

This is an example of using Application Layer Gateway (ALG) to allow the SIP (Session Initiation Protocol) voice traffic through the ZyWALL/USG. To achieve high-quality voice transmissions, use ZyWALL/USG provides Bandwidth Management (BWM) function to effectively manage bandwidth according to flexible criteria. You can limit bandwidth consuming services, such as Peer-to-Peer (P2P) and FTP service while providing a higher priority and consistent bandwidth for voice traffic.

ZyWALL/USG with Voice Traffic Management Example



 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the SIP ALG on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > SIP > SIP Settings**, select **Enable SIP ALG**, **Enable SIP Transformations** (optional), **Restrict Peer to Peer Signaling Connection** and **Restrict Peer to Peer Media Connection**. Make sure the **SIP Signaling Port** is configured the same as your VoIP phone SIP signaling port. Click **Apply**.

CONFIGURATION > BWM > Configuration > Add Policy

SIP Settings

☒ Enable SIP ALG

☒ Enable SIP Transformations

☒ Enable Configure SIP Inactivity Timeout

 SIP Media Inactivity Timeout : (seconds)

 SIP Signaling Inactivity Timeout : (seconds)


☒ Restrict Peer to Peer Signaling Connection

☒ Restrict Peer to Peer Media Connection ⓘ

 SIP Signaling Port :

+ Add
Edit
Remove

| # | Port ▲ |
|---|--------|
| 1 | 5060 |

 Note: If you are using a custom or additional UDP port number (not 5060) for SIP traffic, use the **Add** icon to add **SIP Signaling Port** numbers.

Set Up the Bandwidth Management for SIP on the ZyWALL/USG


In the ZyWALL/USG, go to **CONFIGURATION > BWM > BWM Global Settings**, select

Enable **BWM** and **Enable Highest Bandwidth Priority for SIP Traffic**.

CONFIGURATION > BWM > BWM Global Settings > Enable BWM

BWM Global Setting

☒ Enable BWM

☒ Enable Highest Bandwidth Priority for SIP Traffic
 

Set Up the Bandwidth Management for P2P on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > BWM > Configuration > Add Policy**, select **Enable** and type **P2P Any-to-WAN** as the policy's **Description**.

Leave the **Incoming Interface** to **any** and select the Outgoing Interface to be **WAN1**. Select **Service Type** to be the **Application Object** and select **P2P** from the list box.


Set the **Guaranteed Bandwidth Inbound** to 100 (kbps) and set **Priority** 5. Set the **Maximum** to 150 (kbps). Set the **Guaranteed Bandwidth Outbound** to 100 (kbps) and set **Priority** 5. Set the **Maximum** to 150 (kbps). Click **OK** to return to the **General** screen.

CONFIGURATION > BWM > Configuration > Add Policy

Configuration

☒ Enable

Description: P2P Any-to-WAN (Optional)

BWM Type:
 ☒ Shared
 ☐ Per user
 ☐ Per-Source-IP
 

Criteria

User: any

Schedule: none

Incoming Interface: any

Outgoing Interface: WAN1

Source: any

Destination: any

DSCP Code: any

Service Type:
 ☐ Service Object
 ☒ Application Object

Application Object: P2P

DSCP Marking

DSCP Marking

Inbound Marking: preserve

Outbound Marking: preserve

Bandwidth Shaping

Guaranteed Bandwidth

Inbound: 100 kbps (0 : disabled)
 Priority: 5

☐ Maximize Bandwidth Usage
 Maximum: 150 kbps

Outbound: 100 kbps (0 : disabled)
 Priority: 5

☐ Maximize Bandwidth Usage
 Maximum: 150 kbps



Note: In Bandwidth Shaping, the highest priority is (1) the lowest priority is (7).

Set Up the Bandwidth Management for FTP on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > BWM > Configuration > Add Policy**, select **Enable** and type **FTP Any-to-Any** as the policy's **Description**.

Leave the **Incoming Interface** to **any** and select the Outgoing Interface to be **WAN1**. Select **Service Type** to be the **Service Object** and select **FTP** from the list box.

Set the **Guaranteed Bandwidth Inbound** to 150 (kbps) and set **Priority** 5. Set the **Maximum** to 200 (kbps). Set the **Guaranteed Bandwidth Outbound** to 150 (kbps) and set **Priority** 5. Set the **Maximum** to 200 (kbps). Click **OK** to return to the **General** screen.

CONFIGURATION > BWM > Configuration > Add Policy

Configuration

☒ Enable

Description: FTP Any-to-WAN (Optional)

BWM Type: ☒ Shared ☐ Per user ☐ Per-Source-IP

Criteria

User: any

Schedule: none

Incoming Interface: any

Outgoing Interface: WAN1

Source: any

Destination: any

DSCP Code: any

Service Type: ☒ Service Object ☐ Application Object

Service Object: FTP

DSCP Marking

DSCP Marking

Inbound Marking: preserve

Outbound Marking: preserve

Bandwidth Shaping

| | | | | | |
|----------------------|---|---------------------|---------------------|----------------|-----------------------|
| Guaranteed Bandwidth | Inbound: | 150 | kbps (0 : disabled) | Priority: | 5 |
| | <input type="checkbox"/> Maximize Bandwidth Usage | | | Maximum: | 200 kbps |
| Outbound: | 150 | kbps (0 : disabled) | Priority: | 5 | |
| | <input type="checkbox"/> Maximize Bandwidth Usage | | | Maximum: | 200 kbps |



Note: In Bandwidth Shaping, the highest priority is (1) the lowest priority is (7).

Test the Result

Add a **Security Policy** rule to view the SIP log:

CONFIGURATION > BWM > Configuration > Add Policy

☒ Enable

Name:

Description: (Optional)

From:

To:

Source:

Destination:

Service:

User:

Schedule:

Action:

Log matched traffic:







Dial Phone Number 1001 (192.168.10.2 in this example) from Phone Number 1002 (192.168.100.2 in this example), go to the ZyWALL/USG **Monitor > Log**, you will see [alert] log message such as below. The **Destination** IP address is the SIP Server IP address.

Monitor > Log

| Priority | Category | Message | Source | Destination | Note |
|----------|-------------------------|---|--------------------|----------------------|----------------|
| alert | Security Policy Control | priority:1, from ANY to ANY, UDP, service SIP, ACCEPT | 192.168.100.2:5060 | 172.124.163.150:5060 | ACCESS FORWARD |

Go to the ZyWALL/USG **Monitor > Traffic Statics** and review the SIP traffic and other services to optimize the **Guaranteed** and **Maximum BW** of bandwidth consuming services.

Monitor > Traffic Statics

| # | Service Port | Protocol | Direction | Amount |
|---|-------------------|----------|-----------|--|
| 1 | sip(Port : 5060) | UDP | Ingress |  10.137(MBytes) |
| 2 | sip(Port : 5060) | UDP | Egress |  10.138(MBytes) |
| 3 | ftp(Port : 21) | TCP | Ingress |  863(Bytes) |
| 4 | ftp(Port : 21) | TCP | Egress |  807(Bytes) |
| 5 | https(Port : 443) | TCP | Ingress |  29.716(KBytes) |
| 6 | www(Port : 80) | TCP | Egress |  1.196(KBytes) |

What Could Go Wrong?

If you see [alert] log message such as below, the voice traffic is blocked by the priority 1 **Security Policy**. The ZyWALL/USG checks the security policy in order and applies the first security policy the traffic matches. If the voice traffic matches a policy that comes earlier in the list, it may be unexpectedly blocked. Please change your policy setting or move the voice traffic policy to the higher priority.

Monitor > Log

| Priority | Category | Message | Source | Destination | Note |
|----------|-------------------------|--|--------------------|----------------------|--------------|
| alert | Security Policy Control | priority:1, from ANY to ANY, UDP, service others, DROP | 192.168.100.2:5060 | 172.124.163.150:5060 | ACCESS BLOCK |
| alert | Security Policy Control | priority:1, from ANY to ANY, UDP, service others, DROP | 192.168.100.2:5060 | 172.124.163.150:5060 | ACCESS BLOCK |

How to Manage ZyWALL/USG Configuration Files

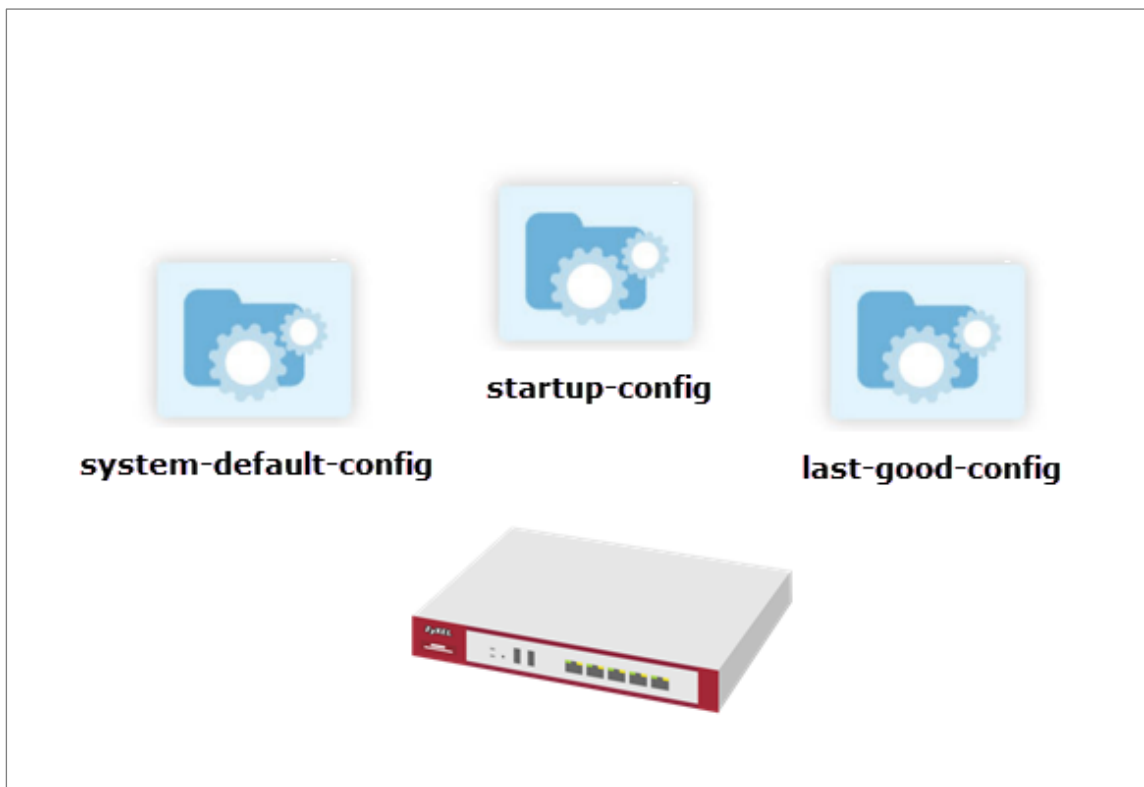
This is an example of how to rename, download, copy, apply and upload configuration files. Once your ZyWALL/USG is configured and functioning properly, it is highly recommended that you back up your configuration file before making further configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

The **system-default.conf** file contains the ZyWALL/USG's default settings. This configuration file is included when you upload a firmware package.

The **startup-config.conf** file is the configuration file that the ZyWALL/USG is currently using. If you make and save changes during your management session, the changes are applied to this configuration file.

The **lastgood.conf** is the most recently used (valid) configuration file that was saved when the device last restarted.

ZyWALL/USG with Configuration Files Example

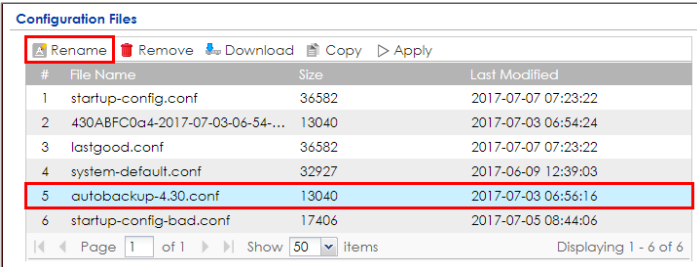


 Note: This example was using USG310 (Firmware Version: ZLD 4.25).

Rename the Configuration Files from the ZyWALL/USG

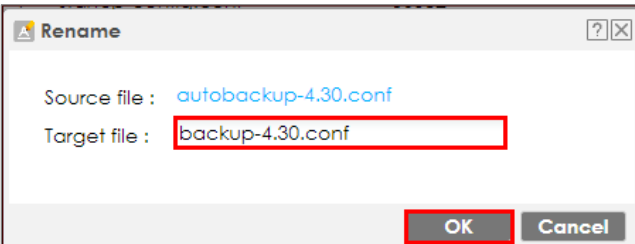
In the ZyWALL/USG, go to **MAINTENANCE > File Manager > Configuration File**, select the configuration file and click **Rename**. A pop-up screen will appear allowing you to edit the **Target file** name. Click **OK** to save the **Rename** configuration.

MAINTENANCE > File Manager > Configuration File



| # | File Name | Size | Last Modified |
|---|---------------------------------|-------|---------------------|
| 1 | startup-config.conf | 36582 | 2017-07-07 07:23:22 |
| 2 | 430ABFC0a4-2017-07-03-06-54-... | 13040 | 2017-07-03 06:54:24 |
| 3 | lastgood.conf | 36582 | 2017-07-07 07:23:22 |
| 4 | system-default.conf | 32927 | 2017-06-09 12:39:03 |
| 5 | autobackup-4.30.conf | 13040 | 2017-07-03 06:56:16 |
| 6 | startup-config-bad.conf | 17406 | 2017-07-05 08:44:06 |

MAINTENANCE > File Manager > Configuration File > Rename



Rename

Source file : autobackup-4.30.conf

Target file : backup-4.30.conf

OK Cancel

Download the Configuration Files on the ZyWALL/USG

In the ZyWALL/USG, go to **MAINTENANCE > File Manager > Configuration File**, select the configuration file and click **Download** to back up your configuration file from ZyWALL/USG to your computer.

MAINTENANCE > File Manager > Configuration File

| Configuration Files | | | |
|---|---------------------------------|-------|---------------------|
| Rename Remove Download Copy Apply | | | |
| # | File Name | Size | Last Modified |
| 1 | startup-config.conf | 36582 | 2017-07-07 07:23:22 |
| 2 | 430ABFC0a4-2017-07-03-06-54-... | 13040 | 2017-07-03 06:54:24 |
| 3 | lastgood.conf | 36582 | 2017-07-07 07:23:22 |
| 4 | system-default.conf | 32927 | 2017-06-09 12:39:03 |
| 5 | autobackup-4.30.conf | 13040 | 2017-07-03 06:56:16 |
| 6 | startup-config-bad.conf | 17406 | 2017-07-05 08:44:06 |
| Page 1 of 1 Show 50 items Displaying 1 - 6 of 6 | | | |

Copy the Configuration Files on the ZyWALL/USG

In the ZyWALL/USG, go to **MAINTENANCE > File Manager > Configuration File**, select the configuration file and click **Copy**. A pop-up screen will appear allowing you to edit the **Target file** name. Click **OK** to save the **Copy** configuration.

MAINTENANCE > File Manager > Configuration File

| Configuration Files | | | |
|---|---------------------------------|-------|---------------------|
| Rename Remove Download Copy Apply | | | |
| # | File Name | Size | Last Modified |
| 1 | startup-config.conf | 36582 | 2017-07-07 07:23:22 |
| 2 | 430ABFC0a4-2017-07-03-06-54-... | 13040 | 2017-07-03 06:54:24 |
| 3 | lastgood.conf | 36582 | 2017-07-07 07:23:22 |
| 4 | system-default.conf | 32927 | 2017-06-09 12:39:03 |
| 5 | autobackup-4.30.conf | 13040 | 2017-07-03 06:56:16 |
| 6 | startup-config-bad.conf | 17406 | 2017-07-05 08:44:06 |
| Page 1 of 1 Show 50 items Displaying 1 - 6 of 6 | | | |

MAINTENANCE > File Manager > Configuration File > Copy

Copy File

Source file : startup-config.conf
 Target file : startup-config(1).conf

OK Cancel

Apply the Configuration Files on the ZyWALL/USG

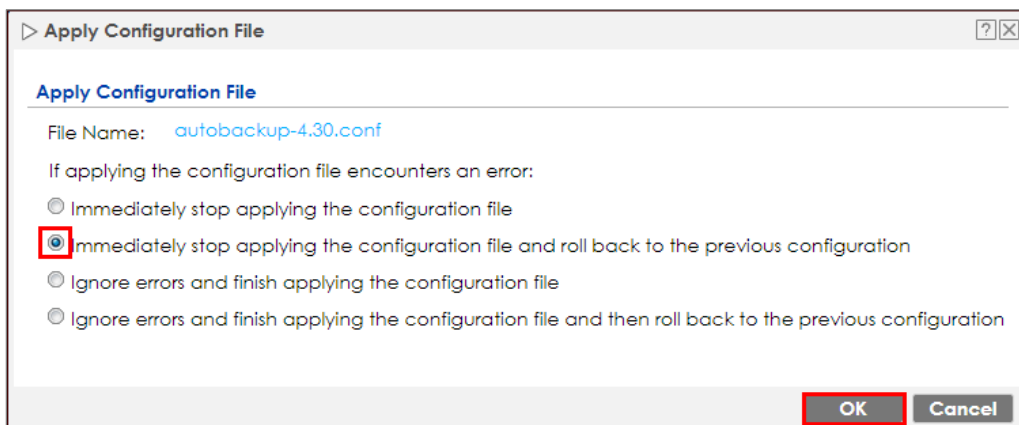
In the ZyWALL/USG, go to **MAINTENANCE > File Manager > Configuration File**, select a specific configuration file to have ZyWALL/USG use it. For example, select the **system-default.conf** file and click **Apply** to reset all of the ZyWALL/USG settings to the factory defaults. Or select the **lastgood.conf** which is the most recently used (valid) configuration file that was saved when the device last restarted. If you uploaded and applied a configuration file with an error, select this file then click **Apply** to return to a valid configuration.

MAINTENANCE > File Manager > Configuration File

| Configuration Files | | | |
|---|---|-------|---------------------|
| | Rename Remove Download Copy Apply | | |
| # | File Name | Size | Last Modified |
| 1 | startup-config.conf | 36582 | 2017-07-07 07:32:04 |
| 2 | 430ABFC0a4-2017-07-03-06-54-... | 13040 | 2017-07-03 06:54:24 |
| 3 | lastgood.conf | 36582 | 2017-07-07 07:23:22 |
| 4 | system-default.conf | 32927 | 2017-06-09 12:39:03 |
| 5 | autobackup-4.30.conf | 13040 | 2017-07-03 06:56:16 |
| 6 | startup-config-bad.conf | 17406 | 2017-07-05 08:44:06 |
| Page 1 of 1 Show 50 items Displaying 1 - 6 of 6 | | | |

A pop-up screen will appear allowing you to edit the **Target file** name. Select **Immediately stop applying the configuration file and roll back to the previous configuration** to get the ZyWALL/USG started with a fully valid configuration file as quickly as possible. Click **OK** to have the ZyWALL/USG start applying the configuration file.

MAINTENANCE > File Manager > Configuration File > Apply Configuration File

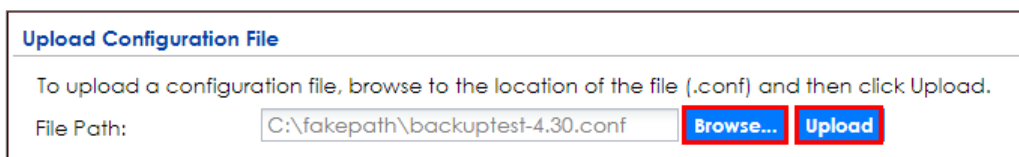


Note: Do not shut down the ZyWALL/USG while the configuration file is being applied.

Upload the Configuration Files from the ZyWALL/USG

In the ZyWALL/USG, go to **MAINTENANCE > File Manager > Configuration File > Upload Configuration File**, select **Browse** to upload a new or previously saved configuration file from your computer to your ZyWALL/USG. You cannot upload a configuration file named **system-default.conf** or **lastgood.conf**. If you upload **startup-config.conf**, it will replace the current configuration and immediately apply the new settings.

MAINTENANCE > File Manager > Configuration File

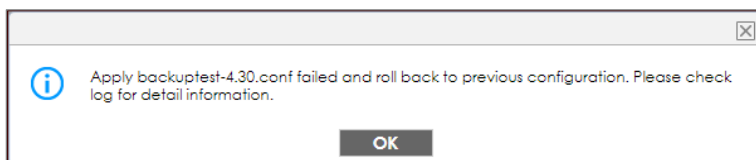


What Could Go Wrong?

If you cannot apply a configuration file and the device shows error message, go to **Monitor > Log** to check the [alert] log message and make the correction of the

configuration file. In this example, the [alert] log message shows the configuration file has an incomplete static DHCP address so that the device can't apply it.

MAINTENANCE > File Manager > Configuration File > Apply Configuration File



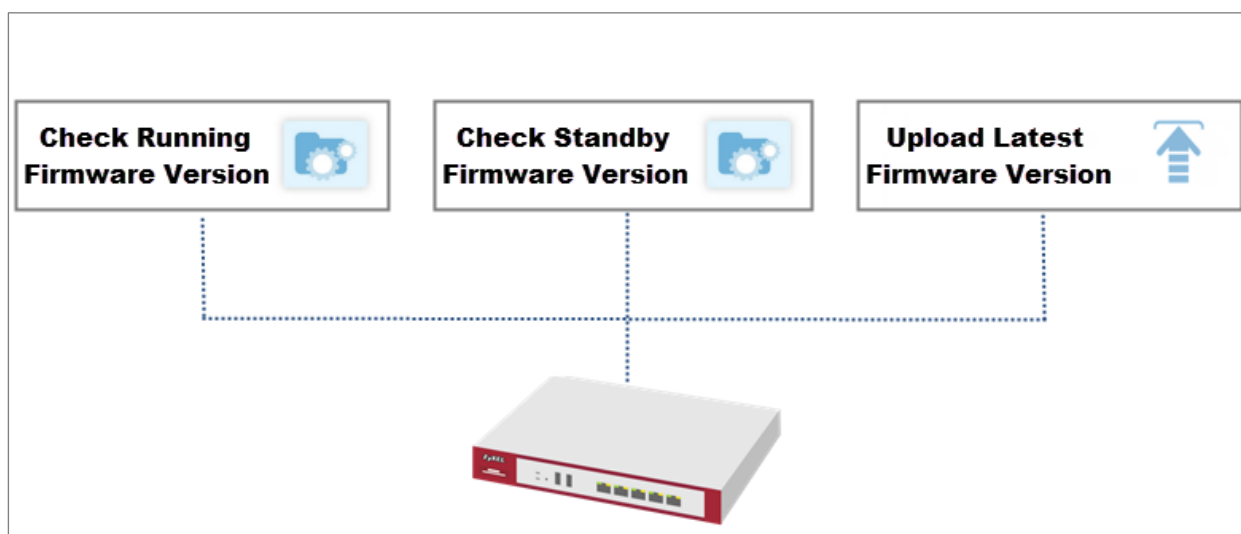
Monitor > Log


| Priority | Category | Message | Note |
|----------|--------------|--|--------------|
| alert | File Manager | Going to rollback previous running-config. | Apply Config |
| alert | File Manager | ERROR: #configure terminal interface _ether dmz ip address 192.168.3.1 255.... | Apply Config |

How to Manage ZyWALL/USG Firmware

This is an example of using ZyWALL/USG to check your current firmware version and upload firmware to the ZyWALL/USG. You can upload firmware to be the **Running** firmware or **Standby** firmware.

ZyWALL/USG with Firmware Management Example





 Note: The firmware update can take up to five minutes. Do not turn off or reset the ZyWALL/USG while the firmware update is in progress. This example was using USG110 (Firmware Version: ZLD 4.25).


Download the Current Firmware Version from ZyXEL.com

Go to www.zyxel.com/support/download_landing.shtml and download the current firmware package.


Search by Model Number



 USG110

 USG1100

Don't know the product model number?

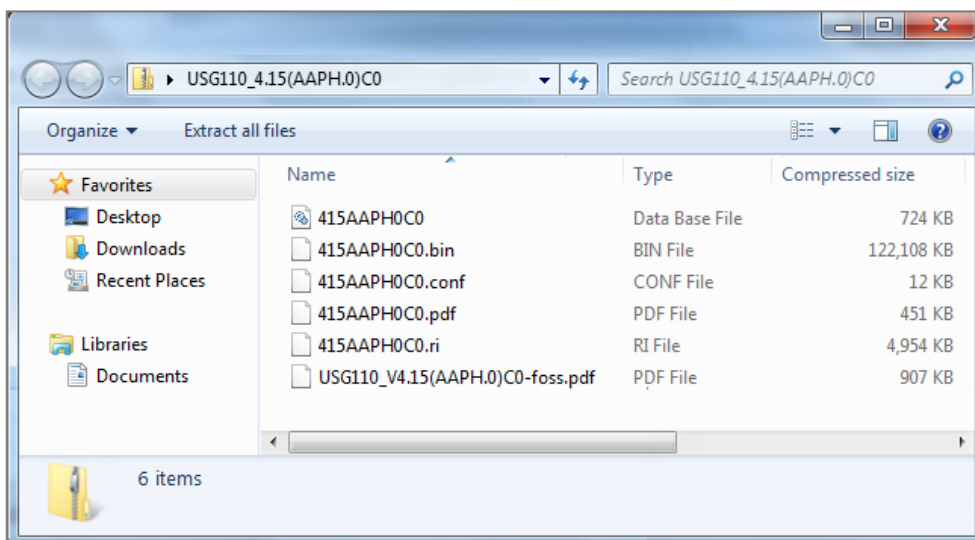
 How to Find Model Number

| ALL | Technical Documentation | Datasheet | Firmware | MIB File | Certification |
|--------------------|-------------------------|-----------|--------------|--------------|---------------|
| Material | Version | Checksum | Release Date | Release Note | Download |
| Firmware | 4.15(AAPH.0)C0 | | Mar 25, 2016 | | |
| 3G Dongle Document | 3 | | Mar 26, 2015 | | |

Extract firmware zip file.



USG110_4.15(AAPH.0)C0.zip



Upload the Firmware on the ZyWALL/USG

In the ZyWALL/USG, go to **MAINTENANCE > File Manager > Firmware Package > Upload File**. Click the **To upload image file in system space** pull-down menu and select (1) or (2). The default **Standby** system space is (2), so if you want to upload new firmware to be the **Running** firmware, then select the **Running** system space

(1). The ZyWALL/USG will reboot automatically.

If you upload firmware to the **Standby** system space (2), you have the option to select **Reboot now** or **Don't Reboot**.

MAINTENANCE > File Manager > Firmware Package > Upload File > (1)

Firmware Status

Reboot now

| # | Status | Model | Version | Released Date |
|---|---------|--------|------------------------------|---------------------|
| 1 | Running | USG110 | V4.13(AAPH.1)ITS-WK41-r64509 | 2015-10-13 23:09:45 |
| 2 | Standby | USG110 | V4.11(AAPH.2) | 2015-04-20 20:41:35 |

Page 1 of 1 | Show 50 items | Displaying 1 - 2 of 2

Upload File

To upload image file in system space: 1

Reboot now
 Don't Reboot

To upload firmware, browse to the location of the file (*.bin) and then click Upload.

File Path: C:\fakepath\415AAPH0C0.bin Browse... Upload

MAINTENANCE > File Manager > Firmware Package > Upload File > (2)

Firmware Status

Reboot now

| # | Status | Model | Version | Released Date |
|---|---------|--------|------------------------------|---------------------|
| 1 | Running | USG110 | V4.13(AAPH.1)ITS-WK41-r64509 | 2015-10-13 23:09:45 |
| 2 | Standby | USG110 | V4.11(AAPH.2) | 2015-04-20 20:41:35 |

Page 1 of 1 | Show 50 items | Displaying 1 - 2 of 2

Upload File

To upload image file in system space: 2

Reboot now
 Don't Reboot

To upload firmware, browse to the location of the file (*.bin) and then click Upload.

File Path: C:\fakepath\415AAPH0C0.bin Browse... Upload

To upload firmware, click **Browse** to the location of the file (*.bin) and then click **Upload**.

Upload File

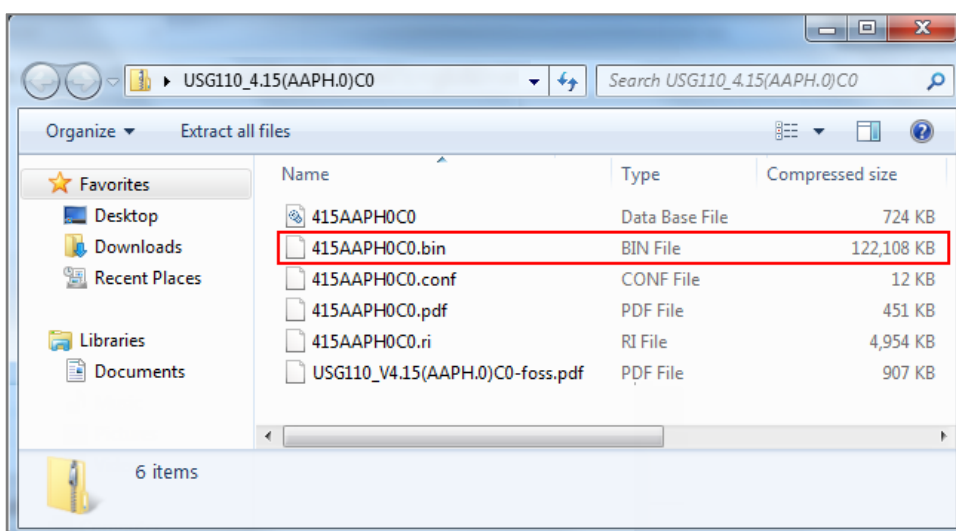
To upload image file in system space: 1

Boot Options

☒ Reboot now
☐ Don't Reboot

To upload firmware, browse to the location of the file (*.bin) and then click Upload.

File Path: Browse... Upload



Upload File

To upload image file in system space: 1

Boot Options

☒ Reboot now
☐ Don't Reboot

To upload firmware, browse to the location of the file (*.bin) and then click Upload.

File Path: Browse... Upload

Note: The default **Running** system space is (1), the **Standby** system space is (2). If you select the **Standby** firmware and click **Reboot now** or you upload file to **Standby** system space (2) and select **Boot Options** to be **Reboot now**. After reboot process complete, the **Running** system space will be (2). **Standby** system space will be (1).

What Could Go Wrong?

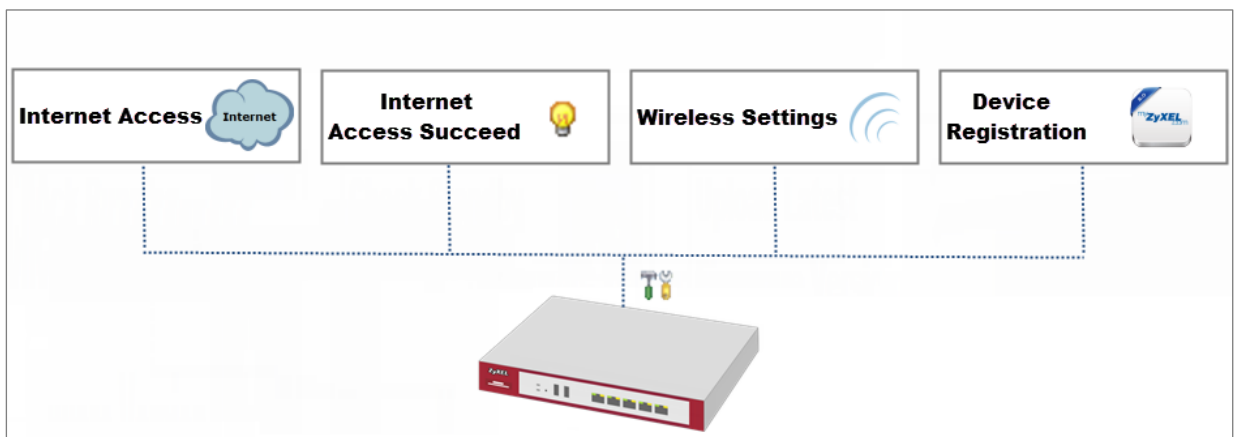
If you cannot download the firmware, please check if you enable the **Destroy compressed files that could not be decompressed** function in **Anti-Virus**.


ZyWALL/USG firmware package is ZIP file, the ZyWALL/USG classifies the firmware package as not being able to decompress will delete it. Please disable this option while downloading the firmware package.

How to Get Started Using the Wizards

When you log into the Web Configurator for the first time or when you reset the ZyWALL/USG to its default configuration, the **Installation Setup Wizard** screen displays. This is an example of using ZyWALL/USG Wizards to configure Internet connection settings, wireless settings and device registration services.

ZyWALL/USG with Installation Setup Wizard Example



 Note: You need internet access to activate your ZyWALL/USG subscription services. This example was tested using USG310 (Firmware Version: ZLD 4.25).

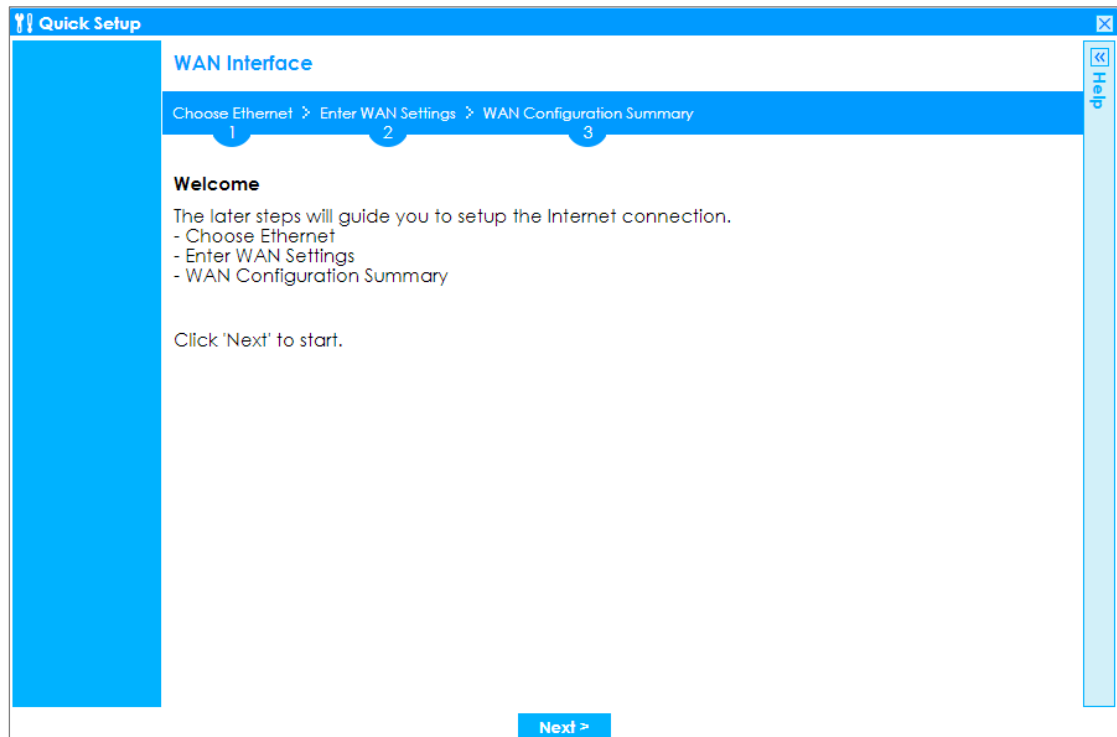
Set Up the Internet Access (Ethernet) Wizard on the

ZyWALL/USG

In the ZyWALL/USG **Installation Setup Wizard** Welcome page, click **Next** to start configuring. Click the double arrow in the upper right corner to display (<<

) or hide (>>) the help.

Installation Setup Wizard > Welcome



In the **Internet Access** page, you can configure Internet connections from two

Internet service providers (ISPs). Connect your ISP devices to your ZyWALL/USG WAN port, select **I have two ISPs** if you want to configure two Internet connections or leave it cleared to configure just one.

Choose the **Encapsulation** option to be **Ethernet**, leave **Zone** as default setting Internet connection belongs to the WAN zone.

In the **IP Address Assignment** section, select **Auto** if your ISP did not assign you a fixed IP address or select **Static** if your ISP did assign you a fixed IP address. Click **Next**.

Installation Setup Wizard > Welcome > Internet Access

The figure consists of three screenshots of the ZyXEL Quick Setup wizard, showing the progression through the WAN Interface configuration steps.

Screenshot 1: The 'WAN Interface' section is active. The breadcrumb trail shows 'Choose Ethernet' (1), 'Enter WAN Settings' (2), and 'WAN Configuration Summary' (3). Under the 'Ethernet' section, the 'Ethernet Selection' dropdown is set to 'ge1'.

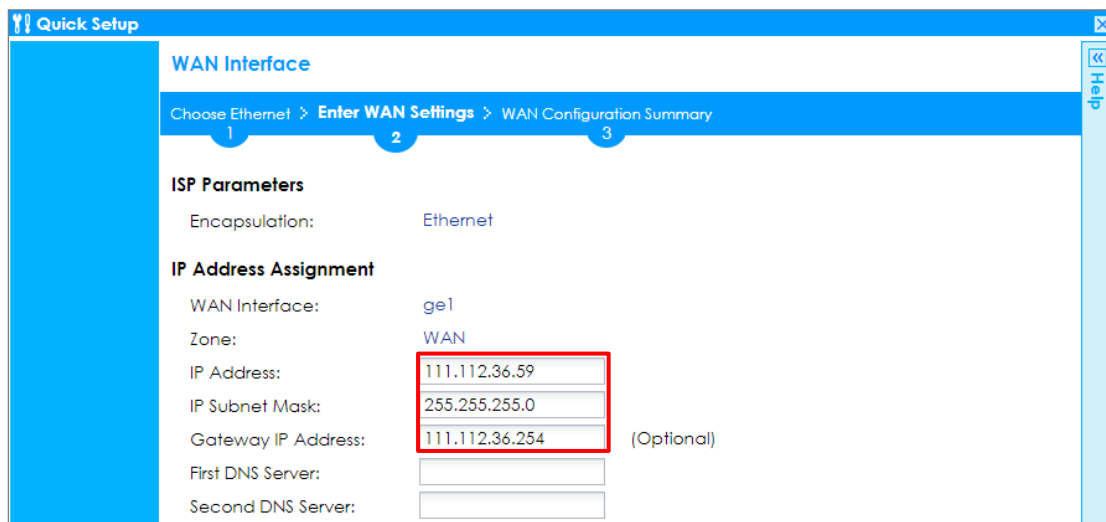
Screenshot 2: The 'IP Address Assignment' section is active. The breadcrumb trail remains the same. Under the 'IP Address Assignment' section, the 'WAN Type Selection' dropdown is set to 'Ethernet'.

Screenshot 3: The 'Interface' section is active. The breadcrumb trail remains the same. Under the 'Interface' section, the 'WAN Interface' is 'ge1', the 'Zone' is 'WAN', and the 'IP Address Assignment' dropdown is set to 'Static' (highlighted with a red box).

Enter the **IP Address**, **IP Subnet Mask** and **Gateway IP Address** exactly as given by

your ISP or network administrator. First/Second DNS Servers are optional. Click **Next**.

Installation Setup Wizard > Welcome > Internet Access



Quick Setup

WAN Interface

Choose Ethernet > **Enter WAN Settings** > WAN Configuration Summary

1 2 3

ISP Parameters

Encapsulation: Ethernet

IP Address Assignment

WAN Interface: ge1

Zone: WAN

IP Address: 111.112.36.59

IP Subnet Mask: 255.255.255.0

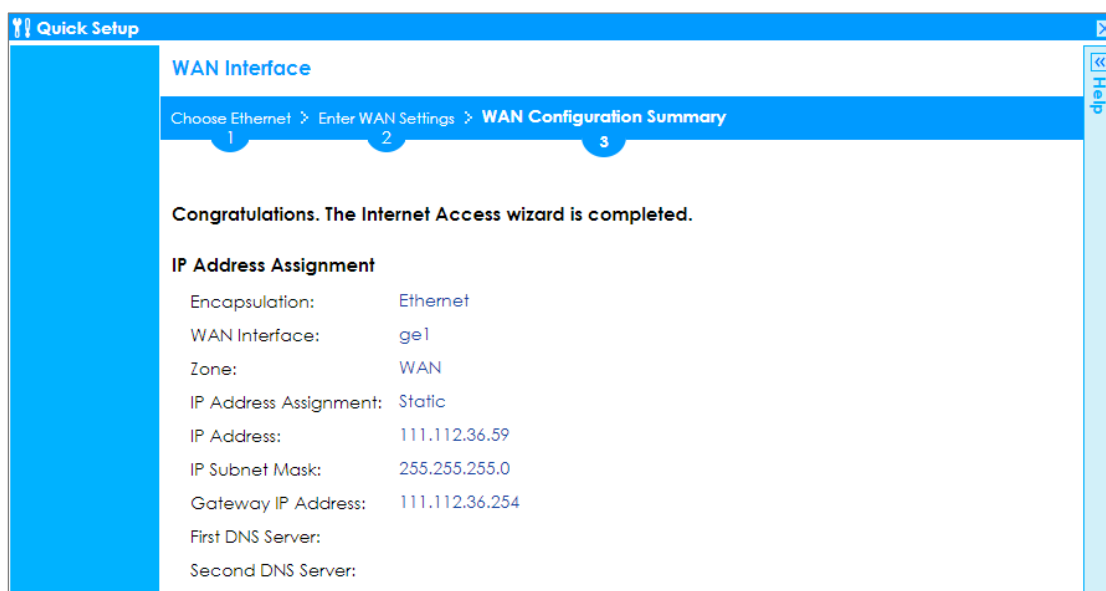
Gateway IP Address: 111.112.36.254 (Optional)

First DNS Server:

Second DNS Server:

The **Internet Access Succeed** page will display the summary of Internet access of the **First Setting**. If you select **I have two ISPs** in **Internet Access > ISP Setting**, click **Next** to configure the second WAN interface or continue to the **Wireless Settings** page.

Installation Setup Wizard > Welcome > Internet Access > Internet Access Succeed



Quick Setup

WAN Interface

Choose Ethernet > Enter WAN Settings > **WAN Configuration Summary**

1 2 3

Congratulations. The Internet Access wizard is completed.

IP Address Assignment

Encapsulation: Ethernet

WAN Interface: ge1

Zone: WAN

IP Address Assignment: Static

IP Address: 111.112.36.59

IP Subnet Mask: 255.255.255.0

Gateway IP Address: 111.112.36.254

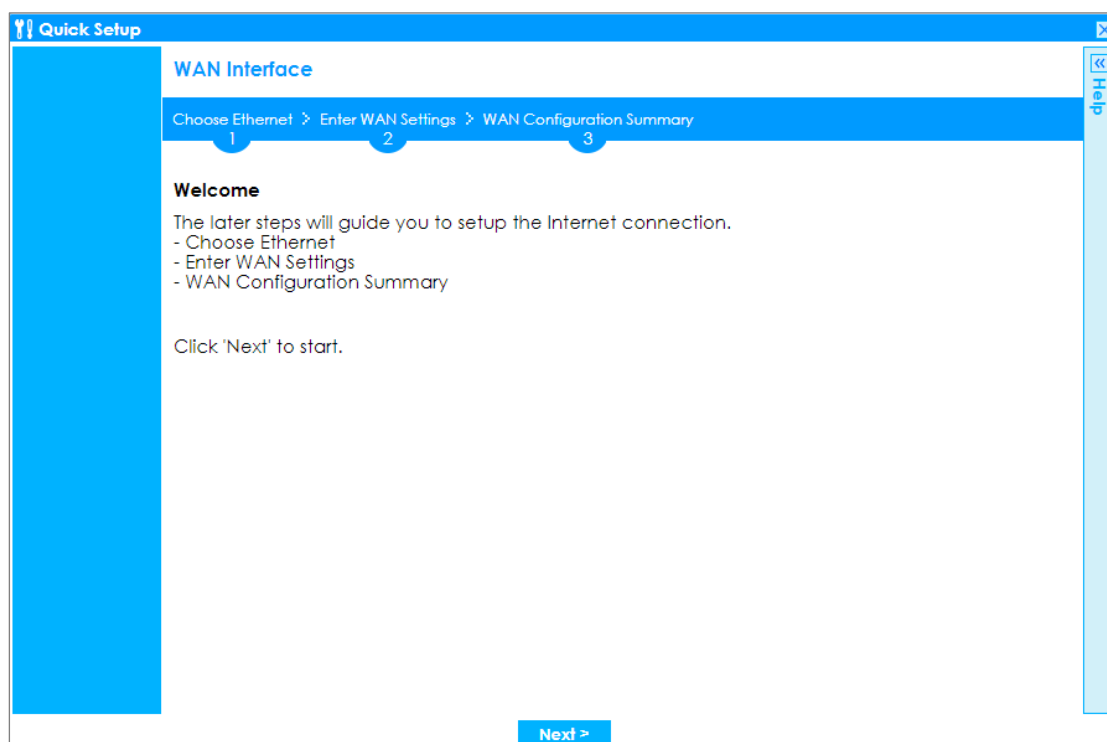
First DNS Server:

Second DNS Server:

Set Up the Internet Access (PPPoE) Wizard on the ZyWALL/USG

In the ZyWALL/USG **Installation Setup Wizard** Welcome page, click **Next** to start configuring for Internet. Click the double arrow in the upper right corner to display (<<) or hide (>>) the help.

Installation Setup Wizard > Welcome



In the **Internet Access** page, you can configure Internet connections from two Internet service providers (ISPs). Connect your ISP devices to your ZyWALL/USG WAN port, select **I have two ISPs** if you want to configure two Internet connections or leave it cleared to configure just one.

Choose the **Encapsulation** option to be **PPP over Ethernet**, leave **Zone** as default setting Internet connection belongs to the WAN zone. Leave the **IP Address**

Assignment section to be the **Auto** and click **Next**.

Installation Setup Wizard > Welcome > Internet Access

Quick Setup

WAN Interface

Choose Ethernet > Enter WAN Settings > WAN Configuration Summary

1 2 3

Ethernet

Ethernet Selection:

Quick Setup

WAN Interface

Choose Ethernet > Enter WAN Settings > WAN Configuration Summary

1 2 3

IP Address Assignment

WAN Type Selection:

Quick Setup

WAN Interface

Choose Ethernet > Enter WAN Settings > WAN Configuration Summary

1 2 3

Interface

WAN Interface:

Zone:

IP Address Assignment:

Select the **Authentication Type** to be the authentication method by the remote node. Enter the **User Name** and **Password** exactly as given by your ISP or network administrator. Select **Nailed-UP** if you want to keep the connection always up or type the desired **Idle Timeout** value in seconds. Click **Next**.

Installation Setup Wizard > Welcome > Internet Access

Quick Setup

WAN Interface

Choose Ethernet > **Enter WAN Settings** > WAN Configuration Summary

1 2 3

ISP Parameters

Encapsulation: PPPoE

Service Name: (Optional)

Authentication Type: Chap/PAP

User Name : ZYXEL_PPPoE

Password:

Retype to Confirm:

☒ Nailed-Up

Idle timeout: 100 Seconds

IP Address Assignment

WAN Interface: ge1_ppp

Zone: WAN

IP Address: Auto

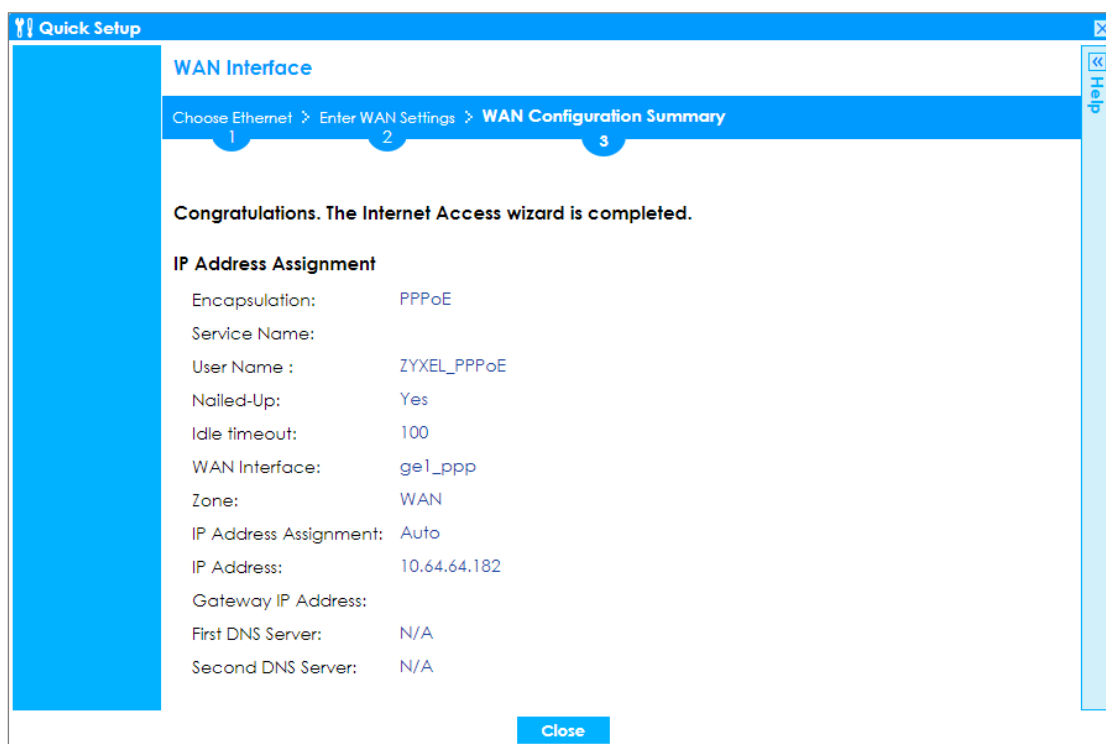
Note

Configure PPPoE will change ethernet interface ip address as 0.0.0.0.

< Back Next >

The **Internet Access Succeed** page will display the summary of Internet access of the **First Setting**. If you select **I have two ISPs** in **Internet Access > ISP Setting**, click **Next** to configure the second WAN interface.

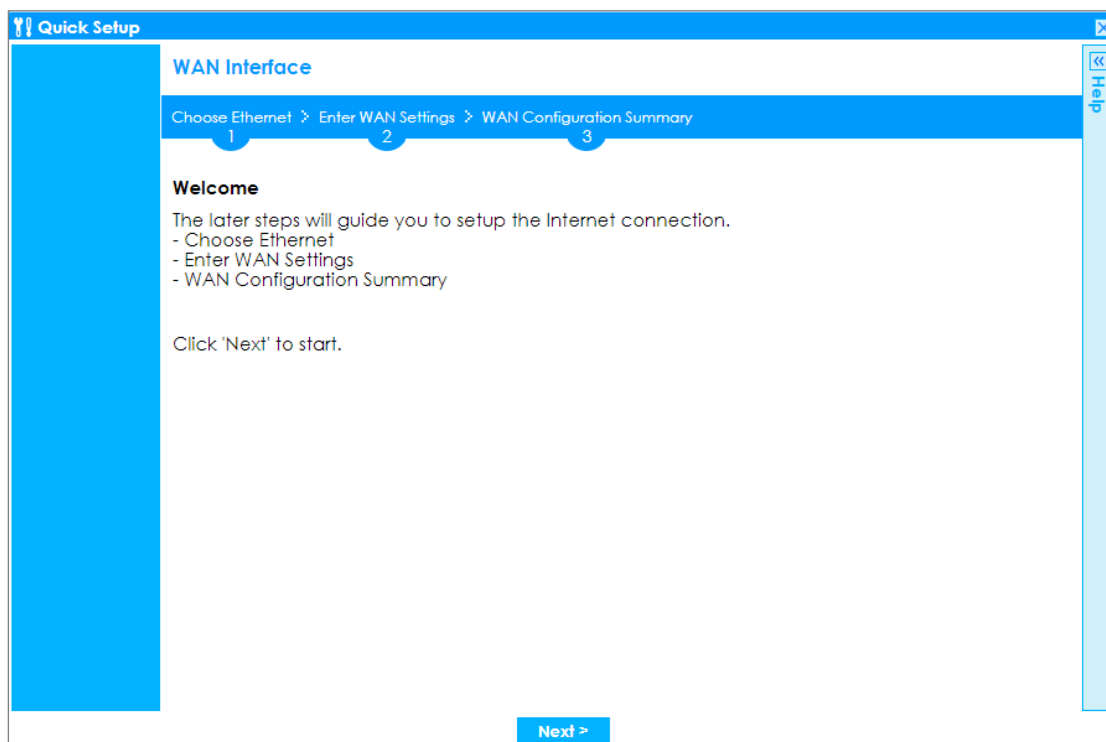
Installation Setup Wizard > Welcome > Internet Access > Internet Access Succeed



Set Up the Internet Access (PPTP) Wizard on the ZyWALL/USG

In the ZyWALL/USG **Installation Setup Wizard** Welcome page, click **Next** to start configuring for Internet. Click the double arrow in the upper right corner to display (<<) or hide (>>) the help.

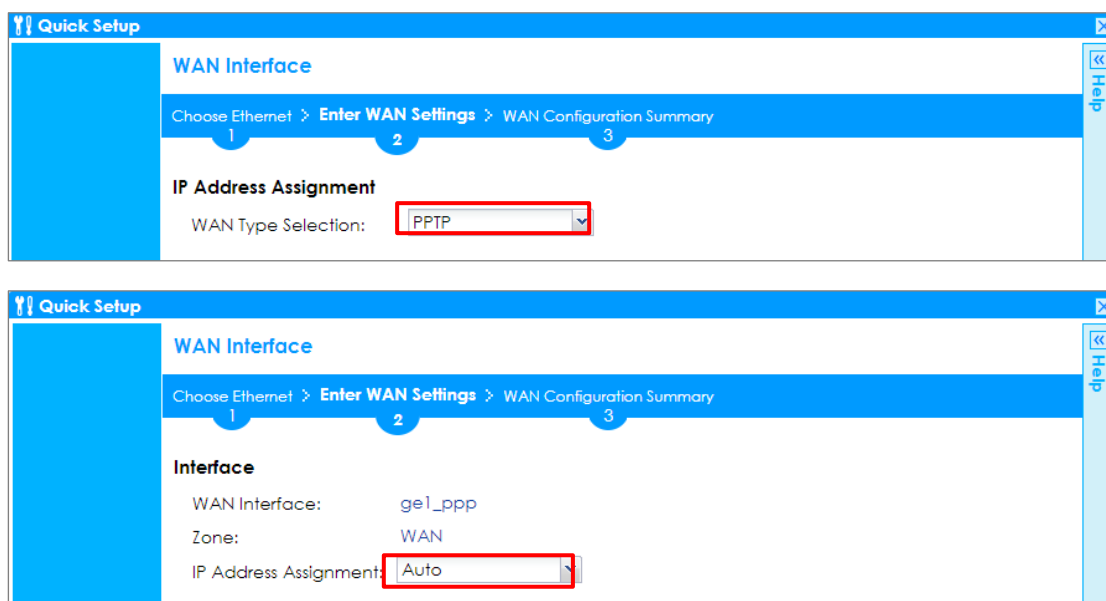
Installation Setup Wizard > Welcome



In the **Internet Access** page, you can configure Internet connections from two Internet service providers (ISPs). Connect your ISP devices to your ZyWALL/USG WAN port, select **I have two ISPs** if you want to configure two Internet connections or leave it cleared to configure just one.

Choose the **Encapsulation** option to be the **PPTP**, leave **Zone** as default setting Internet connection belongs to the WAN zone. Leave the **IP Address Assignment** section to be the **Auto** and click **Next**.

Installation Setup Wizard > Welcome > Internet Access



Quick Setup

WAN Interface

Choose Ethernet > **Enter WAN Settings** > WAN Configuration Summary

1 2 3

IP Address Assignment

WAN Type Selection: PPTP

Quick Setup

WAN Interface

Choose Ethernet > **Enter WAN Settings** > WAN Configuration Summary

1 2 3

Interface

WAN Interface: gel_ppp

Zone: WAN

IP Address Assignment: Auto

Select the **Authentication Type** to be the authentication method by the remote node. Enter the **User Name** and **Password** exactly as given by your ISP or network administrator. Select **Nailed-UP** if you want to keep the connection always up or type the desired **Idle Timeout** value in seconds. Click **Next**.

Enter the **Base IP Address**, **IP Subnet Mask**, **Gateway IP Address** assigned to you by your ISP. Type the **Server IP** address of the **PPTP Server**. Click **Next**.

Installation Setup Wizard > Welcome > Internet Access

Quick Setup

WAN Interface

Choose Ethernet > **Enter WAN Settings** > WAN Configuration Summary

1 2 3

ISP Parameters

Encapsulation: PPTP

Authentication Type: Chap/PAP

User Name : ZYXEL_PPTP

Password:

Retype to Confirm:

☐ Nailed-Up

Idle timeout: 100 Seconds

PPTP Configuration

Base Interface: ge1

Base IP Address: 111.111.36.99

IP Subnet Mask: 255.255.255.0

Gateway IP Address: 111.111.36.254 (Optional)

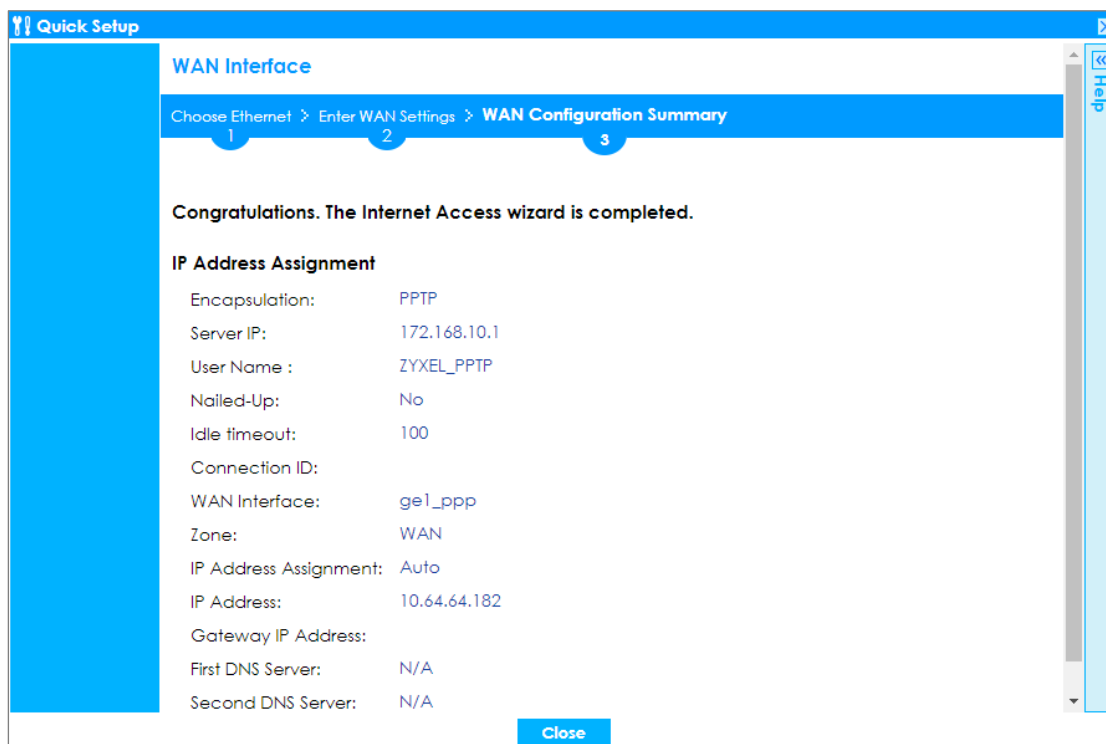
Server IP: 172.168.10.1 (Optional)

Connection ID: (Optional)

< Back Next >

The **Internet Access Succeed** page will display the summary of Internet access of the **First Setting**. If you select **I have two ISPs** in **Internet Access > ISP Setting**, click **Next** to configure the second WAN interface.

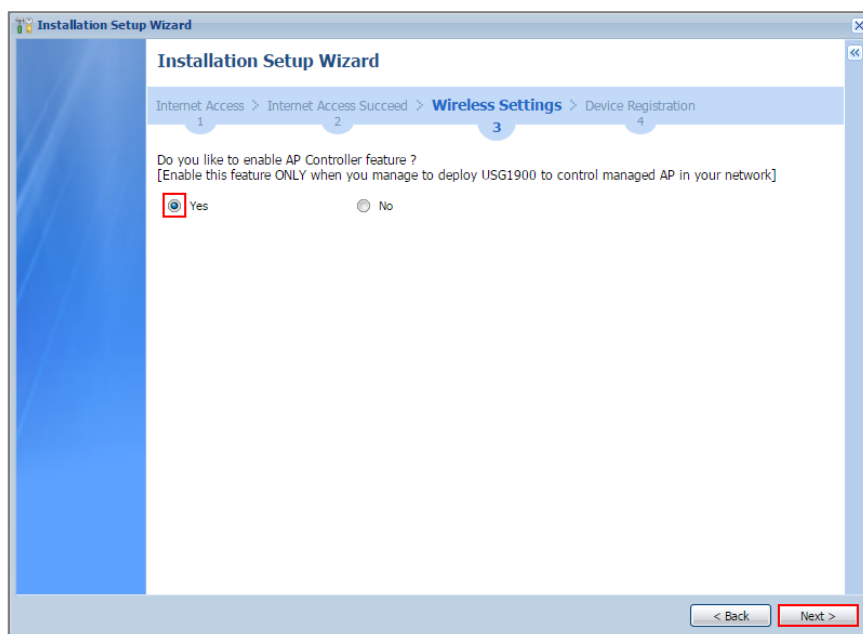
Installation Setup Wizard > Welcome > Internet Access > Internet Access Succeed



Set Up the Wireless Settings Wizard on the ZyWALL/USG

In the **Wireless Settings** page, select **Yes** if you want the ZyWALL/USG to enable AP Controller feature in your network; select **No** if you want to skip this setting. Click **Next**.

Installation Setup Wizard > Welcome > Internet Access > Internet Access Succeed > Wireless Settings



Configure descriptive **SSID** name (1-32 characters) for the wireless LAN. Select **Pre-Shared Key** (8-63 characters) to add security on this wireless network. Otherwise, select **None** to allow any wireless client to associate this network without authentication.

Select **Hidden SSID** to hide the SSID from site tool scanning.

Select **Enable Intra-BSS Traffic blocking** if you want to prevent crossover traffic from within the same wireless network. Wireless clients in that network can still access the wired network but cannot communicate with each other.

For Built-in Wireless AP only, ZyWALL/USGs with **W** in the model name have a built-in AP. Select an interface to bridge with the built-in AP wireless network. Devices connected to this interface will then be in the same broadcast domain as devices

in the AP wireless network.

**Installation Setup Wizard > Welcome > Internet Access > Internet Access Succeed
> Wireless Settings**

Installation Setup Wizard

Internet Access > Internet Access Succeed > **Wireless Settings** > Device Registration

Wireless Settings

SSID Setting

SSID:

Security Mode

☒ Pre-Shared Key

☐ None

☐ Hidden SSID

☒ Enable Intra-BSS Traffic blocking

For Built-in Wireless AP Only

Bridged to:

< Back Next >

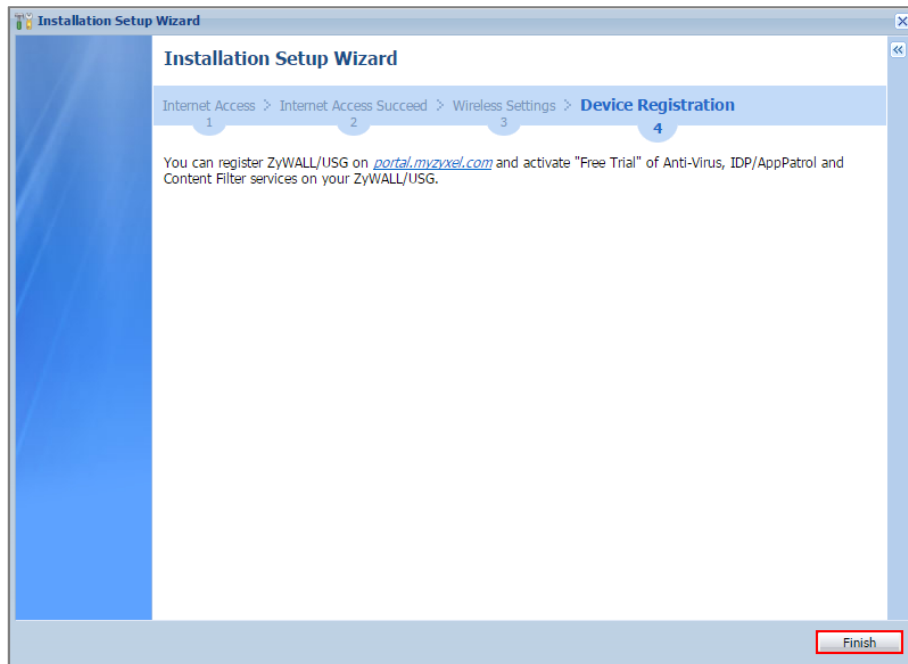
Set Up the Device Registration on the ZyWALL/USG

The ZyWALL/USG must be connected to the Internet in order to register.

Click **portal.myzyxel.com** to register the device, you need the ZyWALL/USG's serial number and LAN MAC address to register it. See **How To Register Your Device and**

Services at myZyXEL.com for more details. Use the **Configuration > Licensing > Registration > Service** screen to update your service subscription status. Click **Finish**.

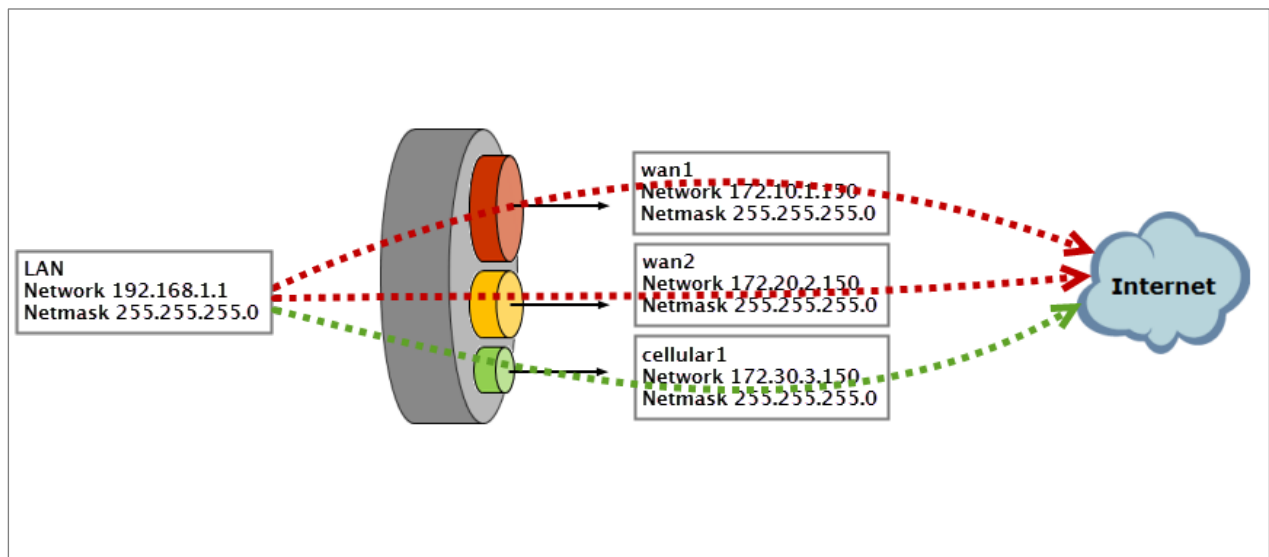
Installation Setup Wizard > Welcome > Internet Access > Internet Access Succeed > Wireless Settings > Device Registration




How to Configure the 3G/LTE Interface on the ZyWALL/USG as a WAN Backup

This is an example of using ZyWALL/USG to configure 3G/LTE interface as a WAN backup that ensures the ZyWALL/USG provides the continuously Internet connections when the primary WAN interface is down. After configuration, it can provide additional mobile broadband WAN connectivity or a redundant link for maximum reliability.

ZyWALL/USG with 3G/LTE Interface as a WAN Backup Example



 **Note:** This example includes weighted load balancing (Weighted Round Robin) so that most of your Internet traffic is handled by ISP connected to wan1 before it fails over to 3G/LTE.

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the 3G/LTE Interface on the ZyWALL/USG

Connect a compatible mobile broadband USB device to use a cellular connection.

In the ZyWALL/USG, go to **CONFIGURATION > Network > Interface > Cellular**, the connected device will automatically display in the **Cellular Interface Summary**. Click **Activate** and then the **Apply** button at the bottom of this page.

CONFIGURATION > Network > Interface > Cellular > Activate

| Add Edit Remove Activate Inactivate Connect Disconnect Object References | | | | | |
|--|--------|-----------|----------------|------------------|------------------|
| # | Status | Name | Extension Slot | Connected Device | ISP Settings |
| 1 | | cellular1 | USB 1 | Huawei E3131 | Device Profile 1 |
| << Page 1 of 1 >> Show 50 items Displaying 1 - 1 of 1 | | | | | |

The default **Connectivity** method is **Nailed-Up**. The connection should always be up after you activate the cellular interface. You can click **Edit** and go to the **Connectivity** section to clear the **Nailed-Up** check box to have the ZyWALL/USG to establish the connection only when there is traffic.

CONFIGURATION > Network > Interface > Cellular > Connect

| Add Edit Remove Activate Inactivate Connect Disconnect Object References | | | | | |
|--|--------|-----------|----------------|------------------|--------------|
| # | Status | Name | Extension Slot | Connected Device | ISP Settings |
| 1 | | cellular1 | USB 1 | Huawei E156G | |
| << Page 1 of 1 >> Show 50 items Displaying 1 - 1 of 1 | | | | | |

CONFIGURATION > Network > Interface > Cellular > Edit

| Connectivity | |
|-------------------------------------|-----------|
| <input checked="" type="checkbox"/> | Nailed-Up |

Set Up the Trunk on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > Interface > Trunk > User Configuration > Add Trunk**, configure a **Name** for you to identify the Trunk profile and set the **Load Balancing Algorithm** field to be the **Weighted Round Robin**.

Add **wan1** and enter **3** in the **Weight** column. Add **wan2** and enter **2** in the **Weight** column. Add **cellular1**, change **Mode** to be the **Passive** mode, enter **1** in the **Weight** column. Click **OK** to return to the **Configuration** screen.

CONFIGURATION > Network > Interface > Trunk > User Configuration > Add Trunk

Edit WAN_backup

Name: WAN_backup

Load Balancing Algorithm: Weighted Round Robin

| # | Member | Mode | Weight |
|---|-----------|---------|--------|
| 1 | ge1 | Active | 1 |
| 2 | cellular1 | Passive | 0 |
| 3 | ge2 | Active | 2 |

Page 1 of 1 | Show 50 items | Displaying 1 - 3 of 3

In the **Configuration** screen, go to **Default WAN Trunk** section, select **User Configured Trunk** and select the newly created Trunk from the list box. Click **Apply**.


CONFIGURATION > Network > Interface > Trunk > Default WAN Trunk > User Configured Trunk

Default WAN Trunk

☐ Advance

Default Trunk Selection

☐ SYSTEM_DEFAULT_WAN_TRUNK
 ☒ User Configured Trunk

WAN_Backup
 

Test the Result

Check the **Interface Statistics** when wan1 and wan2 connections are up. You can see both wan1 and wan2 **Status** are up, **Tx B/s** displays the transmission speed and **Rx B/s** displays the reception speed; cellular1 **Status** is connected but there is no traffic going through this interface.

MONITOR > Interface Status > Interface Statistics

Interface Statistics

Refresh

| Name | Status | TxPkts | RxPkts | Tx B/s | Rx B/s |
|-----------|------------|--------|---------|--------|--------|
| wan1 | 1000M/Full | 359860 | 1314443 | 2587 | 1152 |
| wan2 | 100M/Full | 2438 | 23927 | 192 | 64 |
| ge3 | Down | 0 | 0 | 0 | 0 |
| ge4 | Down | 0 | 0 | 0 | 0 |
| ge5 | Down | 0 | 0 | 0 | 0 |
| ge6 | Down | 0 | 0 | 0 | 0 |
| ge7 | Down | 0 | 0 | 0 | 0 |
| ge8 | Down | 0 | 0 | 0 | 0 |
| cellular1 | Connected | 0 | 0 | 0 | 0 |

After disconnecting both wan1 and wan2, you can see both wan1 and wan2 **Status** are **Down** and no traffic goes through these two interfaces. The backup cellular1 **Status** is connected and all the traffic is going through this interface.

MONITOR > Interface Status > Interface Statistics

| Interface Statistics | | | | | |
|----------------------|----------------------|--------|--------|--------|--------|
| Refresh | | | | | |
| Name | Status | TxPkts | RxPkts | Tx B/s | Rx B/s |
| + ge1 | Down | 0 | 0 | 0 | 0 |
| + ge2 | 1000M/Full | 6764 | 35208 | 0 | 0 |
| + ge3 | Down | 1 | 0 | 0 | 0 |
| + ge4 | Down | 2 | 0 | 0 | 0 |
| + ge5 | Down | 1 | 0 | 0 | 0 |
| + ge6 | Down | 2 | 0 | 0 | 0 |
| + ge7 | Down | 1 | 0 | 0 | 0 |
| + ge8 | Down | 1 | 0 | 0 | 0 |
| + cellular1 | Connected (00:10:34) | 164 | 119 | 0 | 0 |

What Could Go Wrong?

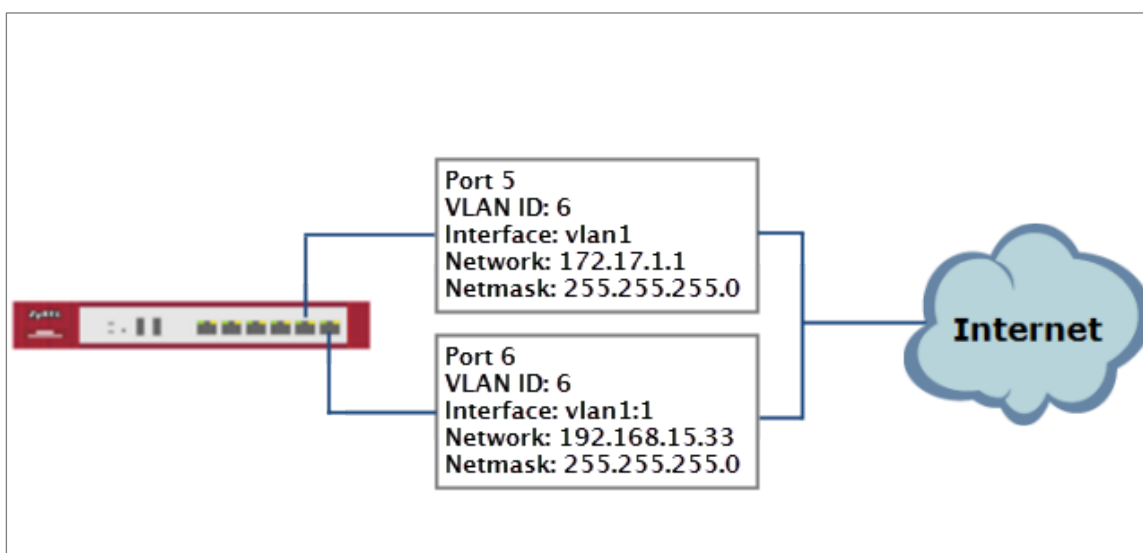
If there is no traffic going through cellular interface when other interfaces are down, please make sure you have a compatible mobile broadband device installed or connected. Go to


http://www.zyxel.com/support/download_landing.shtml and see the **3G Dongle Document** to check the compatible mobile broadband devices. Also, make sure the cellular interface is enabled and the cellular interface has the correct user name, password, and PIN code configured with the correct casing.

How to Configure Two Different WAN Interfaces with Different IP Addresses in the Same VLAN

This is an example of using ZyWALL/USG to configure two different WAN interfaces with different IP addresses in the same VLAN. After configuration, you can have the same VLAN ID for two different WAN interfaces.

ZyWALL/USG with Two Different WAN Interfaces with Different IP Addresses in the Same VLAN Example

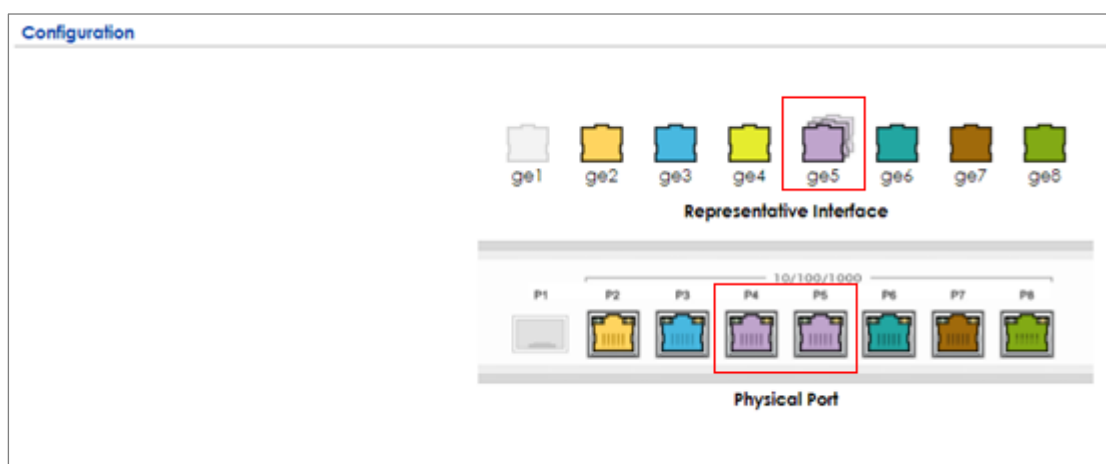


 Note: This example requires the ZyWALL/USG models which can apply port grouping. All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using ZyWALL USG300 (Firmware Version: ZLD 4.25).

Set Up the Port Grouping on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > Interface > Port Grouping**, select the ports that you want to assign to a representative Interface (in this example, **Port 4** and **Port 5** are configured as **ge5**).

CONFIGURATION > Network > Interface > Port Grouping



Set Up the VLAN on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > Interface > VLAN**. Set **Interface Type** to be **External**. Set **Zone** to be **WAN**, configure **Base Port** to be **ge5**. Enter the **VLAN ID** and configure the fixed IP address (172.17.1.1/24 in this example). Click **OK** to go back to the **Configuration** page.

CONFIGURATION > Network > Interface > VLAN

General Settings

☒ Enable Interface

Interface Properties

Interface Type: external
Interface Name: vlan1
Zone: none
Base Port: ge5
VLAN ID: 1 (1-4094)
☒ Advance
Description: (Optional)

IP Address Assignment

☐ Get Automatically
☒ Advance
☒ Use Fixed IP Address
IP Address: 172.17.1.1
Subnet Mask: 255.255.255.0
Gateway: 172.17.1.254 (Optional)
Metric: 0 (0-15)

In the **Configuration** page, select the **vlan1** entry and click **Create Virtual Interface** on the upper bar. Configure the Fixed IP address (192.168.15.33 in this example). Click **OK**.

CONFIGURATION > Network > Interface > VLAN > vlan1

| Configuration | | | | | |
|---|--------|-------|----------|-------------------|---------------|
| <div> Add Edit Remove Activate Inactivate Create Virtual Interface Object References </div> | | | | | |
| # | Status | Name | Port/VID | IP Address | Mask |
| 1 | | vlan1 | ge5/1 | static-172.17.1.1 | 255.255.255.0 |
| Page 1 of 1 Show 50 items | | | | | |

CONFIGURATION > Network > Interface > VLAN > vlan1:1

Interface Properties

Interface Name: vlan1:1
Description: (Optional)

IP Address Assignment

IP Address: 192.168.15.33
Subnet Mask: 255.255.255.0
Gateway: 192.168.15.1 (Optional)
Metric: 0 (0..15)

Set Up the Routing on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > Routing**, set **Next-Hop Type** to be **Interface** and set **Interface** to be the **vlan1**.

CONFIGURATION > Network > Routing

| Configuration | |
|--|-------------------------|
| <input checked="" type="checkbox"/> Enable | |
| Description: | Vlan_Routing (Optional) |
| Criteria | |
| User: | any |
| Incoming: | any (Excluding ZyV) |
| Source Address: | any |
| Destination Address: | any |
| DSCP Code: | any |
| Schedule: | none |
| Service: | any |
| Next-Hop | |
| Type: | Interface |
| Interface: | vlan1 |

Test the Result

Check the **Interface Statistics**, you can see **vlan1 Status** is up, **Tx B/s** displays the transmission speed and **Rx B/s** displays the reception speed. Port 5 and Port 6 are configured in the same **vlan1** but use different IP addresses.

MONITOR > Interface Status > Interface Statistics



| Interface Statistics | | | | | |
|------------------------------|------------|--------|--------|--------|--------|
| Refresh | | | | | |
| Name | Status | TxPkts | RxPkts | Tx B/s | Rx B/s |
| <input type="checkbox"/> ge1 | Down | 0 | 0 | 0 | 0 |
| <input type="checkbox"/> ge2 | 1000M/Full | 9269 | 14934 | 0 | 94 |
| <input type="checkbox"/> ge3 | Down | 2 | 0 | 0 | 0 |
| <input type="checkbox"/> ge4 | Down | 12951 | 11412 | 0 | 0 |
| <input type="checkbox"/> ge5 | Up | 2150 | 2117 | 16803 | 1901 |
| - vlan1 | Up | 326 | 0 | 42 | 0 |
| - ge5_ppp | Inactive | | | 0 | 0 |
| <input type="checkbox"/> ge6 | Down | 4 | 0 | 0 | 0 |
| <input type="checkbox"/> ge7 | Down | 2 | 0 | 0 | 0 |
| <input type="checkbox"/> ge8 | Down | 1 | 0 | 0 | 0 |

What Could Go Wrong?

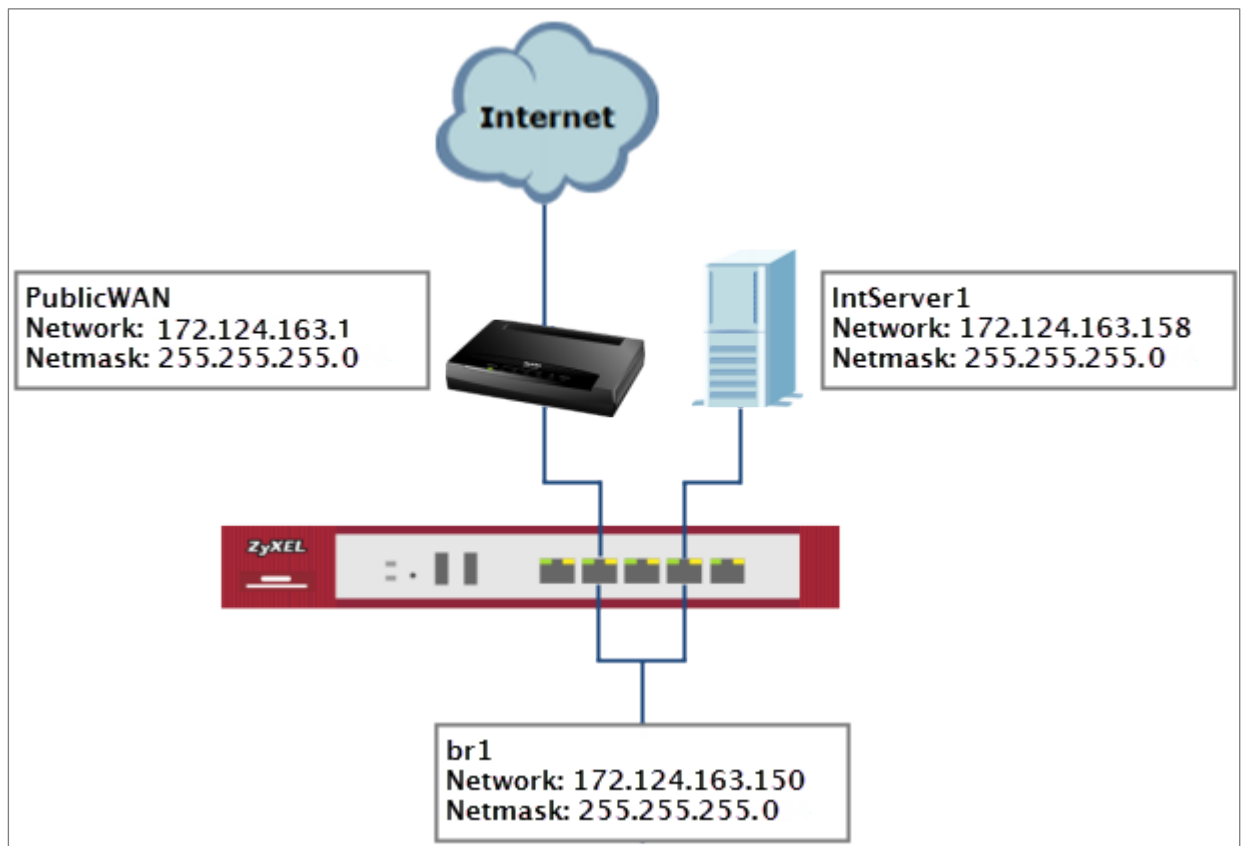
If you cannot configure a particular VLAN interface on top of an Ethernet interface, please whether this VLAN has just been created on top of other Ethernet interface.


How to Let a Server Use the Same Public IP Address as the WAN Interface Using the Bridge Interface

This is an example of using ZyWALL/USG to configure an internal server in bridge mode without applying network address translation (NAT). The Internet users can

reach this server directly by its public IP address.

ZyWALL/USG with Bridge Interface Example



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the Bridge Interface on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > Interface > Bridge > add**

Bridge, select **Interface Type** to be the **general** type, select **Zone** to be the **LAN** zone. In the **Member Configuration**, select internal server (**IntServer1** interface in this example) and public IP address (**Public WAN** interface in this example) to be in the same member group.

In the **IP Address Assignment** section, select **Used Fixed IP Address** and configure br1 IP address (172.124.163.150/24 in this example).

CONFIGURATION > Network > Interface > Bridge > add Bridge

General Settings

☒ Enable Interface

Interface Properties

Interface Type:

general

Interface Name:

br1

Zone:

LAN

Description:

(Optional)

Member Configuration

| Available | | Member |
|------------|---|--------|
| ge1 | | |
| ge2 | | |
| ge3 | | |
| ge4 | | |
| ge5 | | |
| ge6 | | |
| IntServer1 | + | |
| PublicWAN | + | |

IP Address Assignment

☐ Get Automatically

☒ Use Fixed IP Address

☒ Advance

IP Address:

172.124.163.150

Subnet Mask:

255.255.255.0

Gateway:

172.124.163.129

(Optional)

Metric:

0

(0-15)

After creating the bridge interface, connect the server's network cable to **IntServer1** port and set the server's IP to be in the same subnet (172.124.163.158 in this example).

Test the Result

Check the **Interface Statistics**, you can see br1 **Status** is up, **Tx B/s** displays the transmission speed and **Rx B/s** displays the reception speed. **IntServer1** and **PublicWAN** are configured in the same vlan1 but using different IP address.

MONITOR > Interface Status > Interface Statistics

| Interface Statistics | | | | | |
|----------------------|------------|--------|--------|--------|--------|
| Refresh | | | | | |
| Name | Status | TxPkts | RxPkts | Tx B/s | Rx B/s |
| ge1 | Down | 0 | 0 | 0 | 0 |
| ge2 | 1000M/Full | 9877 | 17204 | 0 | 0 |
| ge3 | Down | 2 | 0 | 0 | 0 |
| ge4 | 1000M/Full | 13950 | 13611 | 0 | 0 |
| ge5 | Down | 2434 | 2372 | 0 | 0 |
| ge6 | Down | 4 | 0 | 0 | 0 |
| IntServer1 | Down | 1329 | 1120 | 0 | 0 |
| PublicWAN | 1000M/Full | 1135 | 1320 | 0 | 0 |
| br1 | Up | 14 | 618 | 0 | 0 |

Server can access Internet successfully by using its IP address (172.124.163.158 in this example) and Internet users can also reach this server by this public address as well.

Windows 7 > cmd > ping 172.124.163.158

```
C:\Documents and Settings\ZyXEL-CS0>ping 172.124.163.158

Pinging 172.124.163.158 with 32 bytes of data:

Reply from 172.124.163.158: bytes=32 time=37ms TTL=44
Reply from 172.124.163.158: bytes=32 time=26ms TTL=44
Reply from 172.124.163.158: bytes=32 time=32ms TTL=44
Reply from 172.124.163.158: bytes=32 time=22ms TTL=44

Ping statistics for 172.124.163.158:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

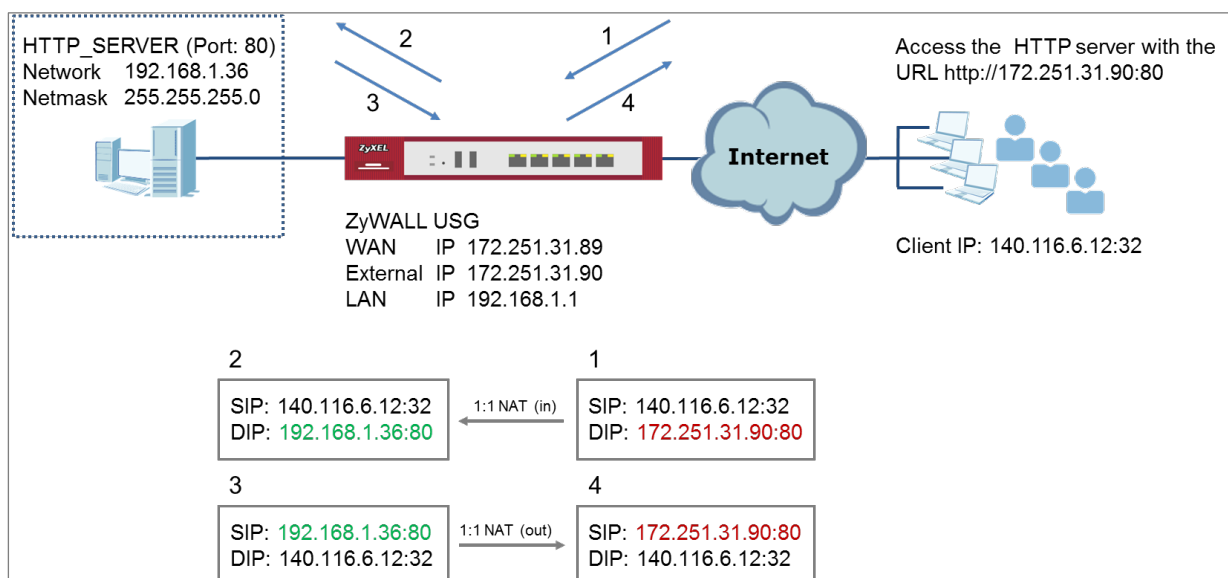

What Could Go Wrong?

If you cannot configure a particular bridge IP address, please check if this IP address already created on other Ethernet interface.

How to Allow Public Access to a Server Behind ZyWALL/USG

This is an example of using ZyWALL/USG to configure a secure access to internal server behind ZyWALL/USG with network address translation (NAT). The Internet users can reach this server directly by its public IP address and a NAT mapping rule will forward the traffic from the Internet to the Intranet. It provides security and decrease the number of IP addresses an organization needs.

ZyWALL/USG enables Public Access to a Server with NAT



Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the NAT on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > NAT > add NAT**, select **Enable Rule**. Select **1:1 NAT**. Set **Incoming Interface** to be the **wan1** interface. Type **User-Defined Original IP** (172.251.31.90 in this example) and type **User-Defined Mapped IP** (192.168.1.34 in this example). Set **Port Mapping Type** to **Service**, set **Original Service** and **Mapped Service** to **HTTP** in this example. Click **OK**.

CONFIGURATION > Network > NAT > add NAT

| General Settings | |
|---|--|
| <input checked="" type="checkbox"/> Enable Rule | |
| Rule Name: | http_server |
| Port Mapping Type | |
| Classification: | <input type="radio"/> Virtual Server <input checked="" type="radio"/> 1:1 NAT <input type="radio"/> Many 1:1 NAT |
| Mapping Rule | |
| Incoming Interface: | ge1 |
| Original IP: | User Defined |
| User-Defined Original IP: | 172.251.31.90 (IP Address) |
| Mapped IP: | User Defined |
| User-Defined Mapped IP: | 192.168.1.34 (IP Address) |
| Port Mapping Type: | any |

Set Up the Security Policy on the ZyWALL/USG

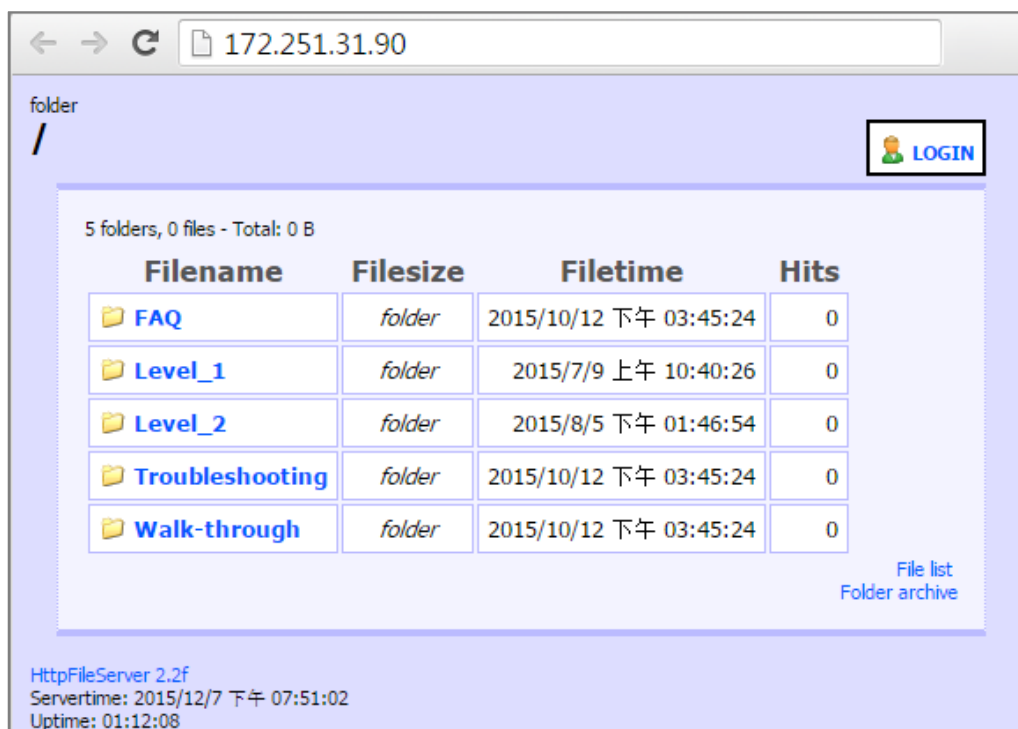
In the ZyWALL/USG, go to **CONFIGURATION > Security Policy > Policy Control > add corresponding**, select **Enable**. Configure a Name for your to identify the security policy (http_server_access in this example). Set **From: WAN** and **To: LAN1**. Set **Destination** to the lan subnet where your server is (LAN_SUBNET_GE3 in this example). Set **Service** to **HTTP**, set **Action** to **allow**. Click **OK**.

CONFIGURATION > Security Policy > Policy Control > add corresponding

| | |
|--|--------------------|
| <input checked="" type="checkbox"/> Enable | |
| Name: | Http_server_access |
| Description: | (Optional) |
| From: | WAN |
| To: | LAN1 |
| Source: | any |
| Destination: | LAN_SUBNET_GE4 |
| Service: | HTTP |
| User: | any |
| Schedule: | none |
| Action: | allow |
| Log matched traffic: | no |

Test the Result

Type <http://172.251.31.90/> into the browser, it displays the HTTP service page.



What Could Go Wrong?

If you cannot access your server via public IP address, please make sure all your public IP addresses are routing properly. To do one by one assign them to the ZyWALL's WAN port. Test to make sure you have internet access with the public IP address.


If you cannot access the ZyWALL from the internet with any IP address on your public IP, this is a routing issue on the service end. Please contact the ISP to fix the

routing for the public IPs.

If you see [notice] log message as below, the HTTPS traffic is blocked by the priority 1 Security Policy. The ZyWALL/USG checks the security policy in order and applies the first security policy the traffic matches. If the HTTPS traffic matches a policy that comes earlier in the list, it may be unexpectedly blocked. Please change your policy setting or move the policy to the higher priority.

Monitor > Log

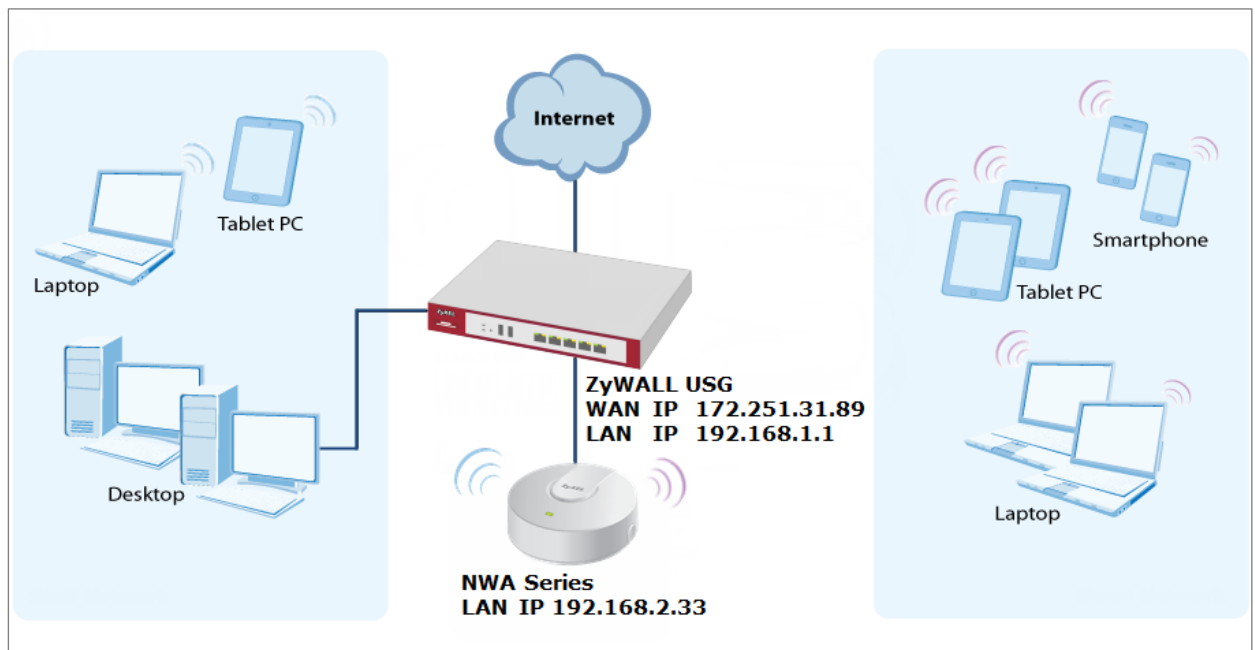
| # ▲ | Priority | Category | Message | Note |
|-----|----------|-------------------------|---|--------------|
| 1 | notice | Security Policy Control | priority:1, from LAN to ANY, TCP, service HTTPS, REJECT [count=3] | ACCESS BLOCK |
| 2 | notice | Security Policy Control | priority:1, from LAN to ANY, TCP, service HTTPS, REJECT [count=3] | ACCESS BLOCK |


 Note: The default setting of **Security Policy** is without log notification (except **PolicyDefault**), if you want to check which policy may potentially block the traffic, please select this policy and set the **Log matched traffic** to be **log** or **log alert**.

How to Set Up a WiFi Network with ZyXEL APs

This is an example of using ZyWALL/USG to manage the Access Points (APs) and allow wireless access to the network.

ZyWALL/USG as AP Controller Example



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the AP Management on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Wireless > Controller > Configuration**, set **Registration Type** to **Manual**. This is recommended as the registration mechanism cannot automatically differentiate between friendly and rogue APs.

CONFIGURATION > Wireless > Controller > Configuration



Controller Setting

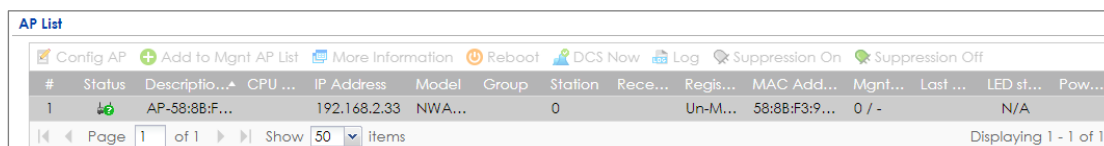
Country Code: Taiwan

Registration Type: ☒ Manual ☐ Always Accept

Connect the ZyXEL AP unit to the lan interface.

Go to **MONITOR > Wireless > AP Information > AP List** and the ZyXEL AP is listed. A green question mark displays in the Status column since the AP is not yet managed by the ZyWALL/USG. Select the listed AP and click **Add to Mgnt AP List** on the upper bar.

Monitor > Wireless > AP Information > AP List



| # | Status | Description | CPU | IP Address | Model | Group | Station | Rece... | Regis... | MAC Add... | Mgnt... | Last ... | LED st... | Pow... |
|---|---------|---------------|-----|--------------|--------|-------|---------|---------|----------|---------------|---------|----------|-----------|--------|
| 1 | Un-M... | AP-58:8B:F... | | 192.168.2.33 | NWA... | | 0 | | Un-M... | 58:8B:F3:9... | 0 / - | | N/A | |



Note: The APs may take few minutes to appear in the AP List.

Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List** to configure a name to identify the **SSID**.

CONFIGURATION > Object > AP Profile > SSID > SSID List

| | | | |
|--|---|----------|---------------------------|
| Profile Name: | default | | |
| SSID: | <div style="border: 1px solid red; padding: 2px;">ZyXEL_API</div> | | |
| Security Profile: | default | ▼ | |
| MAC Filtering Profile: | disable | ▼ | |
| QoS: | WMM | ▼ | |
| Rate Limiting (Per Station Traffic Rate) ⓘ | | | |
| Downlink: | 0 | mbps | ▼ (0~160, 0 is unlimited) |
| Uplink: | 0 | mbps | ▼ (0~160, 0 is unlimited) |
| Band Select: | disable | ▼ | |
| Forwarding Mode: | Local bridge | ▼ | |
| VLAN ID: | 1 | (1~4094) | |
| <input type="checkbox"/> Hidden SSID | | | |
| <input type="checkbox"/> Enable Intra-BSS Traffic blocking | | | |
| <input type="checkbox"/> Schedule SSID ⓘ | | | |

Go to **CONFIGURATION > Object > AP Profile > SSID > Security List** to select the **Security Mode** to be the **wpa2**. Then, set a **Pre-Shared Key** (8-63 characters) and select the **Cipher Type** to be the **auto** to have ZyWALL/USG automatically chooses the best available cipher based on the cipher currently in use by the wireless network. Click **OK**.

CONFIGURATION > Object > AP Profile > SSID > Security List

| | |
|-------------------------|--|
| General Settings | |
| Profile Name: | default |
| Security Mode: | <div style="border: 1px solid red; padding: 2px;">wpa2</div> ▼ |

Authentication Settings

☒ 802.1X

Auth. Method:

ReAuthentication Timer: (30~30000 seconds, 0 is unlimited)

☒ PSK

Pre-Shared Key:

Cipher Type:

Idle timeout: (30~30000 seconds)

Group Key Update Timer: (30~30000 seconds)

☐ Management Frame Protection
 ☒ Optional
 ☐ Required

Test the Result

Go to the ZyWALL/USG **Monitor > Wireless > AP Information > AP List**, you can check the list of APs which are currently connected to it and the details information such as **Registration** type, **Model** and **Recent On-line Time /Last Off-line Time**.

MONITOR > Wireless > AP Information > AP List

AP List

Config AP + Add to Mgmt AP List More Information Reboot DCS Now Log Suppression On Suppression Off

| # | Status | Description | IP Address | Model | Registration | MAC Address | LED status | Power Mode |
|---|--------|----------------------|--------------|------------|--------------|-------------------|------------|------------|
| 1 | | AP-58:8B:F3:91:6B:C7 | 192.168.2.33 | NWA5123-AC | Un-Mgmt AP | 58:8B:F3:91:6B:C7 | N/A | |

Page 1 of 1 Show 50 items

Displaying 1 - 1 of 1

Go to the ZyWALL/USG **Monitor > Wireless > Station Info > Station List**, you can check the list of wireless stations associated with a managed AP and the details information such as **SSID Name**, **Signal Strength** and the transmit (Tx)/receive (Rx) data rate.

MONITOR > Wireless > Station Info > Station List

Station List

| # | MAC Address | Associat... | SSID Name | Security ... | Signal Strength | Channel | Band | IP Address | Tx R... | Rx R... | Tx | Rx |
|---|------------------|-------------|-----------|--------------|-----------------|---------|------|--------------|---------|---------|--------|-------|
| 1 | 04:4B:ED:85:6... | AP-588BF... | ZyXEL | NONE | -65dBm | 6 | 2.4G | 192.168.2... | 15M | 32M | 102177 | 49447 |

Page 1 of 1 Show 50 items

Displaying 1 - 1 of 1

Using a mobile device to connect to SSID: **ZyXEL_AP1** and type the password (zyxel123) for authentication. Go to the ZyWALL/USG **Monitor > Log**, you will see [info] log message as shown below. The ZyWALL/USG will assign an IP address to

the mobile device and the mobile device can access the Internet.

MONITOR > Log

| | | | |
|-----|------|------|--|
| 349 | info | DHCP | DHCP server assigned 192.168.1.33 to TWNBZT02643-02(30:65:EC:49:85:EA... DHCP ACK |
| 350 | info | DHCP | Requested 192.168.1.33 from TWNBZT02643-02(30:65:EC:49:85:EA) [count... DHCP Request |

What Could Go Wrong?

If you can't see AP information in the AP List, please check the number of APs connected to the ZyWALL/USG has exceeded the maximum Managed AP number it can support. You can check the maximum support number of each ZyWALL/USG in the Datasheet from ZyXEL Download Library -

http://www.zyxel.com/support/download_landing.shtml

If your mobile device can't find the AP SSID you configured, please go to **CONFIGURATION > Object > AP Profile > SSID > SSID List** and check if the **Hidden SSID** option is enabled.

If your mobile device can't access to the Internet via AP connects to the ZyWALL/USG, please check if the LAN outgoing security policy allow access to the Internet.

If your mobile device is not connected to the AP automatically even you've joined the Wifi network before and you see [Wlan Station Info] log message as shown below, please check if this AP is removed from your mobile device's saved Wifi network list.

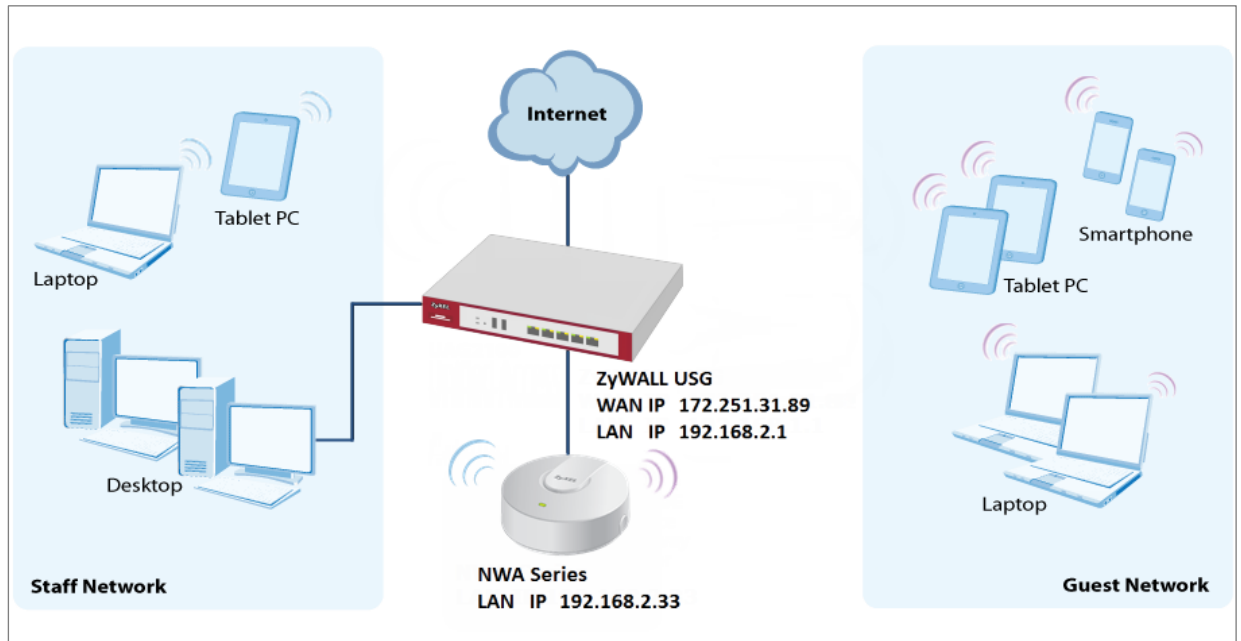
MONITOR > Log


| # | Priority | Category | Message ▼ | Note |
|-----|----------|-------------------|--|------|
| 17 | info | Wlan Station Info | STA Disassociation(8:DISASSOC_STA_HAS_LEFT) by STA Logout. MA... | |
| 100 | info | Wlan Station Info | STA Disassociation(3:DEAUTH_LEAVING) by STA Logout. MAC:D4:9... | |
| 10 | info | Wlan Station Info | STA Disassociation(3:DEAUTH_LEAVING) by STA Logout. MAC:D4:9... | |
| 105 | info | Wlan Station Info | STA Disassociation(3:DEAUTH_LEAVING) by STA Logout. MAC:D4:9... | |

How to Set Up Guest WiFi Network Accounts

This is an example of using ZyWALL/USG to configure guest WiFi accounts to allow limited wireless access to the Internet using only HTTP, HTTPS, and DNS protocols. For the wireless network setup, please see the tutorial about How to Set Up WiFi with ZyXEL AP.

ZyWALL/USG with Guest WiFi Accounts Example



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the WiFi Guest Account, Address Range and Service

Rule on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Object > User/Group > User > Add A User** to configure the **User Name** the guest Wi-Fi user and set **User Type** to **guest**. Set a secured **Password** (4-31 characters) and enter it again for confirmation.

Set the **Authentication Timeout Settings** to be **Use Manual Settings** to enter the number of minutes this user has to renew the current session before the user is logged out.

CONFIGURATION > Object > User/Group > User > Add A User

User Configuration

User Name : WiFi_guest

User Type: user

Password:

Retype:

Description: Local User

Authentication Timeout Settings: ☐ Use Default Settings ☒ Use Manual Settings

Lease Time: 240 (0-1440 minutes, 0 is unlimited)

Reauthentication Time: 240 (0-1440 minutes, 0 is unlimited)

In the ZyWALL/USG, go to **CONFIGURATION > Object > Address > Add Address Rule** to create the guest Wi-Fi user access subnet. In this example, AP is connected to ZyWALL/USG LAN interface 192.168.2.0/24. Configure the **Name** for you to identify the Wi-Fi guest subnet. Set the **Network** to be 192.168.2.0 and set the **Netmask** to be 255.255.255.0. Click **OK**.

CONFIGURATION > Object > Address > Add Address Rule

+ Add Address Rule

Name: WiFi_guest

Address Type: SUBNET

Network: 192.168.2.0

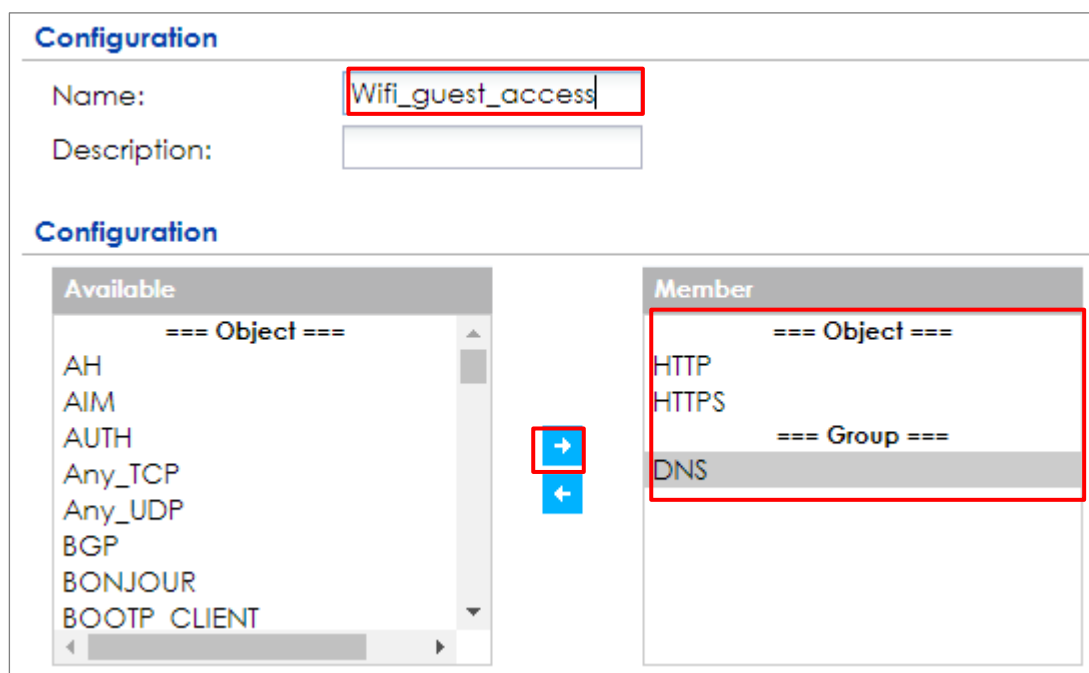
Netmask: 255.255.255.0

OK Cancel

In the ZyWALL/USG, go to **CONFIGURATION > Object > Service > Service Group >**

Add Service Group Rule to create the allowed protocols for guest Wi-Fi user. Configure the **Name** for you to identify the **Service Group**. Set **HTTP**, **HTTPS** and **DNS** to be in the same member group and click **OK**.

CONFIGURATION > Object > Service > Service Group > Add Service Group Rule



Configuration

Name:

Description:


Configuration

| Available | Member |
|--|--|
| <p>=== Object ===</p> <p>AH</p> <p>AIM</p> <p>AUTH</p> <p>Any_TCP</p> <p>Any_UDP</p> <p>BGP</p> <p>BONJOUR</p> <p>BOOTP CLIENT</p> | <p>=== Object ===</p> <p>HTTP</p> <p>HTTPS</p> <p>=== Group ===</p> <p>DNS</p> |

Set Up the Web Authentication on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Web Authentication > Web Authentication Policy Summary > Auth. Policy Add** to configure policy to redirect HTTP traffic to the user login screen. Configure the **Description (Optional)** for you to identify the auth. Policy. Then, scroll down the **Source Address** list to choose the newly created **wifi-guest**. Set the **Authentication** to be **required**. Select **Force User Authentication**.

CONFIGURATION > Web Authentication > Web Authentication Policy Summary > Auth. Policy Add

| General Settings | | |
|---|---|------------------------|
| <input checked="" type="checkbox"/> Enable Policy | | |
| Description: | WiFi_guest | (Optional) |
| User Authentication Policy | | |
| Incoming Interface: | any | |
| Source Address: | WiFi_guest | SUBNET, 192.168.2.0/24 |
| Destination Address: | any | |
| Schedule: | none | |
| Authentication: | required | |
| <input type="checkbox"/> Single Sign-on | | |
| <input checked="" type="checkbox"/> Force User Authentication |  | |
| Authentication Type: | default-web-porta | |

In the ZyWALL/USG, go to **CONFIGURATION > Web Authentication > General Settings** and select **Enable Web Authentication**.

CONFIGURATION > Web Authentication > General Settings

| Global Setting |
|---|
| <input checked="" type="checkbox"/> Enable Web Authentication |

Set Up the Security Policy on the ZyWALL/USG

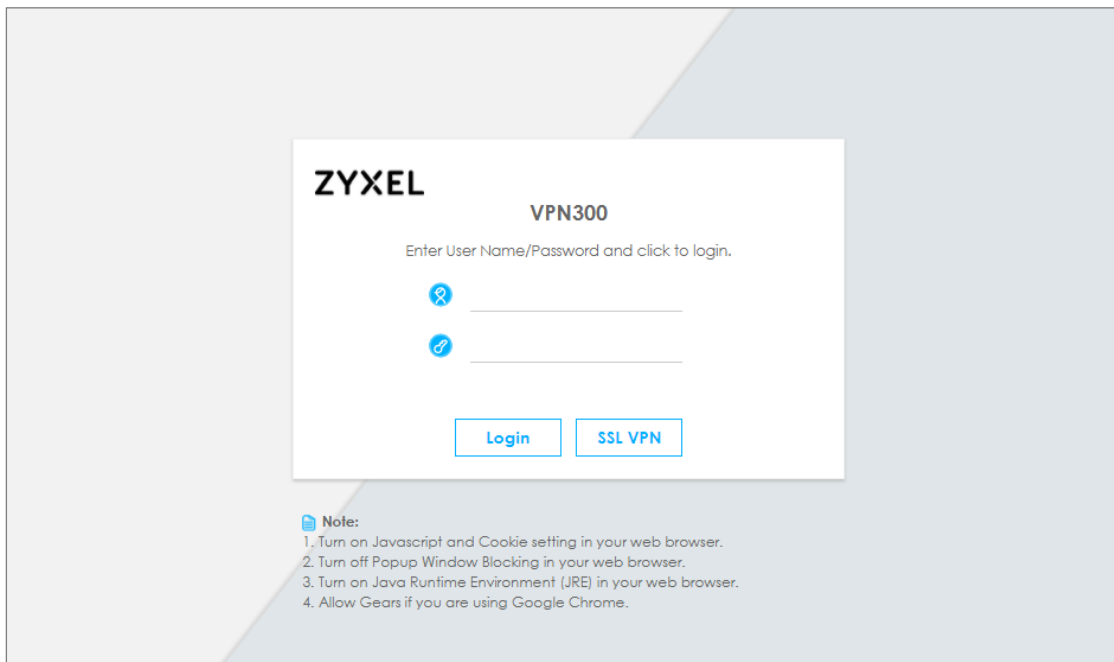
In the ZyWALL/USG, go to **CONFIGURATION > Security Policy > Policy > Add corresponding**. Configure a **Name** for you to identify the **Security Policy** profile. Set **From: LAN** and **To: any (Excluding ZyWALL)**. Set **Service** to be the Service Group Rule (wifi_guest_access in this example). Set **User** to be the Wi-Fi guest user (wifi_guest_access in this example). Select Log type to **log alert** in order to view the result later.

CONFIGURATION > Security Policy > Policy > Add corresponding

| | |
|--|--------------------|
| <input checked="" type="checkbox"/> Enable | |
| Name: | Wifi_guest |
| Description: | (Optional) |
| From: | any |
| To: | any (Excluding ZyV |
| Source: | any |
| Destination: | any |
| Service: | Wifi_guest_access |
| User: | Wifi_guest |
| Schedule: | none |
| Action: | allow |
| Log matched traffic: | log alert |

Test the Result


Using a mobile device to connect to the AP which is connected to the ZyWALL/USG. When you try to access the Internet, it will redirect to the user login screen.




ZYXEL


VPN300

Enter User Name/Password and click to login.

 _____

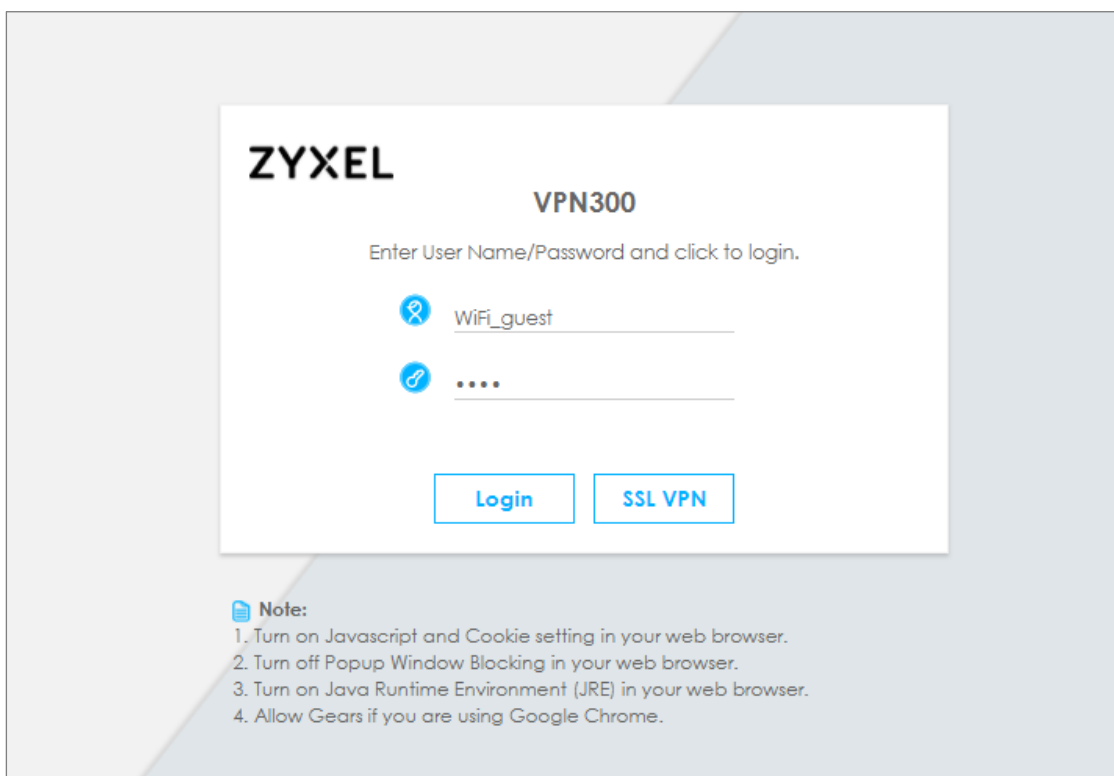
 _____

[Login](#) [SSL VPN](#)

 **Note:**

1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.
4. Allow Gears if you are using Google Chrome.


Type the Wi-Fi guest **User Name** and **Password**, click **Login**.




ZYXEL


VPN300

Enter User Name/Password and click to login.

 WiFi_guest

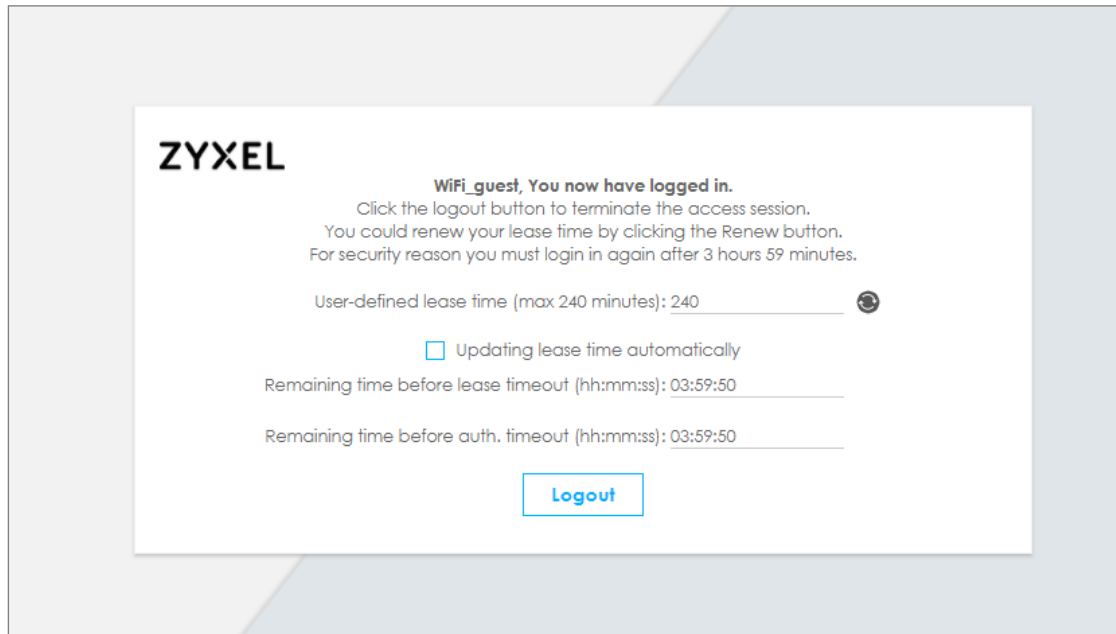


[Login](#) [SSL VPN](#)

 **Note:**

1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.
4. Allow Gears if you are using Google Chrome.

The access session page will appear.



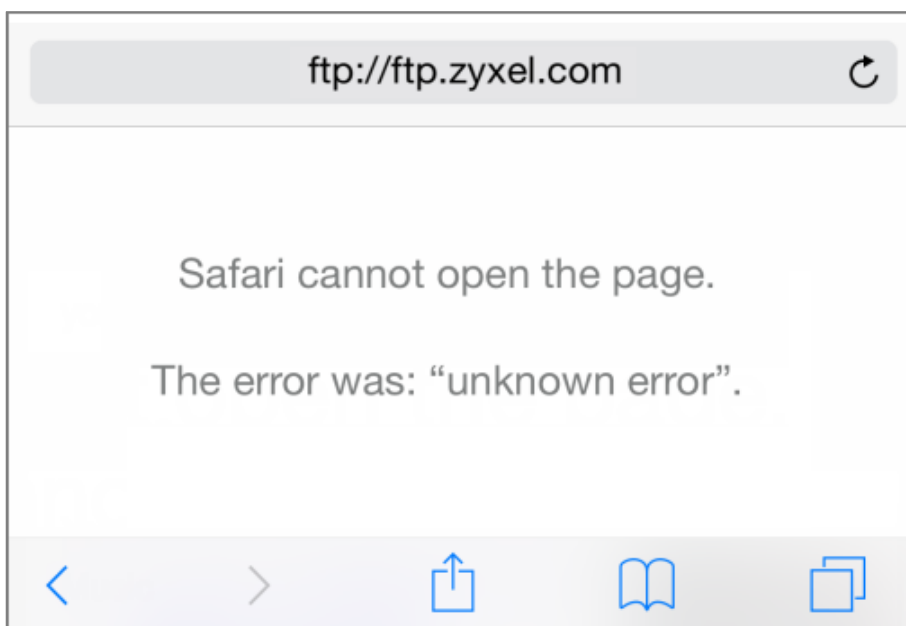
Go to the ZyWALL/USG **Monitor > System Status > Login Users**, you will see current login user list shown as below.

Monitor > System Status > Login Users

| User ID | Reauth/Lease Time | Type | IP Address | MAC | User Info |
|------------|---------------------|------------|--------------|-------------------|-------------------|
| wifi_guest | 03:19:30 / 03:19:30 | http/https | 192.168.2.34 | 90:3C:92:1C:C5:8B | guest(wifi_guest) |

| # | User ID | Reauth/Lease Time | Type | IP Address | MAC | User Info |
|---|------------|---------------------|------------|--------------|-------------------|-------------------|
| 1 | WiFi_guest | 03:57:03 / 03:57:03 | http/https | 192.168.2.33 | 00:1E:33:28:4F:AE | guest(WiFi_guest) |

Attempt to access FTP server (prohibited service in this example) and it gets an error message.



Go to the ZyWALL/USG **Monitor > Log**, you will see [notice] log message shown as below. The access to FTP service port 21 is blocked in this example.

Monitor > Log

| | | | | | |
|--------|-------------------------|------------------------------------|--------------------|------------------|--------------|
| notice | Security Policy Control | Match default rule, DROP [count=2] | 192.168.2.33:56799 | 36.226.188.36:21 | ACCESS BLOCK |
|--------|-------------------------|------------------------------------|--------------------|------------------|--------------|

What Could Go Wrong?

If you see [notice] log shown as below, the Wi-Fi guest traffic is blocked by the **priority 1 Security Policy**. The ZyWALL/USG checks the security policy in order and applies the first security policy to the matched traffic. If the Wi-Fi guest traffic matches a policy that comes earlier in the list, it may be unexpectedly blocked. Please change your policy setting or move the Wi-Fi guest policy to the higher priority.

Monitor > Log

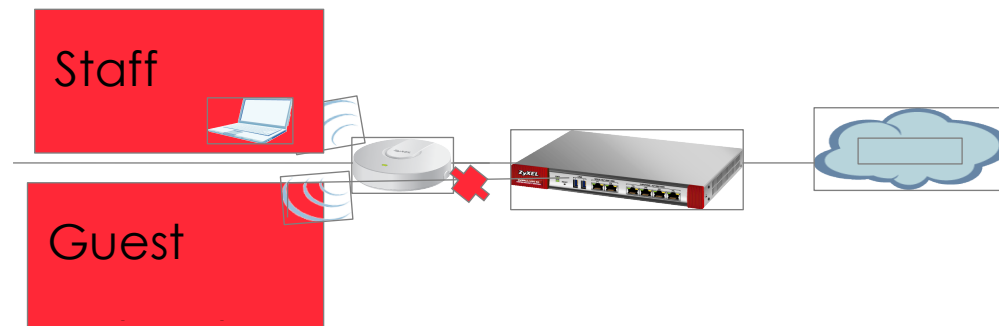
| Priority | Category | Message | Source | Destination | Note |
|----------|-------------------------|--|--------------------|-------------------|--------------|
| notice | Security Policy Control | priority:1, from LAN to ANY, UDP, service Wifi_guest, REJECT | 192.168.2.33:52555 | 172.25.5.210:53 | ACCESS BLOCK |
| notice | Security Policy Control | priority:1, from LAN to ANY, TCP, service Wifi_guest, REJECT | 192.168.2.33:59691 | 119.161.14.17:443 | ACCESS BLOCK |




Note: The default setting of **Security Policy** is without log notification (except **PolicyDefault**), if you want to check which policy may potentially block the traffic, please select this policy and set the **Log matched traffic** to be **log** or **log alert**.

How to create a Wi-Fi VLAN interfaces to separate staff network and Guest network

This example shows how to create Wi-Fi VLAN interfaces to separate staff network and Guest network. Suppose there should be no limitation for the staff network, but restrict the guests not access the USG.



Separate the Staff and Guest network


 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG210 (Firmware Version: ZLD 4.25)

Set up Wi-Fi VLAN interfaces

Create VLAN interfaces

Go to **CONFIGURATION > Object > Zone**. Create a zone for the guest.

CONFIGURATION > Object > Zone

 Add Zone



Group Members

Name:

Guest_Zone

Go to **CONFIGURATION > Network > Interface > VLAN**. Create VLAN16 for Staff_WiFi and VLAN17 for Guest_WiF

CONFIGURATION > Network > Interface > VLAN > VLAN16

| General Settings | |
|--|--|
| <input checked="" type="checkbox"/> Enable Interface | |
| Interface Properties | |
| Interface Type: | internal  |
| Interface Name: | vlan16 |
| Zone: | LAN1  |
| Base Port: | ge1 |
| VLAN ID: | 16 (1-4094) |
| <input checked="" type="checkbox"/> Advance | |
| Description: | Staff_wifi (Optional) |

| IP Address Assignment | |
|---|---------------|
| IP Address: | 172.16.0.1 |
| Subnet Mask: | 255.255.255.0 |
| <input type="checkbox"/> Enable IGMP Support | |
| <input type="radio"/> IGMP Upstream <input checked="" type="radio"/> IGMP Downstream | |

| DHCP Setting | |
|-------------------------------|----------------|
| DHCP: | DHCP Server |
| IP Pool Start Address: | 172.16.0.10 |
| First DNS Server (Optional): | Custom Defined |
| Second DNS Server (Optional): | None |
| Third DNS Server (Optional): | None |

| | |
|------------|---------|
| Pool Size: | 100 |
| | 8.8.8.8 |

CONFIGURATION > Network > Interface > VLAN > VLAN17

General Settings

☒ Enable Interface

Interface Properties

Interface Type: ⓘ
 Interface Name:
 Zone: ⓘ
 Base Port:
 VLAN ID: (1-4094)
☒ Advance
 Description: (Optional)

IP Address Assignment

IP Address:
 Subnet Mask:
☐ Enable IGMP Support
☐ IGMP Upstream
☒ IGMP Downstream

DHCP Setting

DHCP:
 IP Pool Start Address: Pool Size:
 First DNS Server (Optional):
 Second DNS Server (Optional):
 Third DNS Server (Optional):

There will be two VLAN interfaces.

CONFIGURATION > Network > Interface > VLAN

| + Add Edit Remove ⚡ Activate ⚡ Inactivate Create Virtual Interface Object References | | | | | |
|--|--------|--------|----------|---------------------|---------------|
| # | Status | Name + | Port/VID | IP Address | Mask |
| 1 | ⚡ | vlan16 | ge5/16 | static --172.16.0.1 | 255.255.255.0 |
| 2 | ⚡ | vlan17 | ge6/17 | static --172.17.0.1 | 255.255.255.0 |

Page 1 of 1 Show 50 items Displaying 1 - 2 of 2

Set Up the User

Go to **Configuration > Object > User/Group > User**, and create users for the staff and the guest

Configuration > Object > User/Group > User > staff

+

Add A User

?

×

User Configuration

User Name :

staff

User Type:

user

▼

Password:

....

Retype:

....

Description:

Local User

Authentication Timeout Settings

☒ Use Default Settings
 ☐ Use Manual Settings

Lease Time:

1440

minutes

Reauthentication Time:

1440

minutes

Configuration > Object > User/Group > User > guest

+

Add A User

?

×

User Configuration

User Name :

guest

User Type:

user

▼

Password:

....

Retype:

....

Description:

Local User

Authentication Timeout Settings

☒ Use Default Settings
 ☐ Use Manual Settings

Lease Time:

1440

minutes

Reauthentication Time:

1440

minutes

There will be two users.

| User | Group | Setting | MAC Address |
|--|--------------|-----------|------------------------|
| Configuration | | | |
| <div> <div>+</div> <div>Add</div> <div>✎</div> <div>Edit</div> <div>✖</div> <div>Remove</div> <div>🔗</div> <div>Object References</div> </div> | | | |
| # | User Name | User Type | Description |
| 1 | admin | admin | Administration account |
| 2 | ldap-users | ext-user | External LDAP Users |
| 3 | radius-users | ext-user | External RADIUS Users |
| 4 | ad-users | ext-user | External AD Users |
| 5 | WiFi_guest | guest | Local User |
| 6 | staff | user | Local User |
| 7 | guest | user | Local User |

⏪

⏩

Page 1 of 1

⏪

⏩

Show 50 items

Displaying 1 - 7 of 7

Set Up the AP Profile

Go to **CONFIGURATION > Object > AP Profile > SSID > Security List**, and create two security profiles.

CONFIGURATION > Object > AP Profile > SSID > Security List > Guest_WPA2

| General Settings | |
|---|---|
| Profile Name: | <input type="text" value="Guest_WPA2"/> |
| Security Mode: | <input type="text" value="wpa2"/> |
| Fast Roaming Settings | |
| <input type="checkbox"/> 802.11r | |
| Radius Settings | |
| Radius Server Type: | <input type="text" value="Internal"/> |
| <input type="checkbox"/> Proxy by controller directly | |
| MAC Authentication Setting | |
| <input type="checkbox"/> MAC Authentication | |
| Auth. Method: | <input type="text" value="default"/> |
| Delimiter (Account): | <input type="text" value="colon (:)"/> |
| Case (Account): | <input type="text" value="upper"/> |
| Delimiter (Calling Station ID): | <input type="text" value="colon (:)"/> |
| Case (Calling Station ID): | <input type="text" value="upper"/> |

| Authentication Settings | |
|---|---|
| <input type="radio"/> 802.1X | |
| Auth. Method: | <input type="text" value="default"/> |
| ReAuthentication Timer: | <input type="text" value="0"/> (30~30000 seconds, 0 is unlimited) |
| <input checked="" type="radio"/> PSK | |
| Pre-Shared Key: | <input type="text" value="12345678"/> |
| Cipher Type: | <input type="text" value="auto"/> |
| Idle timeout: | <input type="text" value="300"/> (30~30000 seconds) |
| Group Key Update Timer: | <input type="text" value="30000"/> (30~30000 seconds) |
| <input type="checkbox"/> Management Frame Protection <input checked="" type="radio"/> Optional <input type="radio"/> Required | |

CONFIGURATION > Object > AP Profile > SSID > Security List > Staff_WPA2

| General Settings | |
|---|--------------------------------------|
| Profile Name: | Staff_WPA2 |
| Security Mode: | wpa2 |
| Fast Roaming Settings | |
| <input type="checkbox"/> 802.11r | |
| Radius Settings | |
| Radius Server Type: | Internal |
| <input type="checkbox"/> Proxy by controller directly | |
| MAC Authentication Setting | |
| <input type="checkbox"/> MAC Authentication | |
| Auth. Method: | default |
| Delimiter (Account): | colon (:) |
| Case (Account): | upper |
| Delimiter (Calling Station ID): | colon (:) |
| Case (Calling Station ID): | upper |
| Authentication Settings | |
| <input checked="" type="radio"/> 802.1X | |
| Auth. Method: | default |
| ReAuthentication Timer: | 0 (30~30000 seconds, 0 is unlimited) |
| <input checked="" type="radio"/> PSK | |
| Pre-Shared Key: | 12345678 |
| Cipher Type: | auto |
| Idle timeout: | 300 (30~30000 seconds) |
| Group Key Update Timer: | 30000 (30~30000 seconds) |
| <input type="checkbox"/> Management Frame Protection <input checked="" type="radio"/> Optional <input type="radio"/> Required | |

Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, and create two SSID profiles.

CONFIGURATION > Object > AP Profile > SSID > SSID List > Staff_Wifi

Add SSID Profile

Create new Object ▼

Profile Name:

SSID:

Security Profile:

 ▼

MAC Filtering Profile:

 ▼

QoS:

 ▼

Rate Limiting (Per Station Traffic Rate) ⓘ

Downlink:

 ▼
 (0~160, 0 is unlimited)

Uplink:

 ▼
 (0~160, 0 is unlimited)

Band Select:

 ▼

Forwarding Mode:

 ▼

VLAN ID:

 (1~4094)

☐ Hidden SSID

☐ Enable Intra-BSS Traffic blocking

☐ Schedule SSID ⓘ

OK

Cancel

CONFIGURATION > Object > AP Profile > SSID > SSID List > Guest_Wifi

Add SSID Profile

?

×

Create new Object▼

Profile Name:

SSID:

Security Profile:

▼

MAC Filtering Profile:

▼

QoS:

▼

Rate Limiting (Per Station Traffic Rate) ⓘ

Downlink:

▼

(0~160, 0 is unlimited)

Uplink:

▼

(0~160, 0 is unlimited)

Band Select:

▼

Forwarding Mode:

▼

VLAN ID:

(1~4094)

☐ Hidden SSID

☐ Enable Intra-BSS Traffic blocking

☐ Schedule SSID ⓘ

OK

Cancel

Go to **CONFIGURATION > Wireless > AP Management > AP Group**, and add an AP Group as **WiFi**.

CONFIGURATION > Wireless > AP Management > AP Group

+ Add AP Group Profile

General Settings

Group Name:

Description: (Optional)

Radio 1 Setting

OP Mode: ☒ AP Mode ☐ MON Mode ☐ Root AP ☐ Repeater AP i

Radio 1 AP Profile: v

Output Power: dBm (0~30) i

Edit

| # | SSID Profile |
|---|--------------|
| 1 | Staff_wifi |
| 2 | Guest_wifi |
| 3 | disable |
| 4 | disable |
| 5 | disable |
| 6 | disable |
| 7 | disable |
| 8 | disable |

Go to **CONFIGURATION > Wireless > AP Management > Mgmt. AP List**, and Edit the AP List. Change the Group setting as **WiFi**

CONFIGURATION > Wireless > AP Management > Mgmt. AP List,

Edit AP List

Create new Object v

Configuration

MAC: 40:4A:03:69:A5:04

Model: NWA5160N

Description:

Group Setting: v

Radio1 Setting

☐ Override Group Radio Setting

OP Mode: ☒ AP Mode ☐ MON Mode

Radio 1 Profile: v

Set Up the Security policy rule

Go to **CONFIGURATION > Security Policy > Policy Control > Policy**. Add one rule to restrict Guest access USG, and another one to allow to access internet.

CONFIGURATION > Security Policy > Policy Control > Policy > Guest_ZyWALL

+

Add corresponding

Create new Object ▼

☒ Enable

Name:

Guest_Zywall

Description:

(Optional)

From:

Guest_Zone

▼

To:

ZyWALL

▼

Source:

any

▼

Destination:

any

▼

Service:

any

▼

User:

any

▼

Schedule:

none

▼

Action:

deny

▼

Log denied traffic:

no

▼

OK

Cancel

CONFIGURATION > Security Policy > Policy Control > Policy > Guest_Internet

+

Add corresponding

?

✕

Create new Object ▼

☒ Enable

Name:

Description:
(Optional)

From:
▼

To:
▼

Source:
▼

Destination:
▼

Service:
▼

User:
▼

Schedule:
▼

Action:
▼

Log denied traffic:
▼

OK

Cancel

Test result

Connect to the SSID Staff_WiFi, and ping the USG interface.

Wi-Fi

Staff_WiFi

Forget This Network

IP ADDRESS

DHCP

BootP

Static

| | |
|----------------|---------------|
| IP Address | 172.16.0.10 |
| Subnet Mask | 255.255.255.0 |
| Router | 172.16.0.1 |
| DNS | 8.8.8.8 |
| Search Domains | |
| Client ID | |

Renew Lease

Back

Ping

Help

IP Address to ping:

172.16.0.1

Delay: 2000 ms

Start

Clear

PING 172.16.0.1 (172.16.0.1)
44 bytes from 172.16.0.1 : icmp_seq=0 ttl=64
time=31 ms
44 bytes from 172.16.0.1 : icmp_seq=1 ttl=64
time=31 ms
44 bytes from 172.16.0.1 : icmp_seq=2 ttl=64
time=27 ms
44 bytes from 172.16.0.1 : icmp_seq=3 ttl=64
time=23 ms
44 bytes from 172.16.0.1 : icmp_seq=4 ttl=64
time=30 ms
--- 172.16.0.1 ping statistics ---
5 packets transmitted, 5 packets received, lost 0.0
%

Connect to the SSID Guest_WiFi, and ping the USG interface

Wi-Fi Guest_WiFi

[Forget This Network](#)

IP ADDRESS

☒ DHCP ☐ BootP ☐ Static

IP Address 172.17.0.10

Subnet Mask 255.255.255.0

Router 172.17.0.1

DNS 8.8.8.8

Search Domains

Client ID

[Renew Lease](#)

Back Ping Help

IP Address to ping:

172.17.0.1

Delay: 2000 ms

[Start](#) [Clear](#)

72 bytes from 114.34.247.205 : Destination Net Unreachable
 PING 172.17.0.1 (172.17.0.1)
 Request timeout for icmp_seq 0
 Request timeout for icmp_seq 1
 Request timeout for icmp_seq 2
 Request timeout for icmp_seq 3
 --- 172.17.0.1 ping statistics ---
 5 packets transmitted, 0 packets received, lost 100.0 %

What could go wrong

Choose the wrong zone for the Guest VLAN interface.

Edit VLAN

Show Advanced Settings

General Settings

☒ Enable Interface

Interface Properties

Interface Type: internal

Interface Name: vlan17

Zone: Guest_Zone

Base Port: ge6

VLAN ID: 17 (1-4094)

☒ Advance

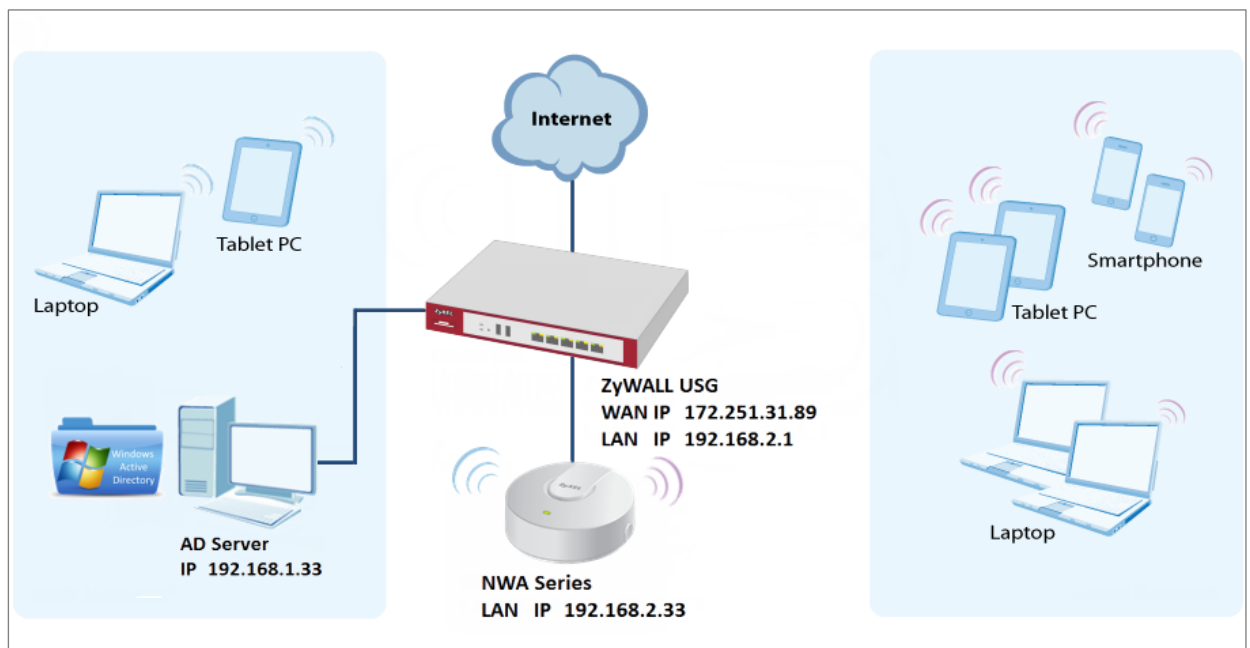
Description: Guest_wifi (Optional)


Not change the AP to the correct group

How to Set Up WiFi Networks with Microsoft Active Directory Authentication

This is an example of using ZyWALL/USG to configure guest WiFi accounts with Microsoft Active Directory (AD) to authenticate your WiFi guests. For the wireless network setup, please go to How to Set Up WiFi with ZyXEL AP.

ZyWALL/USG with AD Guest WiFi Accounts Example

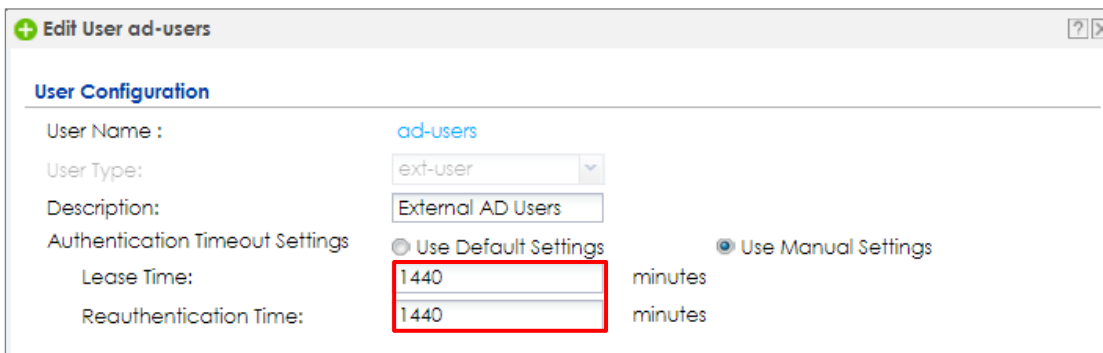


 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the Wi-Fi Guest Account and Authentication Method on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Object > User/Group > User > ad-users**, set the **Authentication Timeout Settings** to **Use Manual Settings** and enter the number of minutes this user has to renew the current session before the user is logged out.

CONFIGURATION > Object > User/Group > User > ad-users

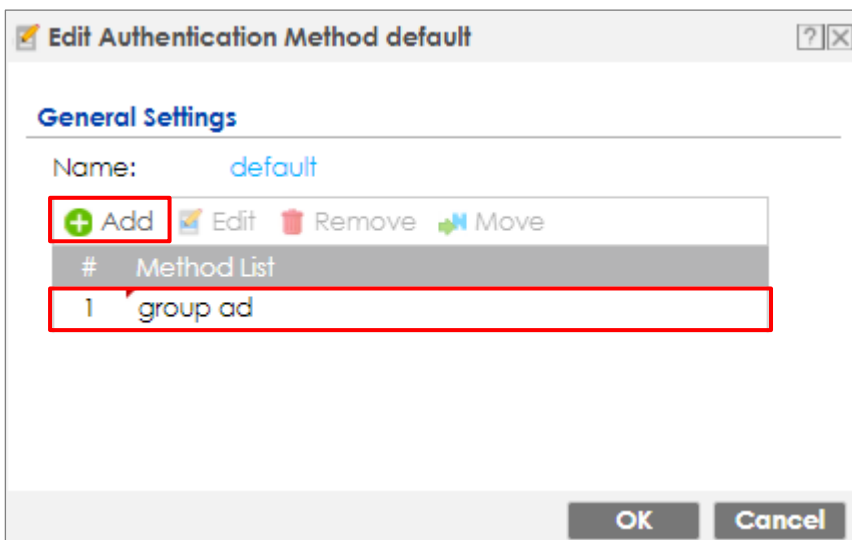


The screenshot shows the 'Edit User ad-users' window with the following settings:

- User Name: ad-users
- User Type: ext-user
- Description: External AD Users
- Authentication Timeout Settings:
 - ☐ Use Default Settings
 - ☒ Use Manual Settings
- Lease Time: 1440 minutes
- Reauthentication Time: 1440 minutes

In the ZyWALL/USG, go to **CONFIGURATION > Object > Authentication Method > default > Edit Authentication Method default**, click **Add** to insert group ad in the table. Click **OK**.

CONFIGURATION > Object > User/Group > User > ad-users



The screenshot shows the 'Edit Authentication Method default' window with the following settings:

- Name: default
- Buttons: Add, Edit, Remove, Move
- Method List table:

| # | Method List |
|---|-------------|
| 1 | group ad |

In the ZyWALL/USG, go to **CONFIGURATION > Web Authentication > General Settings** and select **Enable Web Authentication**.

CONFIGURATION > Web Authentication > General Settings

| Global Setting |
|---|
| <input checked="" type="checkbox"/> Enable Web Authentication |

Set Up the Active Directory Server Account on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Object > AAA Server > Active Directory > Add Active Directory** to configure the AD sever. Enter the **Server Address** (192.168.1.33 in this example) and **Based DN** (dc=cso,dc=net in this example). Specify the **Bind DN** for logging into the AD server (cn=Administrator,cn=users,dc=cso,dc=net in this example). If required, enter the **Password** for the ZyWALL/USG to bind (or log in) to the AD server.

CONFIGURATION > Object > AAA Server > Active Directory > Add Active Directory

| General Settings | | |
|--|----------------------|-------------------------|
| Name: | ad | |
| Description: | <input type="text"/> | (Optional) |
| Server Settings | | |
| Server Address: | 192.168.1.33 | (IP or FQDN) |
| Backup Server Address: | <input type="text"/> | (IP or FQDN) (Optional) |
| Port: | 389 | (1-65535) |
| Base DN: | dc=cso,dc=net | |
| <input type="checkbox"/> Use SSL | | |
| Search time limit: | 5 | (1-300 seconds) |
| <input type="checkbox"/> Case-sensitive User Names | | |
| Server Authentication | | |
| Bind DN: | cn=administrator,cn= | |
| Password: | | |
| Retype to Confirm: | | |

Scroll down to the **Configuration Validation** section, use a user account from the server specified above to test if the configuration is correct. Enter the account's

user name (wifi_guest in this example) in the **Username** field and click **Test**. A pop-up screen will appear allowing you to view the test result. Click **OK** to save the configuration.

CONFIGURATION > Object > AAA Server > Active Directory > Add Active Directory

Configuration Validation

Please enter an existing user account in this server to validate the above settings.

Username:

Test Status:

OK

Returned User Attributes:

dn: CN=wifi_guest,CN=Users,DC=cso,DC=net
 objectClass: top
 objectClass: person
 objectClass: organizationalPerson
 objectClass: user
 cn: wifi_guest
 givenName: wifi_guest
 distinguishedName: CN=wifi_guest,CN=Users,DC=cso,DC=net

Set Up the Security Policy on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Security Policy > Policy > Add corresponding**. Configure a **Name** for you to identify the **Security Policy** profile. Set **From: LAN** and **To: any (Excluding ZyWALL)**. Set **Service** to be the service rule for Wi-Fi guest (wifi_guest_access in this example). Set **User** to be the Wi-Fi guest user (ad-users in this example). Select Log type to be **log alert** in order to view the result later.

CONFIGURATION > Security Policy > Policy > Add corresponding

| | |
|--|---------------------------------|
| <input checked="" type="checkbox"/> Enable | |
| Name: | WiFi_Guest |
| Description: | <input type="text"/> (Optional) |
| From: | LAN |
| To: | any (Excluding ZyV) |
| Source: | any |
| Destination: | any |
| Service: | Wifi_guest_access |
| User: | ad-users |
| Schedule: | none |
| Action: | allow |
| Log matched traffic: | log alert |


Test the Result


Using a mobile device to connect to the AP which is connected to the ZyWALL/USG. When you try to access the Internet, it will redirect to the user login screen.

ZYXEL


VPN300

Enter User Name/Password and click to login.

 _____

 _____

[Login](#) [SSL VPN](#)

 **Note:**


1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.
4. Allow Gears if you are using Google Chrome.


Type the Wi-Fi guest **User Name** and **Password**, click **Login**.

ZYXEL


VPN300

Enter User Name/Password and click to login.

 WiFi_guest

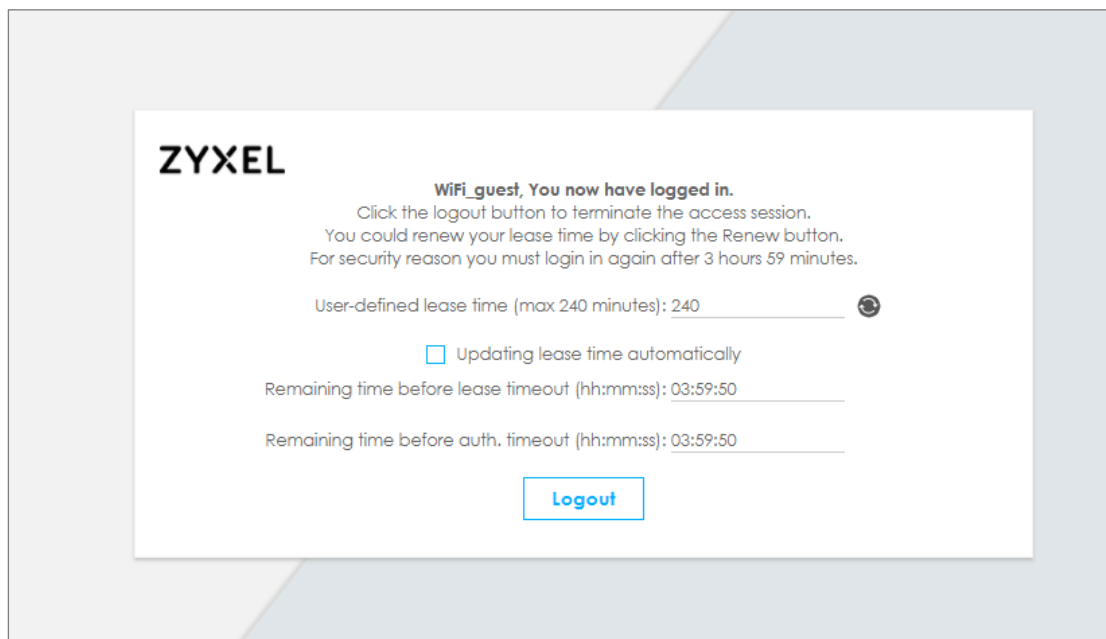


[Login](#) [SSL VPN](#)

 **Note:**

1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.
4. Allow Gears if you are using Google Chrome.

The access session page will appear.



Go to the ZyWALL/USG **Monitor > System Status > Login Users**, you will see current login user list as below.

Monitor > System Status > Login Users

| User ID | Reauth/Lease Time | Type | IP Address | MAC | User Info |
|------------|---------------------|------------|--------------|-------------------|--------------------|
| WIFI_GUEST | 03:59:42 / 03:59:42 | http/https | 192.168.2.34 | 90:3C:92:1C:C5:8B | ext-user(ad-users) |

What Could Go Wrong?

If you see [notice] log shown as below, the Wi-Fi guest traffic is blocked by the **priority 1 Security Policy**. The ZyWALL/USG checks the security policy in order and applies the first security policy the traffic matches. If the Wi-Fi guest traffic matches a policy that comes earlier in the list, it may be unexpectedly blocked. Please change your policy setting or move the Wi-Fi guest policy to the higher priority.


Monitor > Log

| Priority | Category | Message | Note |
|----------|-------------------------|---|--------------|
| notice | Security Policy Control | priority:1, from LAN to ANY, TCP, service HTTPS, REJECT [count=3] | ACCESS BLOCK |
| notice | Security Policy Control | priority:1, from LAN to ANY, TCP, service HTTPS, REJECT [count=3] | ACCESS BLOCK |

If you see [alert] log message shown as below, the Wi-Fi guest traffic failed. Please make sure you enable **Web Authentication** and check your AD server is working properly.

Monitor > Log

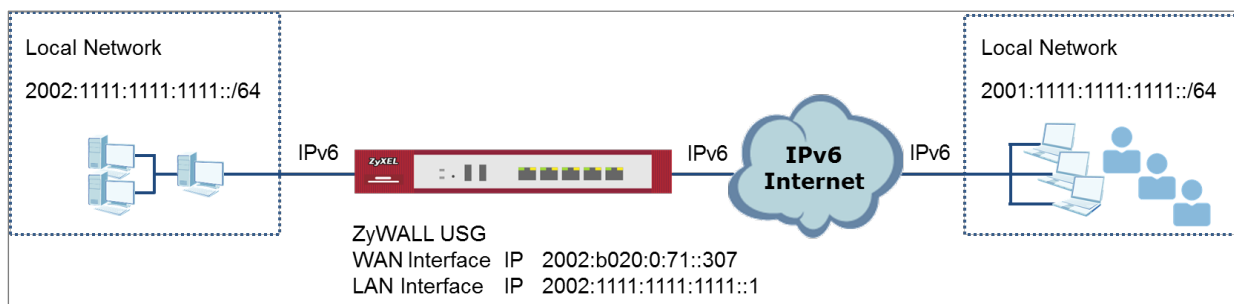
| Priority | Category | Message | Note |
|----------|----------|--|---------------------|
| alert | User | Failed login attempt to Device from http/https (incorrect passw... | Account: wifi_guest |


 Note: The default setting of **Security Policy** is without log notification (except **PolicyDefault**), if you want to check which policy may potentially block the traffic, please select this policy and set the **Log matched traffic** to be **log** or **log alert**.

How to Set Up IPv6 Interfaces for Pure IPv6 Routing

This example shows how to configure your ZyWALL/USG WAN and LAN interfaces which connects two IPv6 networks. ZyWALL/USG periodically advertises a network prefix of 2002:1111:1111:1111::/64 to the LAN through router advertisements.

ZyWALL/USG with Pure IPv6 Network Example



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Enable the IPv6 on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > System > IPv6 > Global Setting**, select the **Enable IPv6** and click **Apply** at the bottom of the screen.




CONFIGURATION > System > IPv6 > Global Setting

| Global Setting |
|---|
| <input checked="" type="checkbox"/> Enable IPv6 |

Set Up the WAN IPv6 Interface on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > Interface > Ethernet > wan1**. Select **Enable Interface** and **Enable IPv6**. Select **Enable Stateless Address Auto-configuration (SLAAC)**. Click **OK**.

CONFIGURATION > Network > Interface > Ethernet > wan1

| | |
|---|--|
| General Settings | |
| <input checked="" type="checkbox"/> Enable Interface | |
| General IPv6 Setting | |
| <input checked="" type="checkbox"/> Enable IPv6 |  |
| Interface Properties | |
| Interface Type: | external  |
| Interface Name: | ge1 |
| Port: | P1 |
| Zone: | WAN  |
| MAC Address: | B8:EC:A3:A9:C0:0B |
| Description: | <input type="text"/> (Optional) |
| IPv6 Address Assignment | |
| <input checked="" type="checkbox"/> Enable Stateless Address Auto-configuration (SLAAC) | |
| Link-Local Address: | n/a |
| IPv6 Address/Prefix Length: | <input type="text"/> (Optional) |



Note: Your ISP or uplink router should enable router advertisement.

Set Up the LAN IPv6 Interface on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > Interface > Ethernet > lan1**. Select **Enable Interface** and **Enable IPv6**. Select **Enable Stateless Address Auto-configuration (SLAAC)**. Select **Enable Router Advertisement** and click **Add** to configure a network prefix for the LAN1 (2002:1111:1111:1111::/64 in this example).

Click **OK**.

CONFIGURATION > Network > Interface > Ethernet > lan1 > General Settings

General Settings

☒ Enable Interface

General IPv6 Setting

☒ Enable IPv6

Interface Properties

Interface Type:

internal

Interface Name:

Lan1

Port:

P5, P6

Zone:

LAN1

MAC Address:

B8:EC:A3:A9:00:0F

Description:

(Optional)

CONFIGURATION > Network > Interface > Ethernet > lan1 > IPv6 Router

Advertisement Setting

IPv6 Router Advertisement Setting

☒ Enable Router Advertisement

Advance

Router Preference:

Medium

Advance

Advertised Prefix Table

+ Add

Edit

Remove

| # | IPv6 Address/Prefix Length |
|---|----------------------------|
| 1 | 2001:1111:1111:1111::/64 |

Page 1 of 1

Show 50 items

Displaying 1 -

Test the Result

Connect a computer to the ZyWALL/USG's LAN1.

720/774

Enable IPv6 support on your computer. In Windows XP, you need to use the IPv6 install command in a Command Prompt. In Windows 7, IPv6 is supported by default. You can enable IPv6 in the **Control Panel > Network and Sharing Center > Local Area Connection** screen

Your computer should get an IPv6 IP address (starting with 2002:1111:1111:1111: for this example) from the ZyWALL/USG.

Window 7 > cmd > ipconfig

```
C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : localdomain
    IPv6 Address. . . . . : 2002:1111:1111:1111:dc9:e2ff:7d32:19c9
    Temporary IPv6 Address. . . . . : 2002:1111:1111:1111:444d:9168:b972:2720
    Link-local IPv6 Address . . . . . : fe80::dc9:e2ff:7d32:19c9%12
    Default Gateway . . . . . : fe80::b2b2:dcff:fe70:c1d8%12
```

Open a web browser and type <http://test-ipv6.com/>. You can see the IPv6 connectivity result shown as below:

The screenshot shows the test-ipv6.com website. The browser address bar shows 'test-ipv6.com'. The page has a navigation bar with 'Test IPv6', 'FAQ', 'Mirrors', and 'stats'. The main heading is 'Test your IPv6 connectivity.' Below this is a 'Summary' tab with the following information:

- Your IPv6 address on the public Internet appears to be 2002:b020:0:71::307
- Your Internet Service Provider (ISP) appears to be HINET Data Communication Business Group, TW
- Since you have IPv6, we are including a tab that shows how well you can reach other IPv6 sites. [\[more info\]](#)
- Good news!** Your current configuration will continue to work as web sites enable IPv6.
- Your DNS server (possibly run by your ISP) appears to have IPv6 Internet access.

Your readiness score

10/10 for your IPv6 stability and readiness, when publishers are forced to go IPv6 only

Click to see [test data](#)

(Updated server side IPv6 readiness stats)

What Could Go Wrong?

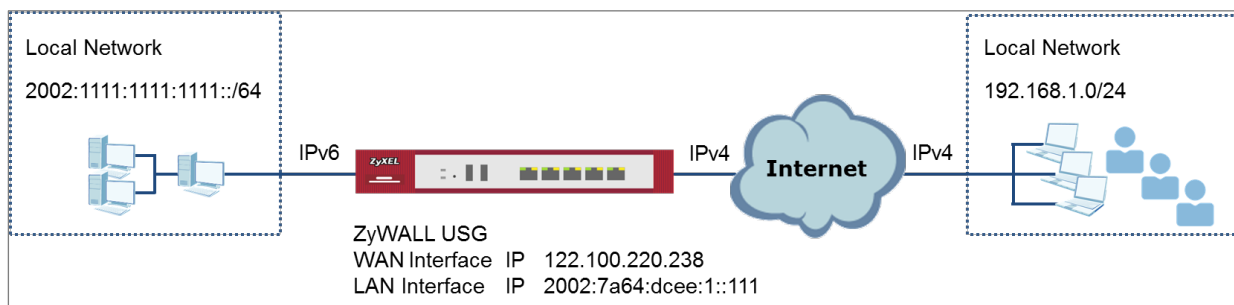
If your IPv6 connection is not working, please make sure you enable Auto-Configuration on the WAN1 IPv6 interface. If not, you will not have any default route to forward the LAN's IPv6 packets.


In Windows, some IPv6 related tunnels may be enabled by default such as Teredo and 6to4 tunnels. It may cause your computer to handle IPv6 packets in an unexpected way. It is recommended to disable those tunnels on your computer.

How to Set Up an IPv6 6to4 Tunnel

This example shows how to configure your ZyWALL/USG to create IPv6 6to4 Tunnel. In this example, the ZyWALL/USG acts as a 6to4 router which connects the IPv4. After configuration, the ZyWALL/USG can assign an IPv6 to clients behind it and pass IPv6 traffic through IPv4 environment to access remote IPv6 network.

ZyWALL/USG with IPv6 6to4 Tunnel Example



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the LAN IPv6 Interface on the ZyWALL/USG

The second and third sets of 16-bit IP address from the left must be converted from wan1 IP (122.100.220.238 in this example). It becomes 7a64:dcee in hexadecimal. (You can go to <https://isc.sans.edu/tools/ipv6.html#form> to convert an IPv4 address into its default 6-to-4 equivalent). You are free to use the fourth set of 16-bit IP address from the left in order to allocate different network addresses (prefixes) to IPv6 interfaces. In this example, the LAN1 network address is assigned to use 2002:7a64:dcee:1::/64 and the LAN1 IP address is set to

2002:7a64:dcee:1::111/128.

In the ZyWALL/USG, go to **CONFIGURATION > Network > Interface > Ethernet > lan1**, Select **Enable Interface** and **Enable IPv6**. Type 2002:7a64:dcee:1::111/128 in the **IPv6 Address/Prefix Length** field for the LAN1's IP address.

Enable **Router Advertisement**. Then click **Add** in the **Advertised Prefix Table** to add **2002:7a64:dcee:1::/64**. The LAN1 hosts will get the network prefix through the router advertisement messages sent by the LAN1 IPv6 interface periodically. Click **OK**.

CONFIGURATION > Network > Interface > Ethernet > lan1 > General Settings

| General Settings | |
|--|---------------------------------|
| <input checked="" type="checkbox"/> Enable Interface | |
| General IPv6 Setting | |
| <input checked="" type="checkbox"/> Enable IPv6 | i |
| Interface Properties | |
| Interface Type: | internal i |
| Interface Name: | Lan1 |
| Port: | P5, P6 |
| Zone: | LAN1 i |
| MAC Address: | B8:EC:A3:A9:C0:0F |
| Description: | <input type="text"/> (Optional) |
| IPv6 Address Assignment | |
| <input type="checkbox"/> Enable Stateless Address Auto-configuration (SLAAC) | |
| Link-Local Address: | fe80::baec:a3ff:fea9:c00f/64 |
| IPv6 Address/Prefix Length: | 2002:7a64:dcee::111, (Optional) |

CONFIGURATION > Network > Interface > Ethernet > lan1 > IPv6 Router Advertisement Setting

| IPv6 Router Advertisement Setting | | | | | |
|---|--|---|----------------------------|--|-----------------------|
| <input checked="" type="checkbox"/> Enable Router Advertisement | | | | | |
| <input type="checkbox"/> Advance | | | | | |
| Router Preference: | Medium | | | | |
| <input type="checkbox"/> Advance | | | | | |
| Advertised Prefix Table | <div> Add Edit Remove </div> <table border="1"> <thead> <tr> <th>#</th> <th>IPv6 Address/Prefix Length</th> </tr> </thead> <tbody> <tr> <td></td> <td>2002:7a64:dcee:1::/64</td> </tr> </tbody> </table> <div> Page 1 of 1 Show 50 items Displaying 1 - </div> | # | IPv6 Address/Prefix Length | | 2002:7a64:dcee:1::/64 |
| # | IPv6 Address/Prefix Length | | | | |
| | 2002:7a64:dcee:1::/64 | | | | |

Set Up the 6to4 Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > Interface > Tunnel > Add**, Select **Enable**. Enter **tunnel0** as the **Interface Name** and select **6to4** as the **Tunnel Mode**. In the **6to4 Tunnel Parameter** section, this example just simply uses the default 6to4 Prefix, **2002::/16**. Enter your **Relay Router**'s IP address (**192.88.99.1** in this example). Select **wan1** as the **Gateway**. Click **OK**.

CONFIGURATION > Network > Interface > Tunnel

| General Settings | |
|---|------------------------|
| <input checked="" type="checkbox"/> Enable | |
| Interface Properties | |
| Interface Name: | tunnel0 |
| Zone: | TUNNEL |
| Tunnel Mode: | 6to4 |
| IPv6 Address Assignment | |
| Metric: | 0 (0-15) |
| 6to4 Tunnel Parameter | |
| 6to4 Prefix: | 2002::/16 |
| Relay Router: | 192.88.99.1 (Optional) |
| <p> NOTE: traffic destined to the non-6to4 prefix domain tunnels to the relay router</p> | |
| <input type="checkbox"/> Advance | |

| Gateway Settings | |
|---|---|
| My Address | |
| <input checked="" type="radio"/> Interface ge2 | DHCP client -- 10.214.30.82/255.255.255.0 |
| <input type="radio"/> IP Address 0.0.0.0 | |
| Remote Gateway Address: Automatic | |

Test the Result

Connect a computer to the ZyWALL/USG's LAN1.

Enable IPv6 support on your computer. In Windows XP, you need to use the IPv6 install command in a Command Prompt. In Windows 7, IPv6 is supported by default. You can enable IPv6 in the **Control Panel > Network and Sharing Center > Local Area Connection** screen.

Your computer should get an IPv6 IP address (starting with 2002:7a64:dcee:1: in this example) from the ZyWALL/USG.

Window 7 > cmd > ipconfig

```
C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : localdomain
    IPv6 Address. . . . . : 2002:7a64:dcee:1:dc9:e2ff:7d32:19c9
    Temporary IPv6 Address. . . . . : 2002:7a64:dcee:1:393c:37d8:5564:8f34
    Link-local IPv6 Address . . . . . : fe80::dc9:e2ff:7d32:19c9%12
    IPv4 Address. . . . . : 192.168.1.34
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::b2b2:dcff:fe70:c1d8%12
                                192.168.1.1
```

Type **ping -6 ipv6.google.com** in a Command Prompt to test. You should get a response.

Window 7 > cmd > ping -6 ipv6.google.com

```
C:\Windows\system32>ping -6 ipv6.google.com

Pinging ipv6.1.google.com [2404:6800:4001:801::1000] with 32 bytes of data:
Reply from 2404:6800:4001:801::1000: time=69ms
Reply from 2404:6800:4001:801::1000: time=69ms
Reply from 2404:6800:4001:801::1000: time=69ms
Reply from 2404:6800:4001:801::1000: time=69ms
Ping statistics for 2404:6800:4001:801::1000
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 69ms, Maximum = 69ms, Average = 69ms
```

What Could Go Wrong?

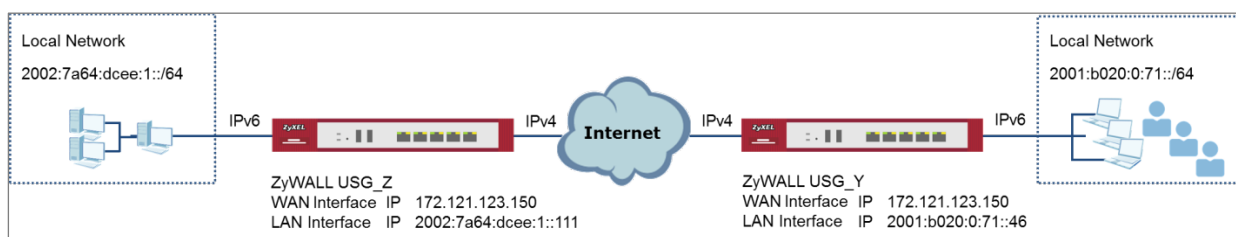
If your IPv6 connection is not working, please make sure you disable Auto-Configuration on the LAN1 IPv6 interface. Enabling it will cause two default routes, however, the ZyWALL/USG only needs a default route generated by your relay router setting. Also, make sure you enable the WAN1 IPv4 interface. In 6to4, the ZyWALL/USG uses the WAN1 IPv4 interface to forward your 6to4 packets over the IPv4 network.


In Windows, some IPv6 related tunnels may be enabled by default such as Teredo and 6to4 tunnels. It may cause your computer to handle IPv6 packets in an unexpected way. It is recommended to disable those tunnels on your computer.

How to Set Up an IPv6-in-IPv4 Tunnel

This example shows how to configure your ZyWALL/USG to create IPv6-in-IPv4 Tunnel. In this example, the ZyWALL/USG acts as IPv6-in-IPv4 routers which connect the IPv4 Internet and an individual IPv6 network. This configuration example only shows the settings on ZyWALL/USG_Z. You can use similar settings to configure ZyWALL/USG_Y.

ZyWALL/USG with IPv6-in-IPv4 Tunnel Example



 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the LAN IPv6 Interface on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > Interface > Ethernet > lan1**. Select **Enable Interface** and **Enable IPv6**. Type **2002:7a64:dcee:1::111/128** in the **IPv6 Address/Prefix Length** field for the LAN1's IP address.

Enable **Router Advertisement**. Then click **Add** in the **Advertised Prefix Table** to add **2002:7a64:dcee:1::/64**. The LAN1 hosts will get the network prefix through the router advertisement messages sent by the LAN1 IPv6 interface periodically. Click **OK**.

CONFIGURATION > Network > Interface > Ethernet > lan1 > General Settings

General Settings
☒ Enable Interface

General IPv6 Setting
☒ Enable IPv6 ⓘ

Interface Properties

| | |
|-----------------|---------------------------------|
| Interface Type: | internal ⓘ |
| Interface Name: | Lan1 |
| Port: | P5, P6 |
| Zone: | LAN1 ⓘ |
| MAC Address: | B8:EC:A3:A9:C0:0F |
| Description: | <input type="text"/> (Optional) |

IPv6 Address Assignment

| |
|--|
| <input type="checkbox"/> Enable Stateless Address Auto-configuration (SLAAC) |
| Link-Local Address: fe80::baec:a3ff:fea9:c00f/64 |
| IPv6 Address/Prefix Length: 2002:7a64:dcee::1111 (Optional) |

CONFIGURATION > Network > Interface > Ethernet > lan1 > IPv6 Router

Advertisement Setting

IPv6 Router Advertisement Setting
☒ Enable Router Advertisement

☒ Advance

Router Preference: Medium

☒ Advance

Advertised Prefix Table

+ Add Edit Remove

| # | IPv6 Address/Prefix Length |
|---|----------------------------|
| 1 | 2002:7a64:dcee:1::/64 |

Page 1 of 1 Show 50 items Displaying 1 -

Set Up the 6to4 Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > Interface > Tunnel > Add** and select **Enable**. Enter **tunnel0** as the **Interface Name** and select **IPv6-in-IPv4** as the **Tunnel Mode**. Select **wan1** as the gateway interface. Enter your **Remote Gateway Address** (172.121.123.150 in this example). Click **OK**.

CONFIGURATION > Network > Interface > Tunnel

General Settings

☒ Enable

Interface Properties

Interface Name: tunnel0

Zone: TUNNEL

Tunnel Mode: IPv6-in-IPv4

IPv6 Address Assignment

IPv6 Address/Prefix Length: (Optional)

Metric: 0 (0-15)

Gateway Settings

My Address

☒ Interface

ge2 DHCP client -- 10.214.30.82/255.255.255.0

☐ IP Address

0.0.0.0

Remote Gateway Address: 172.121.123.150

Set Up the Policy Route on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > Routing > IPv6**

Configuration > Add, click **Create New Object** to create an IPv6 address object with the address prefix of **2002:7a64:dcee:1::/64**. Select **Enable**. Select the address object you just created in the **Source Address** field. Select **any** in the **Destination Address** field. Select **Interface** as the **next-hop** type and then **tunnel0** as the interface. Click **OK**.

CONFIGURATION > Network > Routing > Policy Route > IPv6 Configuration

Add IPv6 Address Rule

Name: Lan1_subnet

Object Type: SUBNET

IPv6 Address Prefix: 2002:7a64:dcee:1::/6

Add Policy Route

Show Advanced Settings Create new Object ▼

Configuration

☒ Enable

Description: (Optional)

Criteria

User: any

Incoming: any (Excluding ZyV

Source Address: **Lan1_subnet**

Destination Address: any

DSCP Code: any

Schedule: none

Service: any

▼ Advance

Next-Hop

Type: **Interface**

Interface: **tunnel0**

Test the Result

Connect a computer to the ZyWALL/USG's LAN1.

Enable IPv6 support on your computer. In Windows XP, you need to use the IPv6 install command in a Command Prompt. In Windows 7, IPv6 is supported by default. You can enable IPv6 in the **Control Panel > Network and Sharing Center > Local Area Connection** screen.

Your computer should get an IPv6 IP address (starting with 2002:7a64:dcee:1: for this example) from the ZyWALL/USG.

Window 7 > cmd > ipconfig

```
C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : localdomain
    IPv6 Address. . . . . : 2002:7a64:dcee:1:dc9:e2ff:7d32:19c9
    Temporary IPv6 Address. . . . . : 2002:7a64:dcee:1:393c:37d8:5564:8f34
    Link-local IPv6 Address . . . . . : fe80::dc9:e2ff:7d32:19c9%12
    IPv4 Address. . . . . : 192.168.1.34
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::b2b2:dcff:fe70:c1d8%12
                                192.168.1.1
```

Use the ping -6 [IPv6 IP address] command in a Command Prompt to test whether you can ping a computer behind ZyWALL/USG_Y. You should get a response.

Window 7 > cmd > ping -6 2001:b020:0:71::46

```
C:\Windows\system32>ping -6 2001:b020:0:71::46

Pinging 2001:b020:0:71::46 with 32 bytes of data:

Reply from 2001:b020:0:71::46: time=21ms
Reply from 2001:b020:0:71::46: time=21ms
Reply from 2001:b020:0:71::46: time=21ms
Reply from 2001:b020:0:71::46: time=21ms

Ping statistics for 2001:b020:0:71::46
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 21ms, Maximum = 21ms, Average = 21ms
```

What Could Go Wrong?

If your IPv6 connection is not working, please make sure you enable the WAN1 IPv4 interface. In IPv6-in-IPv4, the ZyWALL/USG uses the WAN1 IPv4 interface to forward your 6to4 packets to the IPv4 network.

In Windows, some IPv6 related tunnels may be enabled by default such as Teredo and 6to4 tunnels. It may cause your computer to handle IPv6 packets in an unexpected way. It is recommended to disable those tunnels on your computer.

How to Update Firmware Automatically from a USB Storage

This example illustrates how to update the ZyWALL/USG's firmware automatically from a USB storage. With this feature, it is more efficient for users to upgrade the firmware for numerous devices without Internet or GUI access. The user can also downgrade the firmware by using this feature.

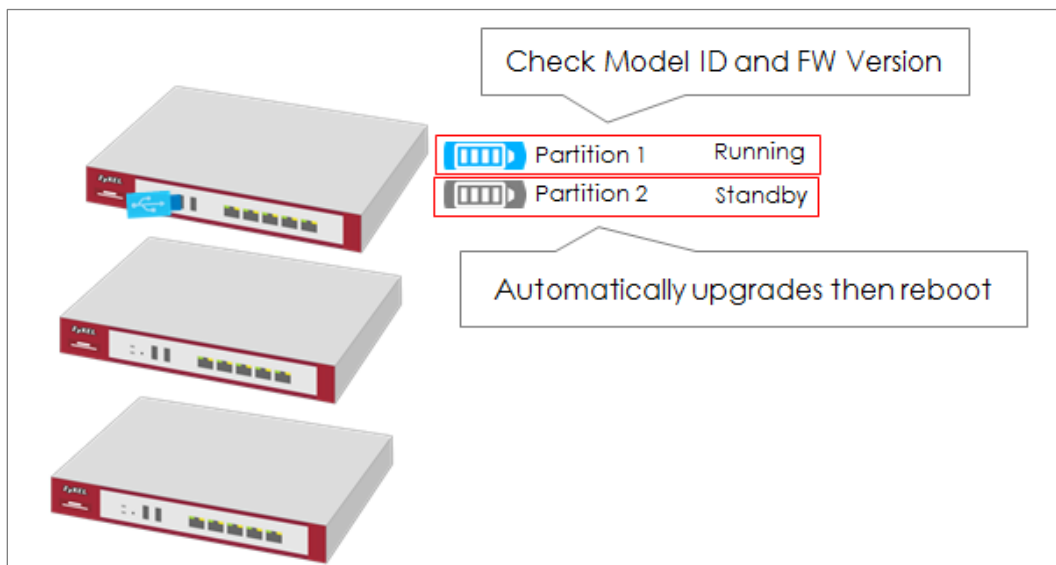



Figure 1 Automatic USB Firmware Upgrade

 **Note:** This feature does not support Device HA Pro firmware auto upgrade to passive devices. Do not use USB firmware upgrade on the devices with Device HA Pro function activated. This example was tested using the USG210 (Firmware Version: ZLD 4.25).

- 1 Enable the USB firmware upgrade function by CLI command.
- 2 Save the firmware on the USB.
- 3 Plug the USB into the device.
- 4 The device checks running partition for the model ID and the firmware version.
- 5 Upgrade the firmware to the standby partition and then the device reboots.

Enable the USB Firmware Upgrade Function by CLI Command

For security concerns, the function is disabled by default. The administrator needs to enable the function by the following CLI command:

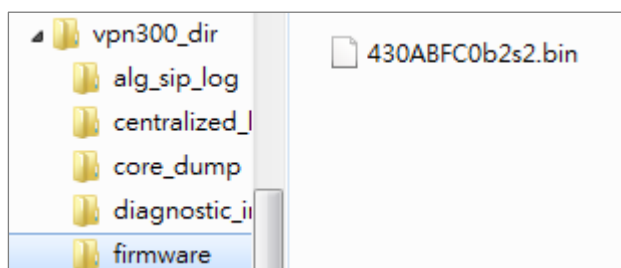
Router(config)# usb-storage update-firmware enable

Save the Firmware on the USB

There are two ways to create the firmware folder on the USB storage.

- 1 Follow the folder structure to create the firmware folder manually. It does not matter if the letters of the folder name are capitalized or not. For example: D:\vpn300_dir\firmware

Create the Firmware Folder Manually: Root Directory\vpn300_dir\firmware



- 2 Plug the USB storage to the device and the device will automatically create the folder **Vpn300_dir**, which includes the following sub-folders. Save the .bin file to the **firmware** folder.

centralized_log

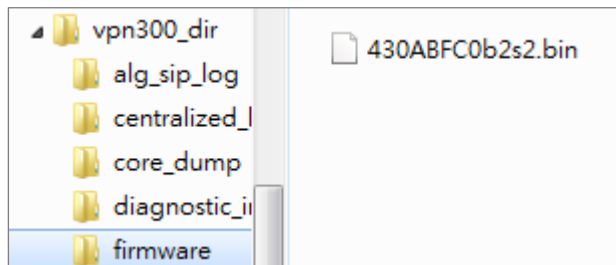
core_dump

diagnostic_info

firmware

packet_trace

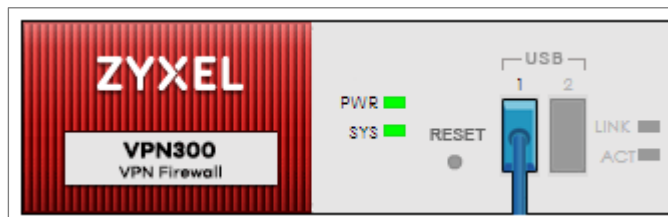
Firmware Folder is Created Automatically



Plug the USB into the Device

Once the .bin file in the firmware folder is detected, the device will copy it to the RAM.

Plug the USB storage into the USB port



The following message shows on the console if the device fails to copy the .bin file.

Router> USB update-firmware failed: firmware copy fail

The Device Checks Running Partition for the Model ID and the Firmware Version

The device checks the USB firmware with the running partition only. It does not check the standby partition.

1 Check model ID:

If incompatible, the device deletes the firmware in the RAM.

If compatible, the device checks the firmware version.

2 Check firmware version:

If it is the same as the running firmware, the device deletes the firmware in the RAM.

If it is not the same as the running version, the device starts to upgrade to the standby partition.

Check Model ID and Firmware Version

```
Router(config)# firmware verifying...
Product model id is compatible!!
This product's model id is E134
The kernel image supports the following product model id:
E134
firmware updating...
Please Wait about 5 minutes!!
```

Check Firmware Status

The device upgrades the standby partition and then reboots. After been upgraded to the standby partition, the device automatically reboots to switch from running to standby partition. The SYS LED starts to blink when the device begins to upgrade its firmware until the rebooting process is completed.

Check the Firmware Version on the Dashboard

| Device Information | | |
|--------------------------|--|--|
| System Name | Serial Number | MAC Address Range |
| <u>VPN300</u> | S172L15290016 | B8:EC:A3:A9:C0:0B ~ B8:EC:A3:A9:C0:12 |
| System Uptime | Boot Status | Firmware Version |
| 00:29:24 | OK | <u>V4.30(A8FC.0)b2 / 2017-07-28 22:44:54</u> |
| Firmware Upgrade License | Current Date/Time | |
| Activated | <u>2017-09-07 / 11:09:03 UTC+08:00</u> | |









MONITOR > Log > View log

| | | | |
|-----|--------|------|--|
| 254 | 201... | info | VPN300 is configured successfully with startup configuration file. |
|-----|--------|------|--|

What Can Go Wrong?

- 1 The USB storage must use the FAT16, FAT32, EXT2, or EXT3 file system.
Otherwise, it may not be detected by the ZyWALL/USG.
- 2 The device only checks the firmware under the specific folder.
Therefore, make sure the firmware is saved in the correct folder under the root directory: **\ProductName_dir\firmware**. For example:
\\vpn300_dir\firmware
- 3 If there are multiple firmware files in the firmware folder of one model, the device only checks the first one in order.

Multiple firmware files of one model in the same folder is not supported.

| | | | |
|---|-------------------------------------|-------------------|--------------------|
|  | 430_Internal_Release_Note_b2s2.docx | 2017/8/31 下午 0... | Microsoft Word ... |
|  | 430ABFC0b2s2.bin | 2017/8/31 下午 0... | BIN 檔案 |
|  | 430ABFC0b2s2.conf | 2017/8/31 下午 0... | CONF 檔案 |
|  | 430ABFC0b2s2.db | 2017/8/31 下午 0... | Data Base File |
|  | 430ABFC0b2s2.ri | 2017/8/31 下午 0... | RI 檔案 |
|  | 430ABFC0b2s2-MIB.zip | 2017/8/31 下午 0... | 壓縮的 (zipped) ... |
|  | ABFC119.bm | 2017/8/31 下午 0... | BM 檔案 |
|  | firmware.xml | 2017/8/31 下午 0... | XML Document |

- 4 Make sure the product model ID of the USB firmware is compatible with the device. The device writes logs on the console and device log if the firmware model ID is incompatible.

Console Message

```
Router(config)# firmware verifying...
Product model id is not compatible!!
This product's model id is E134
The ZLD-current image supports the following product model id :
E10B
USB update-firmware fail: File damaged. file name: 430AALA0a1.bin
```

MONITOR > Log > View log

| # | Time | Priority | Category | Message | Note |
|----|---------------------|----------|----------|---|--------------------|
| 20 | 2017-09-11 09:54... | alert | System | USB update-firmware fail: File damaged. file name: 430AALA0a1.bin | USB update firm... |

- Make sure the version of the USB firmware is different from that of the running partition. The device writes logs on the console and device log if the firmware version is the same as the running firmware.

Console Message

```
Router(config)# firmware verifying...
USB update-firmware fail: Same firmware version. file name: 430ABFC0b2s2.bin
```

MONITOR > Log > View log

| # | Time | Priority | Category | Message | Note |
|-----|---------------------|----------|----------|--|--------------------|
| 166 | 2017-09-11 09:42... | notice | System | Device do not have token to access cloud server [count=2] | System |
| 201 | 2017-09-11 09:42... | notice | System | Device do not have token to access cloud server [count=2] | System |
| 236 | 2017-09-11 09:41... | notice | System | Device do not have token to access cloud server [count=2] | System |
| 282 | 2017-09-11 09:40... | notice | System | Device do not have token to access cloud server [count=2] | System |
| 283 | 2017-09-11 09:40... | alert | System | USB update-firmware fail: Same firmware version. file name: 430ABFC0b2s2.bin | USB update firm... |
| 786 | 2017-09-11 09:26... | notice | System | Device do not have token to access cloud server [count=2] | System |

- This feature does not support the Device HA Pro firmware auto upgrade to passive devices. Do not use USB firmware upgrade on devices with

Device HA Pro function activated. When using USB firmware upgrade on a device HA or in a device HA Pro scenario, make sure you plug the USB storage to the passive device for firmware upgrade first. After the passive device has finished firmware upgrading through the USB, plug the USB storage to the active device for firmware upgrade.

How to Configure DHCP Option 60 – Vendor Class Identifier

The following figure depicts how the ZyWALL/USG uses DHCP option 60. By matching the VCI strings, a DHCP client can choose one specific DHCP server on the WAN network. This function is useful when there are several DHCP servers providing different services in an environment. Clients that need Internet service can be directed to the DHCP server which provides Internet connection information with the same option 60 string. IPTV clients may relay to another DHCP server which obtains IPTV service information.

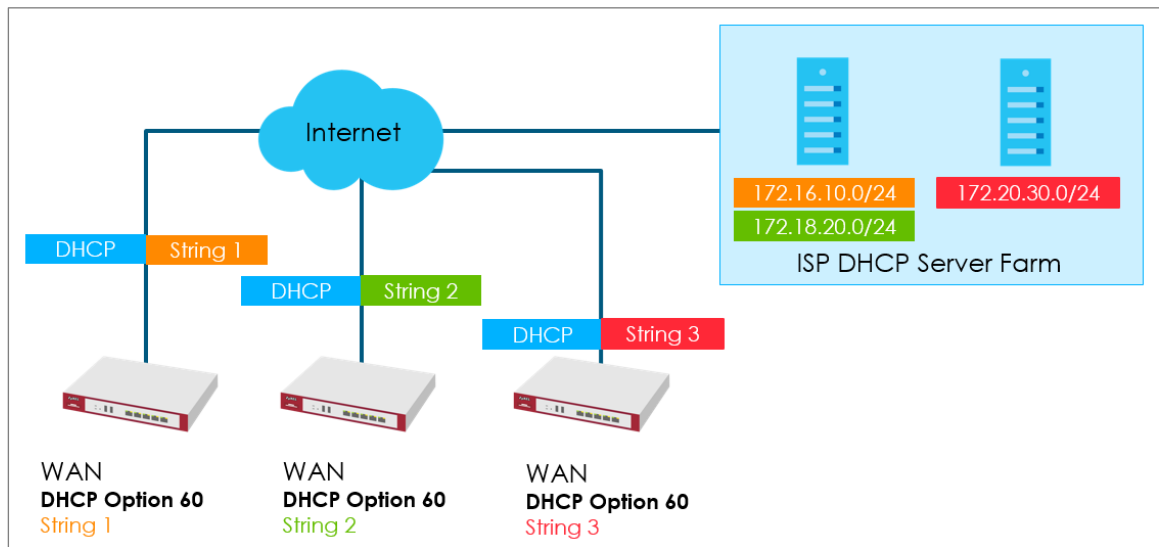


Figure 1 DHCP Option 60 Vendor Class Identifier

DHCP Option 60 Deployment Flow

- 1 Enable the WAN ports as DHCP clients (enabled by default).
- 2 Navigate to the WAN interface configuration screen.
- 3 Type in user defined option 60 string in the **Advance** setting section.

Setting Up DHCP Option 60 on the Web GUI

- 1 In the ZyWALL/USG's navigation panel, go to **Configuration > Network > Interface**.

Port Group

Ethernet

PPP

Cellular

Tunnel


VLAN


Bridge


VTI


Trunk


Configuration


 Edit









 Remove

 Activate

 Inactivate

 Create Virtual Interface

 Object References

| # | Sta... | Name | IP Address | Mask |
|---|---|------|------------------------|---------------|
| 1 |  | ge1 | STATIC -- 0.0.0.0 | 0.0.0.0 |
| 2 |  | ge2 | DHCP -- 10.214.30.65 | 255.255.255.0 |
| 3 |  | ge3 | DHCP -- 10.214.30.66 | 255.255.255.0 |
| 4 |  | ge4 | STATIC -- 192.168.91.1 | 255.255.255.0 |
| 5 |  | ge5 | STATIC -- 192.168.92.1 | 255.255.255.0 |
| 6 |  | ge6 | STATIC -- 192.168.93.1 | 255.255.255.0 |
| 7 |  | ge7 | STATIC -- 0.0.0.0 | 0.0.0.0 |
| 8 |  | ge8 | STATIC -- 0.0.0.0 | 0.0.0.0 |

«

«

Page

1

of 1

»

»

Show

50

▼

items

Displaying 1 - 8 of 8

- Click the **Ethernet** tab, go to **WAN > Edit**. Enter the VCI string in the **Advance** section of **DHCP Option 60**.

Edit Ethernet

Show Advanced Settings

General Settings

☒ Enable Interface

Interface Properties

Interface Type:

general

Interface Name:

ge1

Port:

P1

Zone:

OPT

MAC Address:

B8:EC:A3:A9:C0:0B

Description:

(Optional)

IP Address Assignment

☒ Get Automatically

☒ Advance

DHCP Option 60:

ZYXEL_CSO

(Optional)

☐ Use Fixed IP Address

IP Address:

0.0.0.0

OK

Cancel

Setting Up DHCP Option 60 on the CLI

Under the specific interface path, use these commands to:

Enable option 60

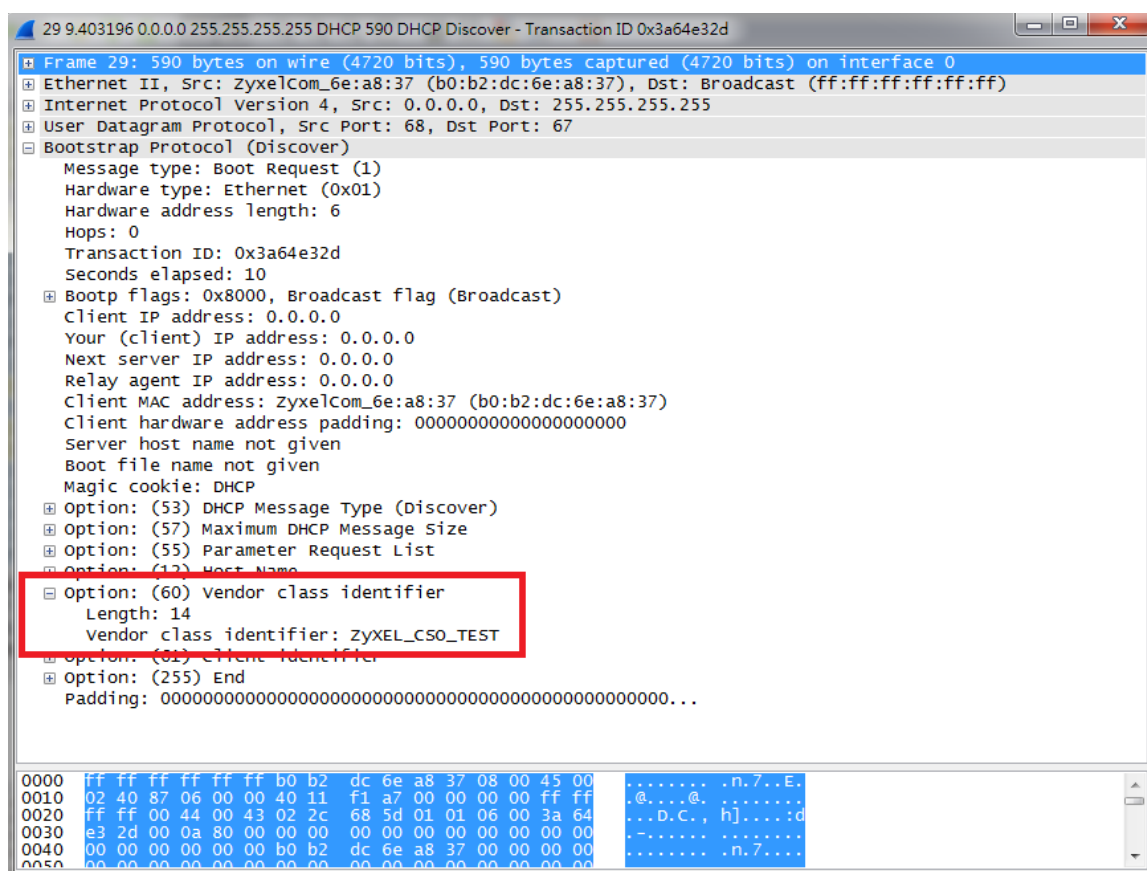
```
Router(config-if-wan1)# ip address dhcp option-60 {VCI_STRING}
```

Disable option 60

```
Router(config-if-wan1)# no ip address dhcp option-60
```

Test DHCP Option 60

To test the DHCP option 60 function, use a packet capture software to check if option 60 string exists in the DHCP discover message sent from the ZyWALL/USG WAN port.

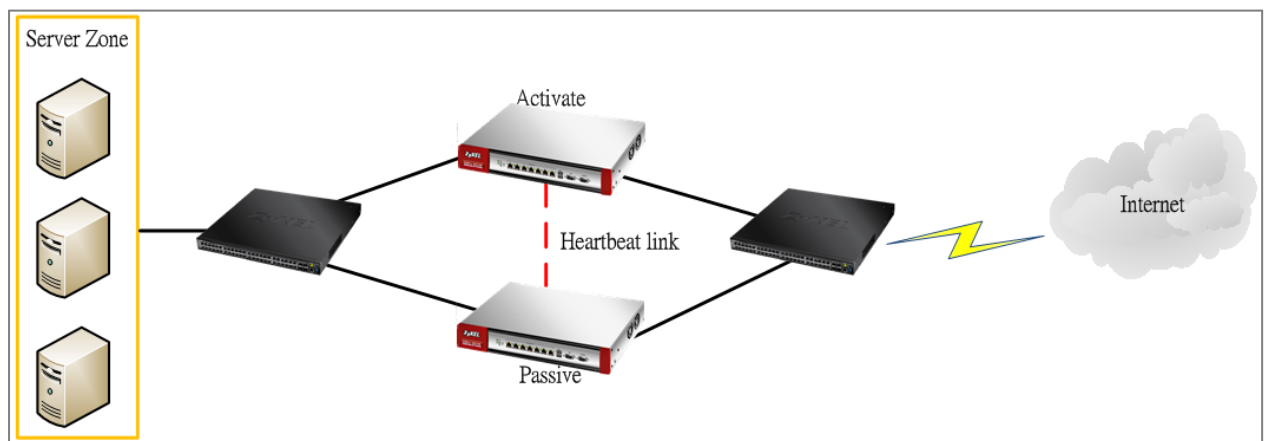


What Can Go Wrong?

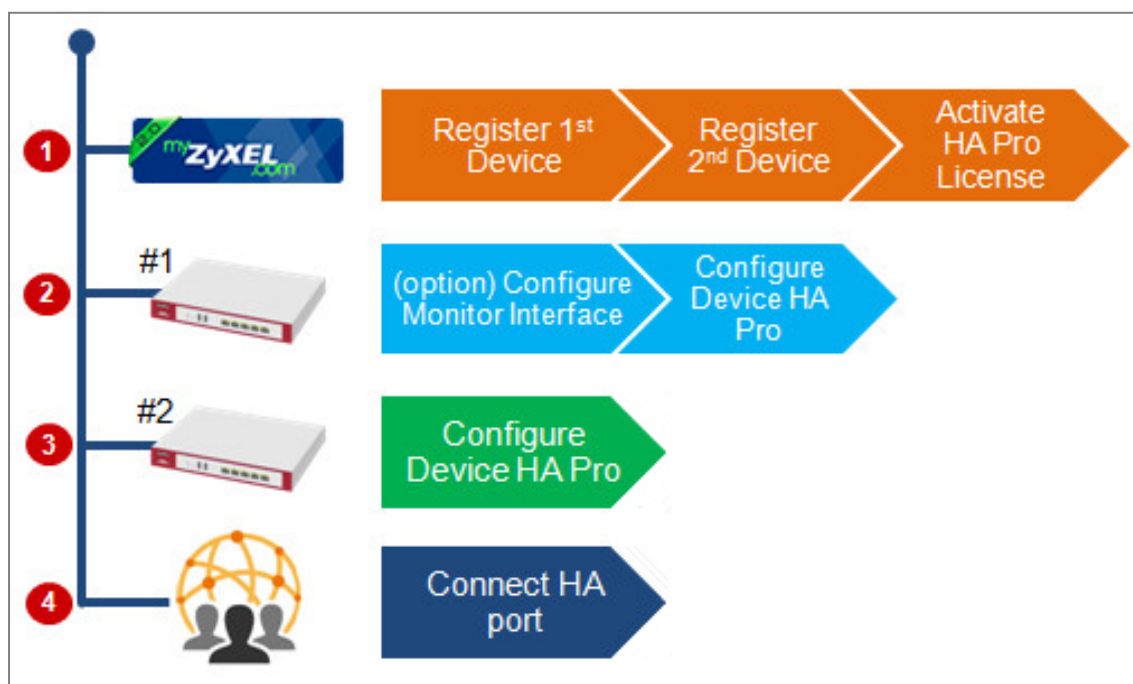
- 1 Avoid using the same option 60 string on two or more DHCP servers. It may cause duplicate DHCP serving confliction.
- 2 Since packets with option 60 are clear, do not consider it as a secure way for DHCP server authentication.

How to Configure Device HA Pro

The Device HA feature acts as a failover when one of the devices in the network is dead or can't access the Internet. Therefore, this is a popular feature for network environments. In the previous firmware version, the USG supports AP (Activate-Passive/Master-Backup) mode. In V4.25, the Device HA feature is enhanced and named **Device HA Pro**.



In Device HA Pro, a "heartbeat link" is added for monitoring the interface status and synchronizing settings. Follow the steps below to deploy the Device HA Pro feature in your network environment.



Device HA Pro License

The Device HA Pro feature is license required. You must register both of your devices on the **myZyXEL.com** server first. Then make sure the Device HA Pro license is available on both of your devices.

| Registration Service | | | | | |
|----------------------|--|--------------|--------------|-----------------|-------|
| Service Status | | | | | |
| # | Service | Status | Service Type | Expiration Date | Count |
| 1 | Content Filter 2.0 | Activated | Trial | 2017-10-20 | N/A |
| 2 | Geo Enforcer | Activated | Standard | 2018-10-21 | N/A |
| 3 | Managed AP Service | Default | Standard | | 4 |
| 4 | SSL VPN Service | Default | | | 50 |
| 5 | Zymesh Service | Not Licensed | | | N/A |
| 6 | Hotspot Management Subscription Ser... | Activated | Trial | 2017-10-20 | N/A |
| 7 | Concurrent Device Upgrade | Default | Standard | | 200 |
| 8 | Device HA Pro | Activated | Standard | | N/A |
| 9 | Firmware Upgrade Service | Activated | | | N/A |

Page 1 of 1 Show 50 items

Service Refresh
Service License Refresh

Note:
 Update device license information from myZyXEL.com server. If you want to activate license, please go to portal.myzyxel.com

Behavior of the Device HA Pro

The behavior of the Device HA Pro includes a heartbeat link to monitor the “activate” device’s interface status. If one of the monitored interfaces is dead or fails, the “passive” device’s status will become “activate”. (This means only 1 device’s status can be “activate” at a time.)

Be aware that the Device HA status of the devices might constantly change due to the network environment situation. In the current firmware design, Device HA Pro will not fallback when the primary device interface is working normally again.

Device-HA Pro Setting Screen

A. Enable configuration provisioning on the activated device

This function is for the secondary device. If you are configuring the primary device, this function is unnecessary.

B. Serial number of the licensed device for license synchronization

Entering the serial number of license from the **myZyXEL.com** server.

C. Configure the Device HA Pro interface

Enter the management IP address of the active and passive devices. Also, enter the password for synchronizing configuration with each other.

D. Monitoring Interfaces

Select the interfaces which you would like to monitor.

E. Synchronization

Enable failover when one of the interfaces fails.

Device HA Status

Device HA Pro

View Log

Configuration

☐ Enable Configuration Provisioning From Active Device.

Serial Number of Licensed Device for License Synchronization:

S172L15290017

Active Device Management IP:

20.20.20.1

Passive Device Management IP:

20.20.20.2

Subnet Mask:

255.255.255.0

Password:

....

Retype to Confirm:

....

Heartbeat Interval:

2

seconds (1-10)

Heartbeat Lost Tolerance:

2

(1-10)

Monitor Interface

Available Interfaces

=== Object ===

ge3

ge4

ge5

ge6

Monitor Interface

=== Object ===

ge1

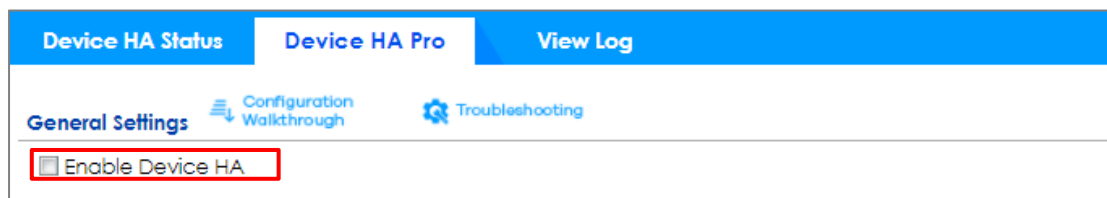
ge2

Failover Detection

☒ Enable Failover When Interface Failure (Option)

☐ Enable Failover When Device Service Fails (Option)

The Main Function of the Device HA Pro



Heartbeat Link

The heartbeat port is a new physical port on the device.

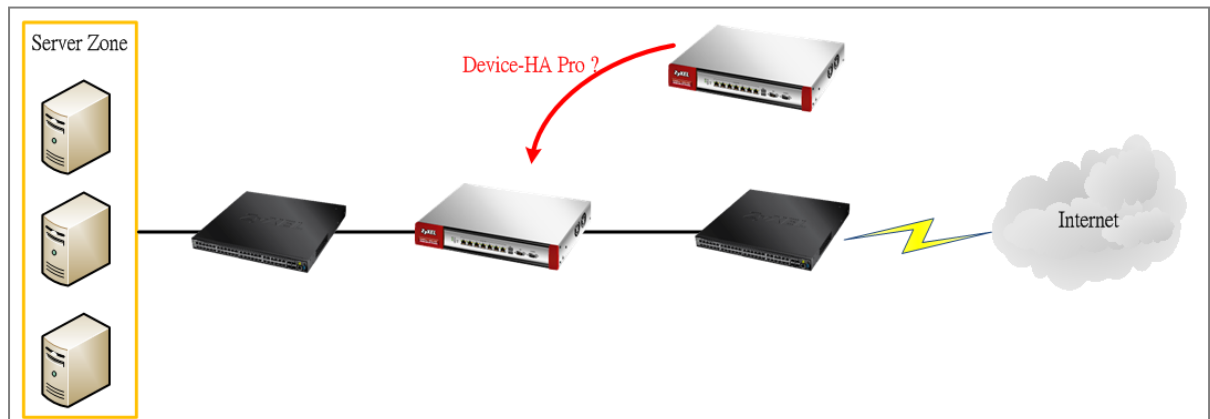
After you have enabled Device HA Pro, the devices will transmit multicast packets (UDP 694) to check each device's status.

When the passive device is working properly, the system LED light will be on. Only the heartbeat port's LED light can be on.

Suggestions

1. Transfer all the licenses to the primary device. This helps to avoid the system from recounting licenses every time.
2. Enable the connectivity check function on the monitored interfaces. When an interface doesn't receive any response from the remote server for a certain period of time, the device will consider the interface status as fail. Then the Device HA Pro feature will change the status of the interface.

How do I Configure Device HA Pro in My Current Environment?



License

The Device HA Pro feature is license required. Please go to register both of your devices on **myZyXEL.com** and make sure the devices have the license after syncing with the **myZyXEL.com** server.

| Registration | | | | | |
|---|--|--------------|--------------|-----------------|-------|
| Service | | | | | |
| Service Status | | | | | |
| # | Service | Status | Service Type | Expiration Date | Count |
| 1 | Content Filter 2.0 | Activated | Trial | 2017-10-20 | N/A |
| 2 | Geo Enforcer | Activated | Standard | 2018-10-21 | N/A |
| 3 | Managed AP Service | Default | Standard | | 4 |
| 4 | SSL VPN Service | Default | | | 50 |
| 5 | Zymesh Service | Not Licensed | | | N/A |
| 6 | Hotspot Management Subscription Ser... | Activated | Trial | 2017-10-20 | N/A |
| 7 | Concurrent Device Upgrade | Default | Standard | | 200 |
| 8 | Device HA Pro | Activated | Standard | | N/A |
| 9 | Firmware Upgrade Service | Activated | | | N/A |
| Page 1 of 1 Show 50 items | | | | | |
| Service Refresh | | | | | |
| Service License Refresh | | | | | |
| Note: Update device license information from myZyXEL.com server. If you want to activate license, please go to portal.myzyxel.com | | | | | |

Configurations on the Primary Device

1. Go to the **Configuration > Device HA > Device HA Pro** screen.
2. Enter the device's license serial number from the **myZyXEL.com** server.
3. Enter the management IP address after enabling the Device HA Pro feature.
4. Select the interfaces which you would like to monitor.
5. Enable failover when an interface fails.
6. Click **Apply**.

Device HA Status

Device HA Pro

View Log

Configuration

☐ Enable Configuration Provisioning From Active Device.

Serial Number of Licensed Device for License Synchronization:

S172L15290017

Active Device Management IP:

20.20.20.1

Passive Device Management IP:

20.20.20.2

Subnet Mask:

255.255.255.0

Password:

....

Retype to Confirm:

....

Heartbeat Interval:

2

seconds (1-10)

Heartbeat Lost Tolerance:

2

(1-10)

Monitor Interface

Available Interfaces

=== Object ===

ge3

ge4

ge5

ge6

...

Monitor Interface

=== Object ===

ge1

ge2

Failover Detection

☒ Enable Failover When Interface Failure (Option)

☐ Enable Failover When Device Service Fails (Option)

Go to the **Configuration > Device HA > General** screen.

Select **Enable Device HA** and click **Apply** to enable Device HA Pro.

Device HA Status

Device HA Pro

View Log

General Settings

[Configuration Walkthrough](#)
[Troubleshooting](#)

☒ Enable Device HA

Configurations on the Secondary Device

Go to the **Configuration > Device HA > Device-HA Pro** screen.

Select **Enable Configuration Provisioning from Active Device**.

Click **Apply**.

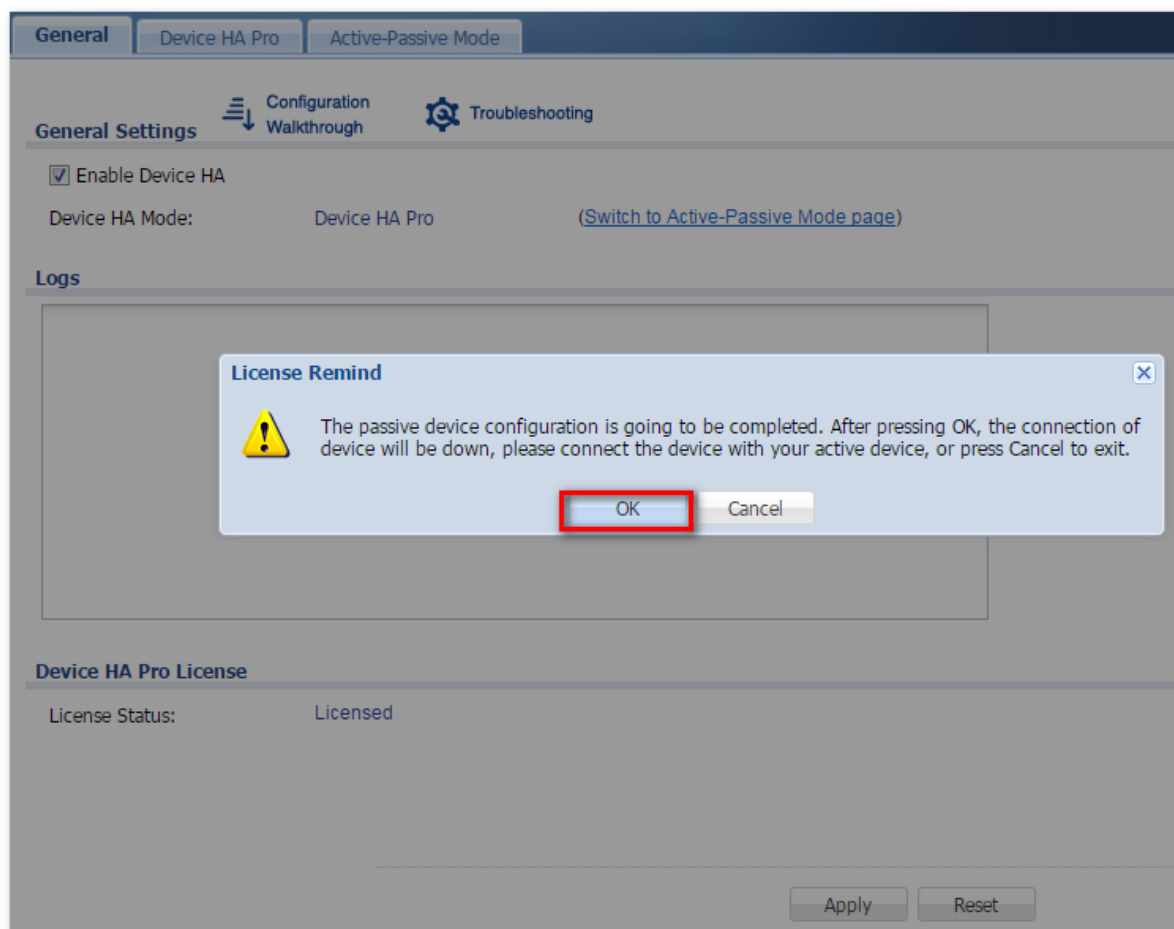
| Device HA Status | Device HA Pro | View Log |
|---|---------------|---|
| Configuration | | |
| <input checked="" type="checkbox"/> Enable Configuration Provisioning From Active Device | | |
| Serial Number of Licensed Device for License Synchronization: | | <input type="text"/> |
| Active Device Management IP: | | <input type="text"/> |
| Passive Device Management IP: | | <input type="text"/> |
| Subnet Mask: | | <input type="text"/> |
| Password: | | <input type="text"/> |
| Retype to Confirm: | | <input type="text"/> |
| Heartbeat Interval: | | <input type="text" value="2"/> seconds (1-10) |
| Heartbeat Lost Tolerance: | | <input type="text" value="2"/> (1-10) |
| Monitor Interface | | |
| <div>Available Interfaces</div> <div>=== Object ===</div> <div> ge1 ge2 ge3 ge4 </div> | | <div>Monitor Interface</div> <div></div> |
| Failover Detection | | |
| <input type="checkbox"/> Enable Failover When Interface Failure (Option) | | |
| <input type="checkbox"/> Enable Failover When Device Service Fails (Option) | | |

Go to the **Configuration > Device HA > General** screen.

Select **Enable Device HA** and click **Apply**.

Before the Device HA Pro feature is enabled on the secondary device, a **warning message** will pop-up for you to confirm. Click **OK** to enable it.

不會顯示這個訊息



1. Connecting the Device HA Pro Port

The Device HA Pro port is a new physical port on the DUT. You can use a cable to connect the devices with each other.

What can go wrong?

1. Why I can't see correct license status from myzyxel.com server?

On the Device-HA Pro setting, there is a function "Serial number of the licensed device for license synchronization". You should enter device's S/N which with licenses. So you can transfer all of the licenses to "Activate" device, and enter this device's S/N in frame.

2. Why nothing happened after enabled Device-HA Pro?

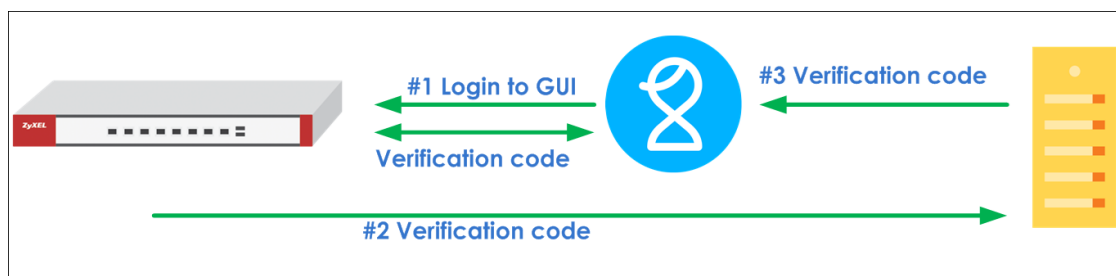
After you enabled Device-HA Pro, the secondary device will not forward any traffic any more except the latest physical port. So you must confirm the physical port already connected with each other.

3. Why after Device-HA failover to secondary device, it will not fallback to primary device?

Because Device-HA Pro purpose is for networking environment stability, so after mechanism failover to secondary device it will keep the latest status even primary device is back. It can avoid the network service unstable.

How to setup Two-Factor Authentication for admin login

2 Factor Authentication is a function can prevent your device login by hacker. It needs additional verification code after logged into WebGUI/SSH/Telnet



You can follow these steps to setup 2 factor authentication when logging to system.

Setup SMTP function on your device

Go to **CONFIGURATION > System > Notification > Mail Server** Field your SMTP serve configuration.

- Mail server
- Mail server ports
- Mail From
- SMTP Authentication

Mail Server

SMS

General Settings

Mail Server:

smtp.gmail.com

(Outgoing SMTP Server Name or IP Address)

Mail Subject:

☐ Append system name
 ☐ Append date time

Mail Server Port:

587

☒ TLS Security
 ☒ STARTTLS
 ☐ Authenticate Server

Mail From:

s.y@gn

(Email Address)

☒ SMTP Authentication

User Name :

s.y

Password:

.....

Retype to Confirm:

.....

Schedule

Time For Sending Report:

0

(hours)

0

(minutes)

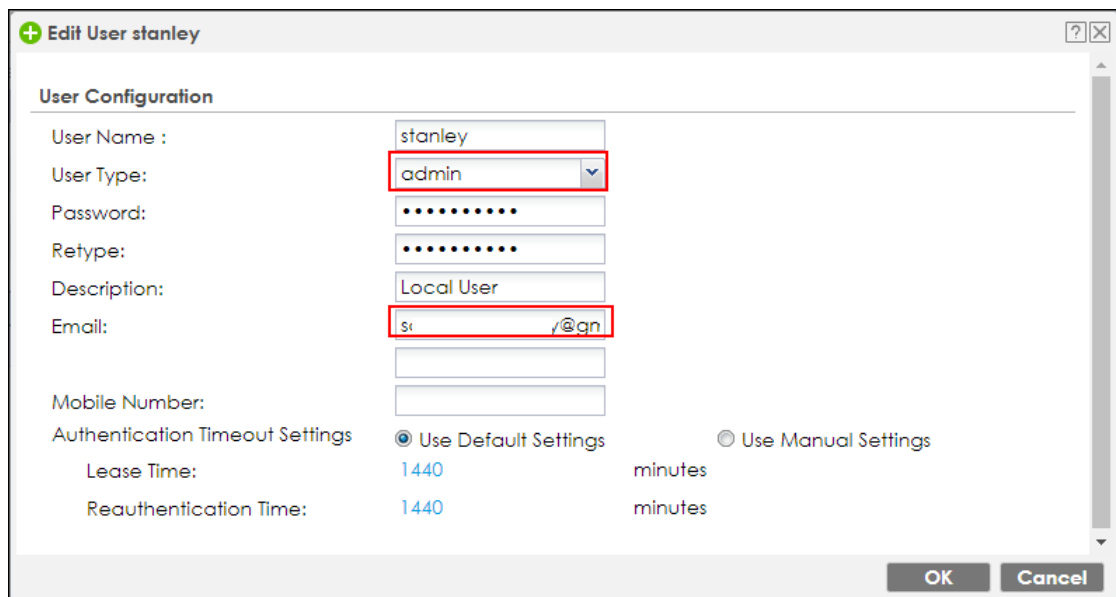


Note: Must make sure SMTP Server configuration is correct otherwise user will unable receive mail successfully.

Create admin type user on device

Go to **Configuration > Object > User/Group > User Click** Add button to create an user and user type is admin.

And also entered email address of this user.



Edit User stanley

User Configuration

User Name : stanley

User Type: admin

Password:

Retype:

Description: Local User

Email: st...@qn...

Mobile Number:

Authentication Timeout Settings

☒ Use Default Settings ☐ Use Manual Settings

Lease Time: 1440 minutes

Reauthentication Time: 1440 minutes

OK Cancel

Setup Two-Factor Authentication for admin on your device

Go to **Configuration > Object > Auth Method > Two-Factor Authentication >**

Admin Access

Enable the function and add admin user which you added in step2 in the rule, and you can select what services are 2 Factor authentication needed.

Authentication Method **Two-factor Authentication**

VPN Access **Admin Access**

General Settings

☒ Enable

Valid Time: (1-5 minutes)

Two-factor Authentication for Services:

☒ Web ☒ SSH ☒ TELNET

User

Selectable User Objects

=== Object ===

admin

→

←

Selectable User Objects

=== Object ===

stanley

Delivery Settings

Deliver Authorize Link Method: ☐ SMS ☒ Email

Test the Result

After setup these steps and login to device by admin user, the verification code is required.

Web Service:

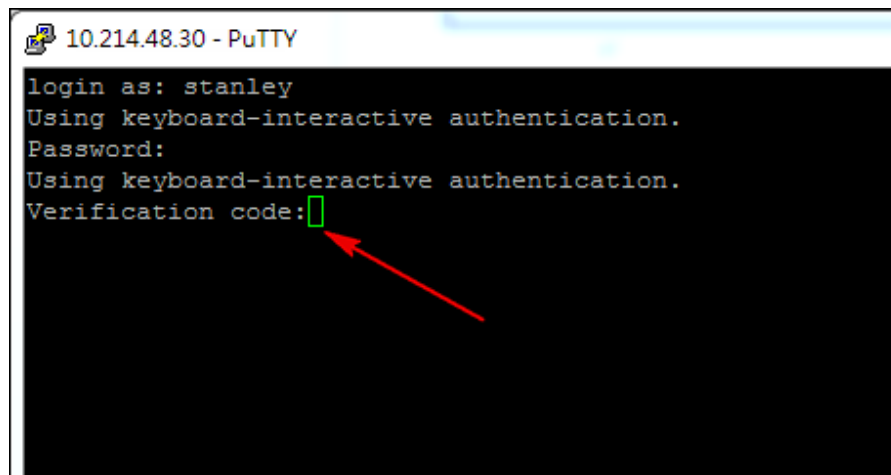
ZYXEL

ATP500

Enter Two-factor Authentication Verification code and click to verify.

Verify

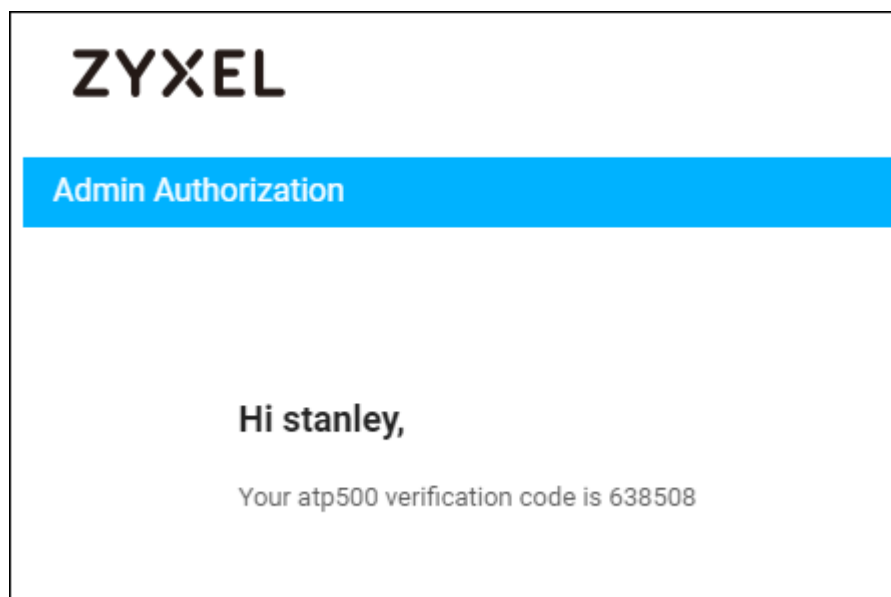
SSH Service:



A screenshot of a PuTTY terminal window titled "10.214.48.30 - PuTTY". The terminal shows a login sequence: "login as: stanley", "Using keyboard-interactive authentication.", "Password:", "Using keyboard-interactive authentication.", and "Verification code:". A green rectangular cursor is positioned after the "Verification code:" prompt, and a red arrow points to it from the right side of the terminal.

```
10.214.48.30 - PuTTY
login as: stanley
Using keyboard-interactive authentication.
Password:
Using keyboard-interactive authentication.
Verification code: 
```

You will receive verification code by Email.



A screenshot of a web page titled "ZYXEL" with a blue header bar containing the text "Admin Authorization". Below the header, the page displays a personalized message: "Hi stanley," followed by "Your atp500 verification code is 638508".

ZYXEL

Admin Authorization

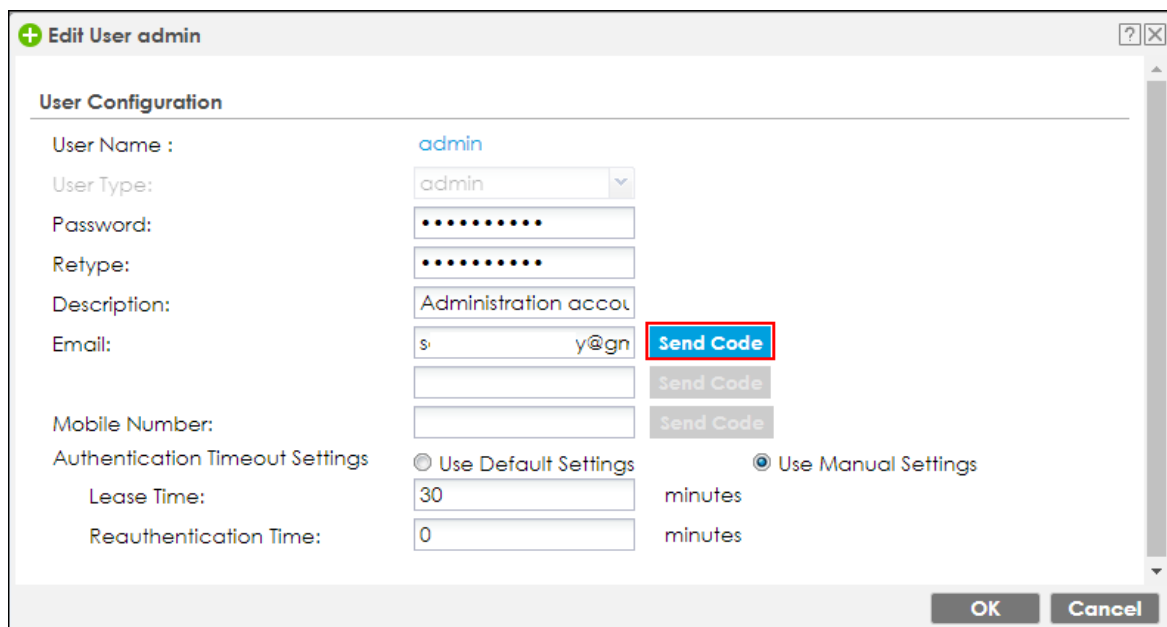
Hi stanley,

Your atp500 verification code is 638508

What Can Go Wrong?

1. **Must make sure SMTP server configuration is correct.**
2. **If you would like to add “admin” into the 2FA rule, you must do verify admin email first**

2-1 Enter Email address and click “send code” button



Edit User admin

User Configuration

User Name : admin

User Type: admin

Password:

Retype:

Description: Administration account

Email: s. y@gn **Send Code**

Mobile Number:

Authentication Timeout Settings: ☐ Use Default Settings ☒ Use Manual Settings

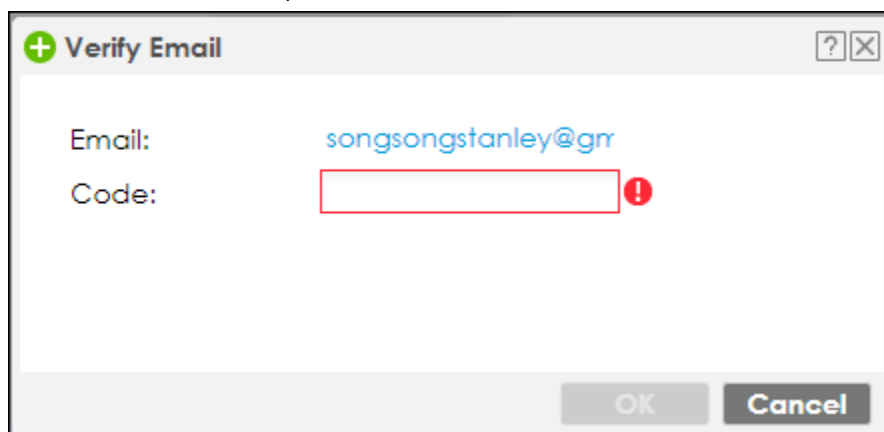
Lease Time: 30 minutes

Reauthentication Time: 0 minutes

OK Cancel

2.2 After clicked “Send Code”, you will receive code by Email.

2.3 Enter code that you received.



Verify Email

Email: songsongstanley@gmr

Code: [Red Box] !

OK Cancel

2.4 After admin Email is verified, it will display success.

+

Edit User admin

?

×

User Configuration

User Name :

admin

User Type:

admin

Password:

.....

Retype:

.....

Description:

Administration accou

Email:

s

/@gn

✓

Send Code

Mobile Number:

Send Code

Authentication Timeout Settings

Use Default Settings

Use Manual Settings

Lease Time:

30

minutes

Reauthentication Time:

0

minutes

OK

Cancel

How to configure Email Security for Phishing mail?

(This feature is only supported on ATP series)

The following depicts a sample configuration of Email security for Phishing mail.

Phishing is a type of online scam where criminals send an email with a fake website and asking you to provide sensitive information.

An example of phishing attack:

1. Attacker creates an fake banking websites which copy the content from real banking website
2. Attacker sends user an phishing emails with an embed URLs to ask change the new banking password
3. User opens the mail then click to the embed URLs, it redirects user access to fake banking websites.
4. User enters the current banking account when they attempt change the password
5. Attacker gets the user's banking account and can steal user's money

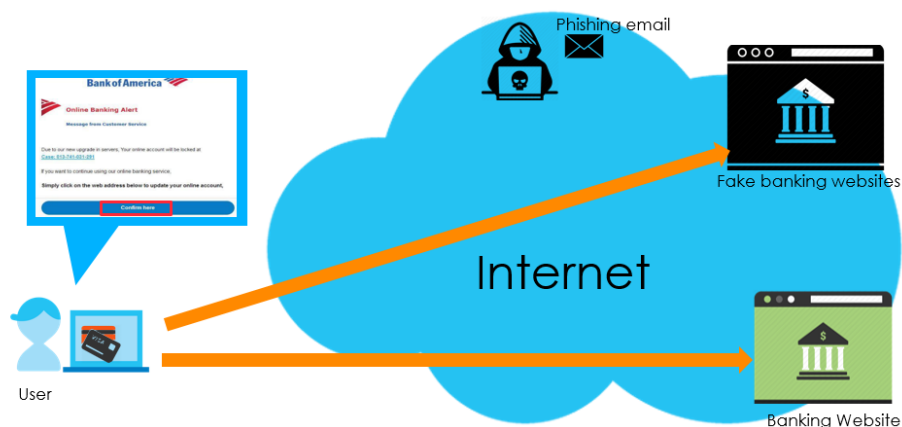


Figure 1 Using Sandboxing to Detect Unknown Malware

How it works

Gateway inspects the email content to detect the embedded URLs. With Anti-phishing enhancement, ATP gateway inspects the mail content to detect the

embedded URLs.

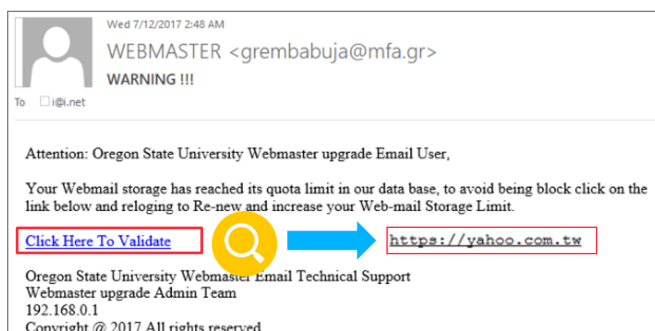
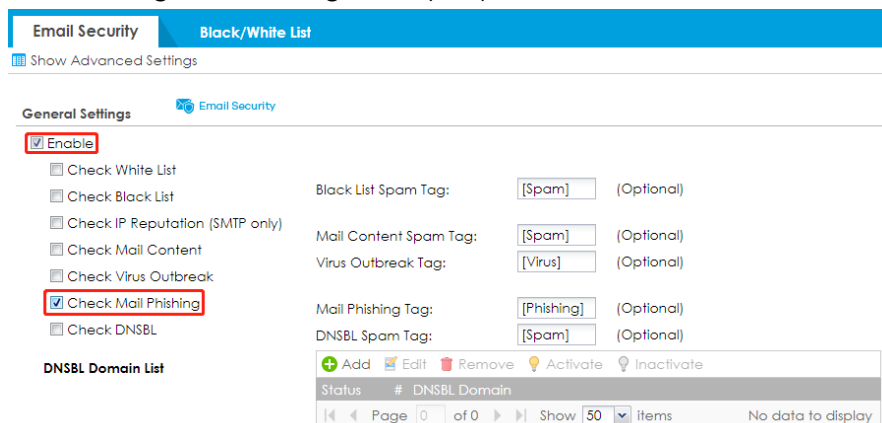


Figure 2 Phishing mail example

Set up Phishing on ATP

In the ATP, Go to **Configuration > Security Service > Email Security** to enable Check Mail Phishing that allows gateway inspects the embed URLs in the email



Test the Result

- 1 Go to **Monitor > Security Statistics > Email Security** to observe mail phishing logs

Monitor > Security Statistics > Email Security

| Time | Prior... | Category | Message | Source | Destination | Note |
|--------|----------|-------------|--|-------------------|-----------------|----------|
| 201... | info | Anti-Spam | SMTP Mail Phishing match, Rule_id=1, Mail From:bbb@ssskkk.com.tw phishing host:websectest.ctmail.com | 192.168.2.33:1766 | 192.168.22.1... | MAIL ... |
| 201... | alert | AP Firmware | AP firmware synchronize cloud server failed. | | | |
| 201... | error | myZyXEL.com | Skip get_time_zone, parameter missing! | | | |
| 201... | notice | myZyXEL.com | GetTimeZone: Processing... | | | |
| 201... | alert | AP Firmware | AP firmware synchronize cloud server failed. | | | |
| 201... | info | DHCP | Sending ACK to 192.168.2.33 | | | DHCP ... |

- 2 Go to **Monitor > Security Statistics > Email Security** to collect Email security statistics

| Summary | | Status |
|---|--|--------|
| General Settings | | |
| <input checked="" type="checkbox"/> Collect Statistics | | |
| <div> <div>Apply</div> <div>Reset</div> <div>Refresh</div> <div>Flush Data</div> </div> | | |
| Email Summary | | |
| Total Mails Scanned: | | 1 |
| Clear Mails: | | 0 |
| Clear Mails Detected by White List: | | 0 |
| Spam Mails: | | 0 |
| Spam Mails Detected by Black List: | | 0 |
| Spam Mails Detected by IP Reputation: | | 0 |
| Spam Mails Detected by Mail Content: | | 0 |
| Spam Mails Detected by Mail Phishing: | | 1 |
| Spam Mails Detected by DNSBL: | | 0 |
| Spam Mails with Virus Detected by Mail Content: | | 0 |
| Virus Mails: | | 0 |
| Query Timeout: | | 0 |

What Can Go Wrong?

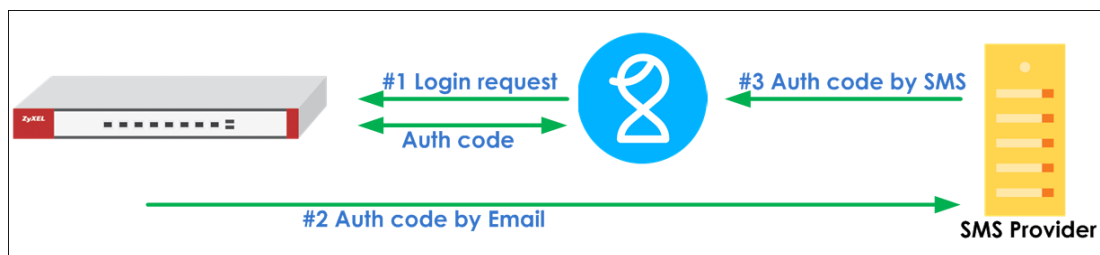
- 1 Make sure the Anti-Spam default service port is SMTP or POP3 by CLI
Router# show utm-manager anti-spam defaultport

```
Router# show utm-manager anti-spam defaultport
No.      Proto      Port
-----
1        smtp      25
2        pop-3     110
```

- 2 It does not support SSL inspection.
- 3 The ATP can inspect email up to 50KB. If the mail size greater than 50KB, gateway will inspect the first 50KB from the header

How to setup Email to SMS

The Email to SMS function can help to send the SMS to client. The SMS message is initiated from device to SMS provider, and then SMS provider send the SMS to client. This function can help to make sure user receives SMS if client without Internet connection.



You can follow these steps to Email to SMS.

Setup SMTP function on your device

Go to **CONFIGURATION > System > Notification > Mail Server** Field your SMTP serve configuration.

- A. Mail server
- B. Mail server ports
- C. Mail From
- D. SMTP Authentication

Mail Server

SMS

General Settings

Mail Server:

smtp.gmail.com

(Outgoing SMTP Server Name or IP Address)

Mail Subject:

☐ Append system name
 ☐ Append date time

Mail Server Port:

587

☒ TLS Security
 ☒ STARTTLS
 ☐ Authenticate Server

Mail From:

s.y@gn

(Email Address)

☒ SMTP Authentication

User Name :

s.y

Password:

.....

Retype to Confirm:

.....

Schedule


Time For Sending Report:

0

(hours)

0

(minutes)

 Note: Must make sure SMTP Server configuration is correct otherwise message will unable send to SMS provider successfullv.

Setup Email to SMS Provider configuration

Go to **“Configuration > system > Notification > SMS Select “SMS Provider”** as Email to SMS Provider. Enter SMS Provider Email server domain name.

And configuring sender mail address in “Mail From”

Mail Server

SMS

General Settings

☒ Enable SMS

Default country code for phone number:

0

(1-4) digit

SMS Provider:

Email-to-SMS Provider

Provider Domain:

email.smsglobal.com

SMS Provider Email domain

☒ auto append to "Mail to"

Mail Subject:

SMS Message

(Optional)

Mail From:

s.y@gmail.com


Email address

(Optional)

Mail To:

\$mobile_number\$


@email.smsglobal.com

 **Note**

1. If you select to use an Email-to-SMS provider, configure a mail server before you enable SMS.

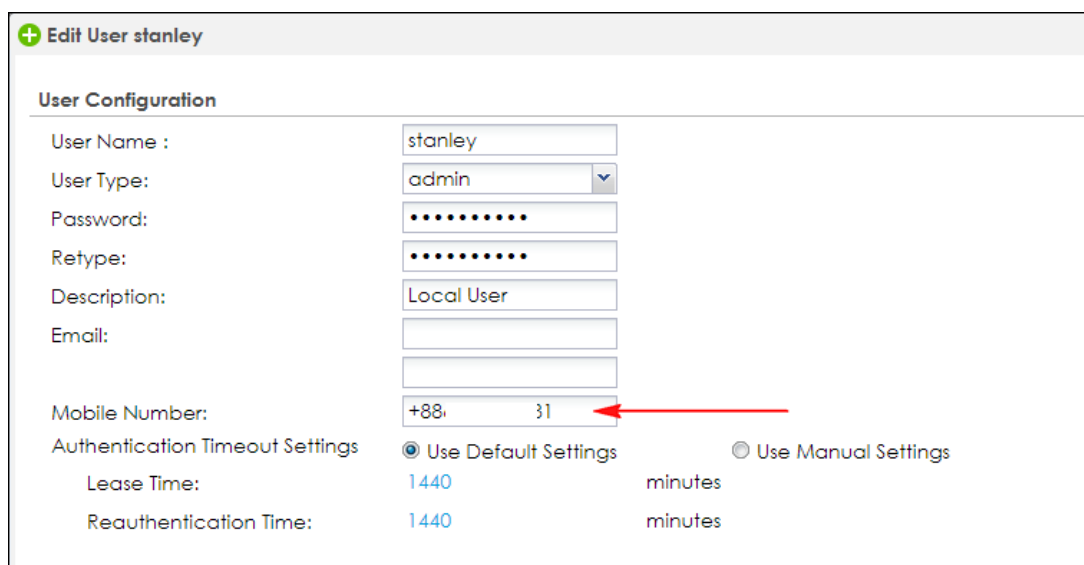
2. If you leave the Mail From field blank here, the system automatically uses the mail address configured in the Mail Server screen.

3. "Mail To" default format is "\$mobile_number\$@provider domain" and some Service Providers might require prefix symbol like "+" added before \$mobile_number\$.

 Note: Your SMS provider has to allow the email address which configured in “Mail From” to prevent the email is denied by SMS provider's mailbox.

Create admin type user on device

Go to **Configuration > Object > User/Group > User** Click Add button to create an user and user type is admin. And also entered phone number of this user.



Edit User stanley

User Configuration

User Name : stanley

User Type: admin

Password:

Retype:

Description: Local User

Email:

Mobile Number: +88: 31

Authentication Timeout Settings

☒ Use Default Settings ☐ Use Manual Settings

Lease Time: 1440 minutes

Reauthentication Time: 1440 minutes

Setup Two-Factor Authentication for admin on your device

Go to **Configuration > Object > Auth Method > Two-Factor Authentication > Admin Access**

Enable the function and add admin user which you added in step3 in the rule, and you can select what services are 2 Factor authentication needed. Enable SMS function to send verification code by SMS.

Authentication Method

Two-factor Authentication

VPN Access

Admin Access

General Settings

☒ Enable

Valid Time: (1-5 minutes)

Two-factor Authentication for Services:

☒ Web
 ☒ SSH
 ☒ TELNET

User

Selectable User Objects

=== Object ===

admin

+

-

Selectable User Objects

=== Object ===

stanley

Delivery Settings

Deliver Authorize Link Method: ☒ SMS ☐ Email

Test the Result


After setup these steps and login to device by admin user, the verification code is required.


Web Service:

ZYXEL

ATP500

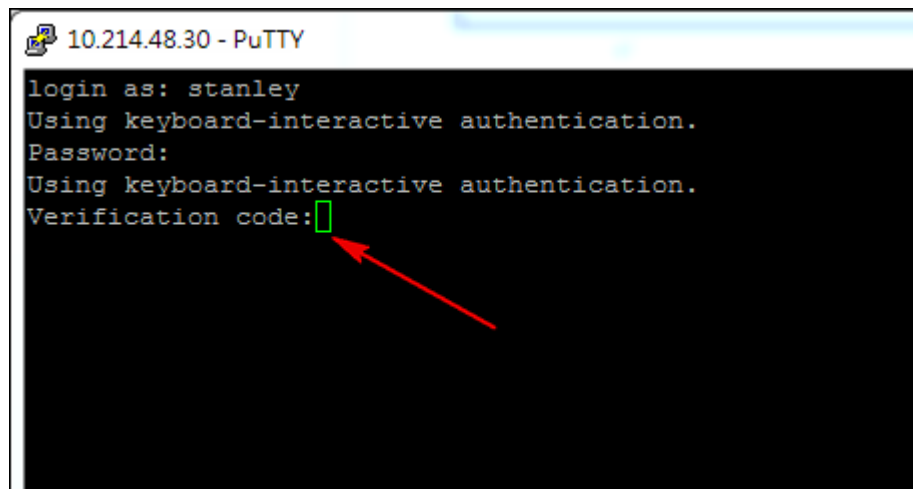
Enter Two-factor Authentication Verification code and click to verify.



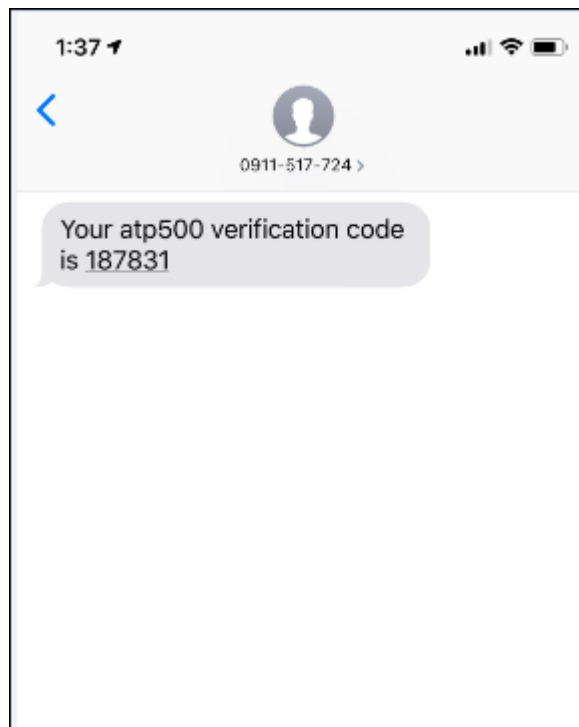


Verify

SSH Service:



You will receive verification code by SMS.



What Can Go Wrong?

- 1 Must make sure SMTP server configuration is correct.
- 2 Must make sure your SMS provider is supported Mail to SMS function.
- 3 Make sure your email address is allowed by your SMS provider.

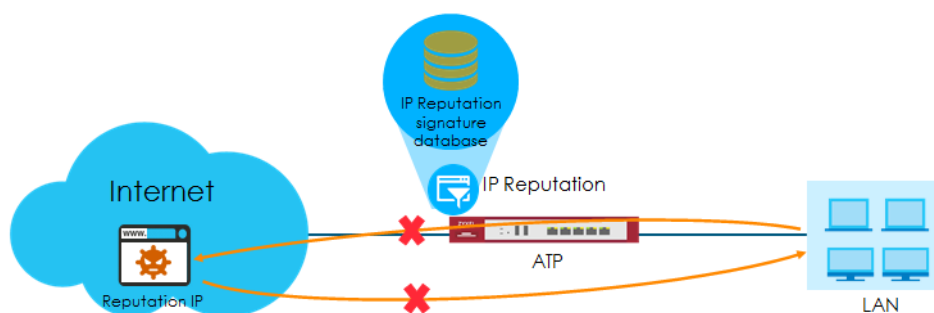
How to Use IP Reputation to Detect Threats

(This feature is only supported on ATP series)


As cyber threats such as scanners, botnets, phishing, etc. grow increasingly, how to identify suspect IP addresses of threats efficiently becomes a crucial task.

With regularly updated IP database, ATP prevents threats by blocking connection to/from known IP addresses based on signature database. It filters source and destination addresses in your network traffic to take the proper risk prevention actions.

This example illustrates how to configure IP Reputation on ATP gateway to detect cyber threats for both incoming and outgoing traffic.



Figure

 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses. This example was tested using the ATP500 (Firmware Version: ZLD 4.35).

Activating Reputation Filter Service

- 1 Register ATP gateway to myZyxel.com.
- 2 Activate Reputation Filter license.

| Service Status | | | | | | |
|----------------|--------------------------|-----------|--------------|-----------------|-------|-----------------------|
| # | Service | Status | Service Type | Expiration Date | Count | Action |
| 1 | Web Security | Activated | Standard | 2020-3-31 | N/A | Renew |
| 2 | Application Security | Activated | Standard | 2020-3-31 | N/A | Renew |
| 3 | Malware Blocker | Activated | Standard | 2020-3-31 | N/A | Renew |
| 4 | Intrusion Prevention | Activated | Standard | 2020-3-31 | N/A | Renew |
| 5 | Geo Enforcer | Activated | Standard | 2020-3-31 | N/A | Renew |
| 6 | Sandboxing | Activated | Standard | 2020-3-31 | N/A | Renew |
| 7 | Reputation Filter | Activated | Standard | 2020-3-31 | N/A | Renew |
| 8 | SecuReporter | Activated | Standard | 2020-3-31 | N/A | Renew |
| 9 | Managed AP Service | Activated | Standard | 2020-3-31 | 34 | Renew |
| 10 | Device HA Pro | Activated | Standard | | N/A | |
| 11 | Firmware Upgrade Service | Activated | | | N/A | |

Page 1 of 1 Show 50 items Displaying 1 - 11 of 11

- 3 On ATP, go to **CONFIGURATION > Licensing > Signature Update**. Click the **Update** icon to check for new signatures.

| Service Status | | | | | | |
|----------------|------------------------|------------------|---------------------------------|---------------------|--------|--|
| Feature | Type | Current Version | Released Date | Last Sync | Action | |
| Anti-Malware | Anti-Malware Signature | 2.0.2.20190601.0 | 2019-06-01 09:35:37 (UTC+08:00) | | | |
| | Cloud Threat Databa... | 1.0.0.20190601.0 | 2019-06-01 02:15:03 (UTC+08:00) | 2019-06-13 23:49:01 | | |
| App-Patrol | App-Patrol | 1.0.0.20190516.0 | 2019-05-16 09:45:23 (UTC+08:00) | 2019-06-02 00:15:01 | | |
| IDP | IDP | 4.0.0.20190524.0 | 2019-05-24 10:10:00 (UTC+08:00) | 2019-06-02 01:53:01 | | |
| Botnet Filter | Botnet Filter | 1.0.0.20190601.0 | 2019-06-01 10:20:50 (UTC+08:00) | 2019-06-14 02:50:01 | | |
| IP Reputation | IP Reputation | 1.0.0.20190601.0 | 2019-06-01 10:30:10 (UTC+08:00) | 2019-06-17 14:56:03 | | |

Enabling IP Blocking on ATP

Go to **CONFIGURATION > Security Service > Reputation Filter > IP Reputation > General**. Click **Enable** to detect reputation IPs. The threat level threshold is measured by the query score of IP signature database.

| General | White List | Black List |
|---|------------|---|
| IP Blocking <input checked="" type="checkbox"/> Enable | | |
| Action: | block | |
| Threat Level Threshold: | high | High Medium and above Low and above |
| Log: | log | |

Selecting specific type of IP addresses to block

In Types of Cyber Threats Coming From The Internet, select the type of threats that are known to pose a security threat for incoming traffic.

In Types of Cyber Threats Coming From The Internet And Local Networks, select the type of threats that are known to pose a security threat for both incoming and outgoing traffic.

| Types of Cyber Threats Coming From The Internet | | |
|--|---|--|
| <input checked="" type="checkbox"/> Anonymous Proxies | <input checked="" type="checkbox"/> Denial of Service | <input checked="" type="checkbox"/> Exploits |
| <input checked="" type="checkbox"/> Negative Reputation | <input checked="" type="checkbox"/> Scanners | <input checked="" type="checkbox"/> Spam Sources |
| <input checked="" type="checkbox"/> TOR Proxies | <input checked="" type="checkbox"/> Web Attacks | |
| Types of Cyber Threats Coming From The Internet And Local Networks | | |
| <input checked="" type="checkbox"/> Botnets | | <input checked="" type="checkbox"/> Phishing |
| Test IP Threat Category | | |
| IP to test: | <input type="text"/> | <input type="button" value="Query"/> |
| Signature Information | | |
| Current Version: | 1.0.0.20190601.0 | |
| Signature Number: | 752104 | |
| Released Date: | 2019-06-01 10:30:10 | |
| Update Signatures | | |

Adding IP addresses to white list and black list

Go to **CONFIGURATION > Security Service > Reputation Filter > IP Reputation > White List** and **Black List** to manually adding IP addresses to the White List and Black List.

IP Blocking

☒ Enable

Action: block

Threat Level Threshold: high

Log: log

Types of Cyber Threats Coming From The Internet

☒ Anonymous Proxies
 ☒ Denial of Service
 ☒ Exploits

☒ Negative Reputation
 ☒ Scanners
 ☒ Spam Sources

☒ TOR Proxies
 ☒ Web Attacks

Types of Cyber Threats Coming From The Internet And Local Networks

☒ Botnets
 ☒ Phishing

- For incoming traffic, set a NAT rule and add a security policy rule for allowing traffic from WAN to LAN.

General Settings

☒ Enable Policy Control

IPv4 Configuration

☐ Allow Asymmetrical Route

+ Add ✎ Edit ✖ Remove 💡 Activate 💡 Inactivate ↔ Move 📄 Clone

| Pri... | St... | Name | From | To | IPv4 Sou... | IPv4 Des... | Service | User | Schedule | Action | Log | Profile |
|--------|-------|--------------|------|------------|-------------|-------------|---------|------|----------|--------|-----|---------|
| 1 | 💡 | test | WAN | LAN | any | any | RDP | any | none | allow | no | |
| 2 | 💡 | LAN_Outgoing | LAN | any (Ex... | any | any | any | any | none | allow | no | |
| 3 | 💡 | DMZ_to_WAN | DMZ | WAN | any | any | any | any | none | allow | no | |

For outgoing traffic, ping an IP address in the threat category "Botnets" from LAN.

- Check statistics for detected IPs.

MONITOR > Security Statistics > Reputation Filter

General Settings

☒ Collect Statistics
 since 2019-06-17 16:16:48 to 2019-06-17 16:23:50

Refresh Flush Data

Summary

IP Scanned: 197

☒ IP Hit Count: 7

URL Scanned: 0

URL Hit Count: 0

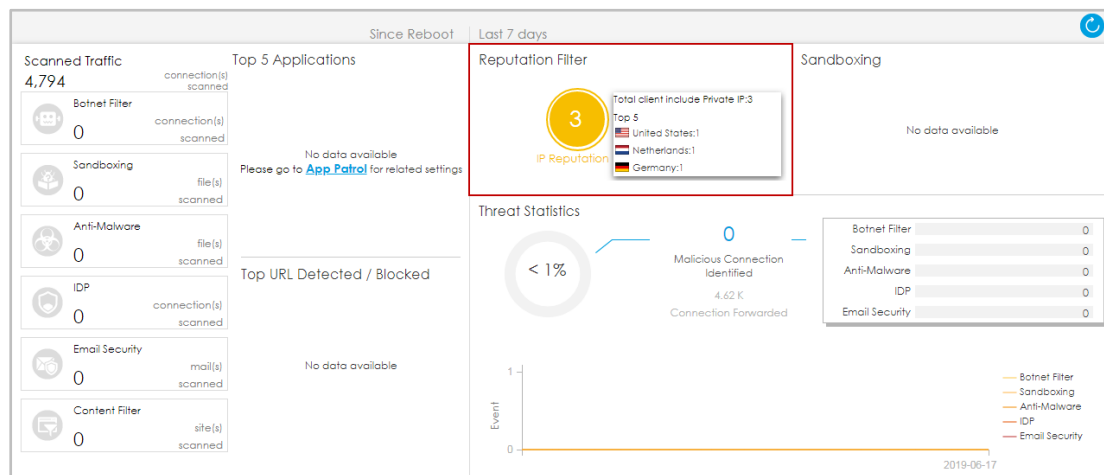
IP Detected

+ Add to white list ✖ Remove from white list

| Time | Malicious IP | Infected/Victim Host | Threat Category | Threat Level |
|---------------------|--|----------------------|-------------------|--------------|
| 2019/06/17 16:23:33 | <input type="checkbox"/> 195.20.42.1 | 192.168.1.33 | BotNets | High |
| 2019/06/17 16:23:32 | <input type="checkbox"/> 195.20.42.1 | 192.168.1.33 | BotNets | High |
| 2019/06/17 16:23:00 | <input type="checkbox"/> 195.20.42.1 | 192.168.1.33 | BotNets | High |
| 2019/06/17 16:22:59 | <input type="checkbox"/> 195.20.42.1 | 192.168.1.33 | BotNets | High |
| 2019/06/17 16:21:45 | <input type="checkbox"/> 148.251.232.132 | 192.168.1.34 | Anonymous Proxies | High |
| 2019/06/17 16:21:45 | <input type="checkbox"/> 148.251.232.132 | 192.168.1.34 | Anonymous Proxies | High |
| 2019/06/17 16:21:44 | <input type="checkbox"/> 148.251.232.132 | 192.168.1.34 | Anonymous Proxies | High |

On dashboard, you can find top 5 countries that are detected the most by IP Reputation.

Dashboard > Advanced Threat Protection



What Can Go Wrong?

1. For device HA or HA Pro, signature synchronization is required.
2. Cloud query is not supported.
3. It doesn't support for IPv6.