



Firmware Release Note

ZyWALL 2 Plus

Release 4.01(XU.0)

Date:
Author:
Project Leader:

October 16, 2006
Keenboy Xu
Lorin Yeh

ZyXEL ZyWALL 2 Plus Standard Version

Release 4.01(XU.0)

Release Note

Date: October 16, 2006

Supported Platforms:

ZyXEL ZyWALL 2 Plus

Versions:

ZyNOS F/W Version: V4.01(XU.0) | 10/16/2006 19:03:59

BootBase: V1.11 | 07/12/2006 14:20:29

Notes:

1. Restore to Factory Defaults Setting Requirement: No
2. The setting of ignore triangle route is on in default ROMFILE. Triangle route network topology has potential security crisis. If you are not clear about it, please refer to Appendix for the triangle route issue.
3. IKE process in phase 2 will check ID information between system and the peer. If you found that the IPSEC connection is failed, please check your settings.
4. Using Web to configure VPN, the phase 1 algorithms have been fixed to DES + MD5. If other algorithms are preferred, please use ADVANCE page to configure them.
5. When firewall turns from "off" to "on", the firewall initialization procedure will disconnect all connections running through the ZyWALL.
6. SUA/NAT address loopback feature was enabled on ZyWALL by default; however, if users do not need it, a C/I command "ip nat loopback off" could turn it off.
7. When UPnP is on, and then reboot the router, Windows XP will not detect UPnP and refresh "My Network Places→Local Network". Plug in network wire again can solve this problem.
8. In bridge mode, If LAN side DHCP clients want to get DHCP address from WAN side DHCP server, you may need to turn on the firewall rule for BOOT_CLIENT service type in WAN→LAN direction.
9. The first entry for static route is reserved for creating WAN default routes and is READ-ONLY.
10. If you want traffic redirect feature to work, you should turn on WAN ping check by "sys rn pingcheck 1".
11. The first entry for static route is reserved for creating WAN default route and is READ-ONLY.
12. If you had activated content filtering service but the registration service state is "Inactive" after upgrading to 4.00, please click "Service License Refresh" in "eWC->REGISTRATION->Registration" or wait until device synchronize with

- the myzyxel.com.
13. Support Vantage CNM -- revision 2.2.00.61.03

Known Issues:

[UPnP]

1. Sometimes on screen the "Local Area Connection" icon for UPnP disappears. The icon shows again when restarting PC.
2. When you use MSN messenger, sometimes you fail to open special applications, such as whiteboard, file transfer and video etc. You have to wait more than 3 minutes and retry these applications.

[Bandwidth Management]

1. Bandwidth management H.323 service does not support Netmeeting H.323 application.
2. Using BWM in PPPoE/PPTP mode, there are two filters for FTP and H323 ALG
 - (1) If we execute FTP first then H323 cannot pass through ZyWALL.
 - (2) If we execute H323 before FTP, all functions work properly.
3. In some cases, BWM (Fairness-Based mode) cannot manage bandwidth accurately. Ex. In WAN interface, there are two subclasses for FTP service, their speed are 100Kbps and 500Kbps, the traffic match the filter which speed is 500Kbps may only use half of it's bandwidth.

[Content Filter]

1. Can't block ActiveX in some case. (Sometime the ActiveX block fails. This is because the ActiveX is cached in C:\WINNT\Downloaded Program Files\ If you want to test the ActiveX block functionality. Please clear the cache in windows.)

[Bridge Mode]

1. When device boots in Bridge Mode, some CI command error messages will be displayed on console. This is because some predefined CI commands in autoexec.net is forbidden to execute in Bridge Mode.
2. Don't use CI command "bridge rstp bridge enable" to enable RSTP, it will change the initial Path Cost value to an incorrect value.

[ALG]

1. Symptom: P2002 can not connect with each other in Peer-to-Peer mode.
Condition:
Topology: P2002--(LAN)ZyWALL_A(WAN, IP=172.21.2.151)--(WAN, IP=172.21.1.134)ZyWALL_B(LAN)--P2002
 - (1) In ZyWALL_A and ZyWALL_B, add a "WAN to LAN" firewall rule to pass traffic with port "5060".
 - (2) In ZyWALL_A and ZyWALL_B, add a port forwarding rule "5060" to P2002.
 - (3) In ZyWALL_A and ZyWALL_B, enable SIP ALG.
 - (4) Setup both P2002 to Peer-to-Peer mode.
 - (5) Making the SIP connection by P2002 will be failed.
 - (6) Turn off firewall in ZyWALL_A and ZyWALL_B, sometimes the connection can be built up if we dial from P2002 which is behind ZyWALL_A.

[MISC]

1. At SMT24.1, the collisions for WAN and LAN port are not really counted.
2. Under PPTP encapsulation mode, we can not access some website like <http://www.kimo.com.tw/>
3. In eWC->Statistics, Tx data for Dial Backup is not correct.

4. Symptom: PC can't ping remote gateway through VPN tunnel under this special topology.

Condition:

PC-----LAN ZyWALL_A WAN-----LAN ZyWALL_B

WAN-----Internet

(192.168.1.33) (192.168.100.33) (192.168.100.1) (172.202.77.145)

(1) VPN configuration in ZyWALL_A:

WAN IP Address=192.168.100.33 , WAN IP Subnet Mask=255.255.255.0 ,

Gateway IP Address=192.168.100.1.

Gateway policy , Name=IKE1 , Remote Gateway Address=192.168.100.1 ,

Pre-Shared Key=12345678.

Network policy for IKE1 , Active=enable , Name=IPSec1 , Local Network/Starting

IP Address=192.168.1.33 , Remote Network/Starting IP Address=0.0.0.0

(2) VPN configuration in ZyWALL_B

WAN IP Address=172.202.77.145 , WAN IP Subnet Mask=255.255.0.0 , Gateway

IP Address=172.202.77.1.

Gateway policy , Name=IKE1 , Remote Gateway Address=192.168.100.33 ,

Pre-Shared Key=12345678.

Network policy for IKE1 , Active=enable , Name=IPSec1 , Local Network/Starting

IP Address=0.0.0.0 , Remote Network/Starting IP Address=192.168.1.33.

(3) When we established the VPN tunnel between ZyWALL_A and ZyWALL_B,

we can access ZyWALL_B (192.168.100.1) with the remote management,

such as Telnet, FTP..., this traffic will go through VPN tunnel. However, we can

not ping ZyWALL_B (192.168.100.1) successfully because this ICMP traffic

did not go through VPN tunnel to ZyWALL_B.

[CNM]

1. DES/3DES encryption key doesn't unique.
2. The 2 check boxes "Log" and "Block" of Matched Web Pages can't be disabled on Content Filter/ Categories page when Schedule to Block has set time interval on Content Filter/General page.
3. Vantage GUI misses to show the NetBIOS port, 445 in Firewall "W2L_Rule_2" default rule.
4. [Symptom] Device will crash, when Vantage set Dial Back Fixed IP in the same subnet with WAN to device.

[Condition]

- (1). Let device register to Vantage.
- (2). Vantage set Dial Backup to enable.
- (3). Vantage set Dial Backup Fixed IP in the same subnet as WAN to device.
- (4). Device will crash after writing above settings.
5. Change NAT mode from "SUA" to "Full Feature", device will create 2 address mapping rules automatically but Vantage Server will not.
6. Vantage and Agent are not consistent at VPN/IPSec/Protocol field. Vantage is a dropdown list with "Any", "ICMP", "TCP", "UDP" selections and Agent is a 0~999 value range.
7. Vantage and Agent are not consistent at Firewall rule's log. Vantage has 4 selections "None", "Match", "Not-Match", "Both". Agent has only a check box.
8. Firewall Default Action can't select "Permit", "Drop" and "Reject" via Vantage.
9. Firewall name can't display on Firewall page on Vantage GUI.

10. Some pre-define custom service can't add to firewall rule when configure from Vantage. For example: AX.25, IPv6, VNC, NTP and so on.
11. The "Mail Sender" field on device/Log settings page hasn't implement on Vantage side.
12. [Symptom] Mbuf double free when add firewall rules by using CI commands.
[Condition]
 - (1). On SMT 24.8, configure firewall rules by using CI commands.
 - (2). Add DMZ to LAN rule and DUT crashed.
 - (3). It couldn't be reproduced.
13. [Symptom] Test Bandwidth Manager a period of time, PPTP will be dropped and reconnected.
[Condition]
PC--- (Lan) DUT (PPTP) ---- PQA lab (192.168.10.X)
 - (1). Set Encapsulation = PPTP.
 - (2). Edit web eWC/Firewall/Rule Summary , Packet Direction=WAN to LAN , edit rule 1 , Selected Service(s) = *H.323 (TCP : 1720)
 - (3). Edit web eWC/NAT/Port Forwarding , WAN Interface=WAN1 , index1/Active=enable , Name=H323 , Incoming Port(s)=1720-1720 , Server IP Address=192.168.1.33
 - (4). Edit web eWC/BW MGMT , WAN1/Active=enable , WAN1/Speed (kbps)=1000 , Scheduler=Fairness-Based
 - (5). Edit web eWC/BW MGMT/Class Setup , Interface=WAN , Add Sub-Class , Class Name=Custom , Bandwidth Budget=200 , Priority=2 , Enable Bandwidth Filter= enable , Service= Custom.
 - (6). Edit web eWC/BW MGMT/Class Setup , Interface=WAN , Add Sub-Class , Class Name=FTP , Bandwidth Budget=200 , Priority=3 , Enable Bandwidth Filter= enable.
 - (7). Edit web eWC/BW MGMT/Class Setup , Interface=WAN , Add Sub-Class , Class Name=H323 , Bandwidth Budget=200 , Priority=5 , Enable Bandwidth Filter=enable , Service=H.323
 - (8). Edit web eWC/BW MGMT/Class Setup , Interface=WAN , Add Sub-Class , Class Name=SIP , Bandwidth Budget=200 , Priority=7 , Enable Bandwidth Filter=enable , Service=SIP
 - (9). Edit web eWC/BW MGMT/Class Setup , Interface=WAN1 , move filter 4 to filter 1.
 - (10). Edit web eWC/BW MGMT/Class Setup , Interface=WAN1 , move filter 4 to filter 2.
 - (11). Edit web eWC/BW MGMT/Class Setup , Interface=WAN1 , move filter 4 to filter 3.
 - (12). FTP upload file from 192.168.1.33 to PQA lab.
 - (13). Use "TfGen" application to send UDP packet/ 500kbps from 192.168.1.33 to PQA Lab.
 - (14). Call Netmeeting (OpenH323) from 192.168.1.34 to 192.168.10.101 and send voice packet.
 - (15). Make a SIP phone call from 192.168.1.33 to 192.168.10.100 and send voice packet.
 - (16).After a period of time, PPTP will be dropped and reconnected.

14. [Symptom] Block ActiveX & Java Applet via IPSec tunnel fails.

[Condition]

HQ and branch office application scenario

PC1-----Branch_1(ZW2+)-----HQ(ZW2+)-----Branch_2(ZW35)----
(192.168.2.0) (192.168.1.0)

-----PC2
(192.168.4.0)

DUT1 (HQ)

- (1). Register CF service; Enable Content Filter and Content Filter for traffic that matches IPSec Policy.
- (2). CF service blocks "ActiveX, Java Applet, Cookies and Web Proxy".
- (3). Edit Denied Access Message & Redirect URL.
- (4). Edit web eWC/VPN , add gateway policy , Name=IKE1 , Remote Gateway Address=0.0.0.0 , Pre-Shared Key=12345678
- (5). Edit web eWC/VPN , add network policy for IKE1 , Active=enable , Name=IPSec1 , Local Address Type=Single , Local Network/Starting IP Address=0.0.0.0 , Remote Address Type=Single , Remote Network/Starting IP Address=0.0.0.0

DUT2 (Branch_1 , LAN=192.168.2.0)

- (1). Edit web eWC/VPN , add gateway policy , Name=IKE1 , Remote Gateway Address=DUT1 WAN IP address , Pre-Shared Key=12345678
- (2). Edit web eWC/VPN , add network policy for IKE1 , Active=enable , Name=IPSec1 , Local Address Type=Subnet , Local Network/Starting IP Address=192.168.2.0 , Local Network/End IP Address=255.255.255.0 , Remote Address Type=Single , Remote Network/Starting IP Address=0.0.0.0

Result:

- (1). PC1 can't http http://dob.tnc.edu.tw/themes/old/showPage.php?s=152&t=5 with Java Applet example and there is blocked log on DUT1. But there is no "Denied Access Message" and can't redirect to configured URL.
- (2). Setup same configuration on Branch_2 (ZW35). PC2 can't http http://dob.tnc.edu.tw/themes/old/showPage.php?s=152&t=5 with Java Applet example and there is blocked log on DUT1. There is "Denied Access Message" and can redirect to configured URL.

Features:

Modifications in V 4.01(XU.0) | 10/16/2006

1. Formal Release.

Modifications in V 4.01(XU.0)b4 | 10/11/2006

1. [BUG FIX]
Symptom: There is not the help page for IPSec_PortForw_Server.html.
Condition:
 - 1) SECURITY>>VPN, add Gateway Policy.
 - 2) Add Network Policy.
 - 3) Active check box "active" of Virtual Address Mapping Rule.

- 4) Select Type of Virtual Address Mapping Rule “Many-to-One”.
- 5) Click button “Port Forwarding Rules”, then click help page.
- 6) There is not the help page.
2. [BUG FIX]
Symptom: Some information on eWc/Home page is different from ZW5 4.01
Condition:
 - 1) There is on MAC address on System Information. They are moved to Interfaces and add DMZ/WLAN/WAN MAC address on eWC/Home.
 - 2) Home/System Information/Firmware Version can’t link to maintenance/F/W Upload Page.
 - 3) Home/Security services/Content Filter Expiration can’t link to Registration/Service page.
 - 4) Home/Up Time clock is not real-time.

Modifications in V 4.01(XU.0)b3 | 09/23/2006

1. [BUG FIX]
Symptom: LAN DHCP pool size is 128
Condition:
LAN DHCP pool size is 128, it should be 32 according to PS.
2. [BUG FIX]
Symptom: Default romfile is incorrect for DMZ and WLAN in BW MGMT>>>Class Setup page.
Condition:
 - 1) Click BW MGMT->Class Setup page.
 - 2) Select DMZ or WLAN interface.
 - 3) It displays the “Root Class: 0 kbps” in the middle of this page, it is incorrect and should be “Root Class: 100000 kbps”.
3. [BUG FIX]
Symptom: There are two error title “ZyWALLZyWALLZyWALLLAN” on help page.
Condition:
 - 1) eWC->NETWORK->LAN->HELP page
 - 2) Help page displays incorrect title “ZyWALLZyWALLZyWALLLAN” instead of “LAN”.
4. [BUG FIX]
Symptom: Default setting is inconsistent with ZW5
Condition:
 - 1) eWC/Firewall/Threshold/TCP Maximum Incomplete.
ZW2+: 10 ZW5: 30
 - 2) eWC/NAT/Max.Concurrent Sessions Per Host:
ZW2+: 2048 ZW5: 3000.
 - 3) ZW5 has not the following items on eWC/WAN/Dial Backup page
Remote IP Subnet Mask
Remote Node IP Address
 - 4) eWC/MAINTENANCE/Time and Date/Time Server Address
ZW2+: a.ntp.alphazed.net ZW5: 0.pool.ntp.org.
 - 5) eWC/Firewall/Default Rule:
Default firewall rule LAN to DMZ should be no log.
Default firewall rule WAN to DMZ should be no log.

5. [ENHANCEMENT]

Symptom: Device can accept the blank password of login user.

Condition:

Device can accept the blank password of login user. For example: eWC/ MAINTENANCE/Password, input Old password and let New password and Retype to Confirm items blank, new password can be applied and it is blank.

Modifications in V 4.01(XU.0)b2 | 09/13/2006

1. [BUG FIX] 060810724

Symptom: Default WLAN firewall rules directions are different from ZW5 V4.01.

Condition:

- 1) ZW5: LAN to WLAN is Permit with no log , but ZW2 Plus is Drop with log.
- 2) ZW5: WAN to WLAN is Drop with log, but ZW2 Plus is Permit with no log.
- 3) ZW5: DMZ to WAN with no log, but ZW2 with log.
- 4) Based on security, please follow ZW5 behavior.

2. [BUG FIX] 060810725

Symptom: NTP server on LAN sometime will fail without logs when WAN is disconnected and click sync fail.

Condition:

- 1) Disconnect WAN interface.
- 2) To Configure a Time Server Address (ex: 192.168.11.4) which is on LAN port (192.168.11.70) and click Synchronize Now. If it fails and there is no failed log on Log page. If it succeed, and there is a log on Log page.
- 3) This is beta user reported issue and we can reproduce it.

3. [BUG FIX] 060810726

Symptom: Default SNMP Configuration can't be applied.

Condition:

- 1) Reset DUT.
- 2) On eWC/ADVANCED/REMOTE MGMT/SNMP, click Apply.
- 3) It failed and Status show "Invalid IP address".
- 4) Trap's Destination can't be configured to 0.0.0.0.

4. [BUG FIX] 060810712

Symptom: "System Resources" picture bar can not appeared on HOME page when using Mozilla Firefox browser.

Condition:

"System Resources" picture bar can not appeared on HOME page when using Mozilla Firefox browser.(my version v1.5.0.6).

5. [BUG FIX] 060810690

Symptom: CF Denied Access Message and Redirect URL have not limit special character, it will cause DUT crash.

Condition:

- 1) eWC CF, Denied Access Message or Redirect URL input %s%s%s and apply, DUT will be crash.
- 2) Attached file is crash dump.
- 3) It is a common bug.
- 4) It has another security issue, if input a script, like as <script>alert ('XSS Vulnerability') </script>, when user browsing internet and CF blocked it. The Denied Access Message will show block message, and then user browser will be

run that script show "XSS Vulnerability" message box. This is like as XSS vulnerability issue.

Note: Step 4 is decided by administrator. Currently it is not controlled.

6. [BUG FIX] 060811833

Symptom: Message to display when a site is blocked failed but there are web sites blocked log on log page.

Condition:

- 1) Register and enable content filter.
- 2) On Message to display when a site is blocked, edit Denied Access Message to kkkkkkkkkk and Redirect URL to tw.yahoo.com.
- 3) On Categories, Select All Categories.
- 4) Open www.gamble.com on PC and the website can't be opened. There is no blocked message appeared and don't redirect website to tw.yahoo.com.
- 5) There is a web site blocked log on log page showed
"www.gameble.com:Gambling 192.168.1.33:4368 198.173.81.173:80 WEB BLOCK"

7. [BUG FIX] 060814876

Symptom: CERTIFICATES log url page can not found.

Condition:

- 1) CERTIFICATES error log like as "2006-08-14 15:59:43 Due to error code(10), cert noRecv:[ID][CER][SIG][NOTFY:INIT_CONT567A6AFE CERT MANAGER", the url at "code(10)".
- 2) Click this url will be redirect to http://DUT IP/h_Certificate_Code.html, but this page can not found.

8. [BUG FIX] 060814878

Symptom: Bridge mode VPN "Adjust TCP Maximum Segment Size" can not work.

Condition:

- 1) DUT1 in bridge mode, create a VPN1 rule.
- 2) VPN Global Setting Adjust TCP Maximum Segment Size=1000.
- 3) DUT2 in router mode, Create a VPN2 rule.
- 4) Ftp from DUT2 PC2 (ftp client) to DUT1 PC1 (ftp server).
- 5) Sniffer package, always show ftp data size is 536 bytes.

9. [BUG FIX] 060815943

Symptom: Bandwidth Management's Number of classes can not add to 10 rules.

Condition:

- 1) Bandwidth Management's Number of classes can not add to 10 rules, it just can add 9 rules.
- 2) And then edit anyone rule click apply, GUI will be show message of "Number of classes reaches the upper bound" and can not save rule.

10. [BUG FIX] 060817043

Symptom: The difference between ZW5/35/70 v4.01 and ZW2 Plus

Condition:

- 1) LAN/DMZ/WAN/Windows Networking(NetBIOS over TCP/IP)
- 2) LAN/DMZ/Static DHCP: MAC format is 00:00:00:00:00:01, ZW5: 000000000001
- 3) Firewall/Service/Custom Service, ZW2 Plus no default settings.
- 4) VPN/Global Setting, VPN rules skip applying to the overlap range of local and remote IP addresses default is disable on ZW5.
- 5) BWM/Edit Class/ Filter Configuration/Custom/Destination Port &Source Port

can set Start port to End port on ZW5.

6) SMT WLAN Zone is different

11. [BUG FIX] 060817054

Symptom: ZW2 Plus V4.01(XU.0)b1 behind the zywall 35 (V4.01) ip alias, VPN tunnel can not work.

Topology:

pc1---(L)zw2-1(W)---(L)zw35(L)---(W)zw2-2(L)---pc2

zw35 lan ip:

ip alias1:10.10.10.1

ip alias2:172.172.172.1

zw2-1 wan ip:10.10.10.200 (bridge mode)

pc1 ip:10.10.10.100

zw2-2 wan ip:172.172.172.200 (route mode)

pc2 ip:192.168.1.33

Condition:

1) Create a VPN rule on zw2-1 and zw2-2.

2) Pc1 ping pc2 and triggered this VPN rule.

3) VPN tunnel will be connected but pc1 ping or ftp to pc2 fail.

12. [ENHANCEMENT]

Add ci command for WAN port Ethernet speed. Steps are the following:

1) ether edit load

2) load <ether no(1:lan).>

3) ether edit load 2

4) ether edit speed (speed <auto|10/half|10/full|100/half|100/full>)

5) ether edit speed auto

6) ether edit save

13. [ENHANCEMENT]

Microsoft cryptographic library supports only odd-sized keys for generating the RSA-modulus.

Let the key number of creator primes be odd-size.

14. [BUG FIX]

Symptom: Import certificate fail.

Condition:

1) Goto eWC>SECURITY>CERTIFICATES>My Certificates page, export the ZyWALL's self-signed auto_generated_self_signed_cert certificate in PKCS#12 format.

2) Import the same certificate file to ZyWALL. The ZyWALL will show the error message "The certificate name cannot be blank".

15. [ENHANCEMENT]

Add PKCS12 for ZyNOS.

16. [ENHANCEMENT]

Add second time schedule setting in content filtering.

17. [BUG FIX]

Symptom: Device crashes because of memory double free in Content Filter.

Condition:

1) Enable Content Filter and Web site customization.

2) After a while, the device will crash sometimes.

18. [ENHANCEMENT]

Enhance the CI command "ip ifconfig".

- 1) Add a new argument "mss" to configure the MSS value.
 - 2) After finishing the configuration, the interface information will be displayed.
- Usage: ip ifconfig [iface] [ipaddr</mask bits>] <broadcast [addr]> <mtu [value]>
<mss [value]> <dynamic> <showoff>

Ex: ip ifconfig enif1 192.168.70.222/24 broadcast 192.168.70.250 mtu 1500 mss 1460.

19. [BUG FIX]

Symptom: The packet will be dropped if the device does not have the ARP entry of the receiver of this packet.

Condition:

- 1) Clear ARP table by "CI>ip arp flush".
- 2) Send a ping to 168.95.1.1, but the PC will not get a response in the first ICMP Echo Request.
- 3) After the first ping, the rest of pings can get responses.

Modifications in V 4.01(XU.0)b1 | 08/08/2006

1. Based on V4.00(XU.2)C0, first release.

Main changes:

- 1) add DMZ/WLAN zone interface
- 2) upgrade concurrent active vpn tunnel number to 5 (originally 2)
- 3) upgrade port forwarding entry number to 20
- 4) add Firewall/BWM/CF/NAT over IPSec
- 5) add 4.01 uniform home page
- 6) add TR069 enhancement

Appendix 1 Remote Management Enhancement (Add SNMP & DNS Control)

New function

- (1) You can change the server port.
- (2) You can set the security IP address for each type of server.
- (3) You can define the rule for server access. (WAN only/LAN only, None, ALL).
- (4) The secure IP and port of the SNMP server is read only
- (5) The port of the SNMP and DNS server is read only.
- (6) The default server access of the SNMP and DNS is ALL.

Modification

- (1) The default value for Server access rule is **ALL**.
- (2) Under the default setting: You can setup the Menu 15 to forwarding the server to LAN IP address. Thus you can configure the router through the WAN and you don't need to modify the server management or filter.

Menu 24.11 - Remote Management Control

| | | |
|----------------|-----------------------------|--------------|
| TELNET Server: | Port = 23 | Access = ALL |
| | Secured Client IP = 0.0.0.0 | |
| FTP Server: | Port = 21 | Access = ALL |
| | Secured Client IP = 0.0.0.0 | |
| Web Server: | Port = 80 | Access = ALL |
| | Secured Client IP = 0.0.0.0 | |
| SNMP server: | Port = 161 | Access = ALL |
| | Secured Client IP = 0.0.0.0 | |
| DNS server: | Port = 53 | Access = ALL |
| | Secured Client IP = 0.0.0.0 | |

Press ENTER to Confirm or ESC to Cancel:

Appendix 2 Trigger Port

Introduction

Some routers try to get around this "one port per customer" limitation by using "triggered" maps. Triggered maps work by having the router watch *outgoing* data for a specific port number and protocol. When the router finds a match, it remembers the IP address of the computer that sent the matching data. When the requested data wants to come back *in* through the firewall, the router uses the port mapping rules that are linked to the trigger, and the IP address of the computer that "pulled" the trigger, to get the data back to the proper computer.

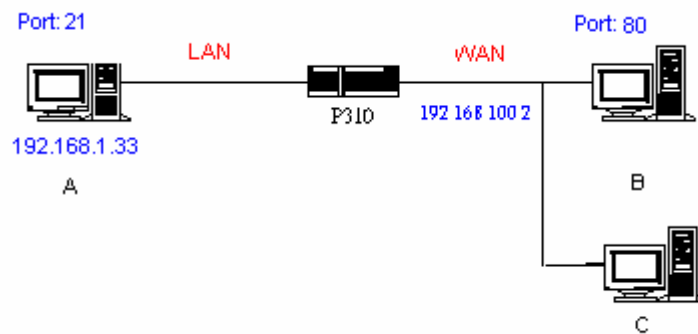
These triggered events can be timed so that they erase the port mapping as soon as they are done with the data transfer, so that the port mapping can be triggered by another Client computer. This gives the *illusion* that multiple computers can use the same port mapping at the same time, but the computers are really just taking turns using the mapping.

How to use it

Following table is a configuration table.

| Name | Incoming | Trigger |
|---------------------------|------------|---------|
| Napster | 6699 | 6699 |
| Quicktime 4 Client | 6970-32000 | 554 |
| Real Audio | 6970-7170 | 7070 |
| User | 1001-1100 | 1-100 |

How it works



For example, you are running a FTP Server on port 21 of machine A. And you may want this server accessible from the Internet without enabling NAT-based firewall. There are one Web Server on port 80 of machine B and another client C on the Internet.

- (1) As Prestige receives a packet from a local client A destined for the outside Internet machine B, it will check the destination port in the TCP/UDP header to see if it matches the setting in "Trigger Port" (80). If it matches, Prestige records the source IP of A (192.168.1.33) in its internal table.
- (2) Now client C (or client B) tries to access the FTP server in machine A. When Prestige to forward any un-requested traffic generated from Internet, it will first check the rules in port forwarding set. When no matches are found, it will then check the "Incoming Port". If it matches, Prestige will forward the packet to the recorded IP address in the internal table for this port. (This behavior is the same as

we did for port forwarding.)

- (3) The recorded IP in the internal table will be cleared if machine A disconnect from the sessions that matches the "Trigger Port".

Notes

- (1) Trigger events can't happen on data coming from *outside* the firewall because the NAT router's sharing function doesn't work in that direction.
- (2) Only one computer can use a port or port range at a time on a given real (ISP assigned) IP address.

Appendix 3 Hard-coded packet filter for "NetBIOS over TCP/IP" (NBT)

The new set C/I commands is under "sys filter netbios" sub-command. Default values of any direction are "Forward", and trigger dial is "Disabled".

There are two CI commands:

(1) "sys filter netbios disp": It will display the current filter mode.

Example output:

```
===== NetBIOS Filter Status =====  
LAN to WAN:          Block  
WAN to LAN:          Forward  
IPSec Packets:       Forward  
Trigger Dial:        Disabled
```

(2) "sys filter netbios config <type> {on|off}": To configure the filter mode for each type.

Current filter types and their description are:

| Type | Description | Default mode |
|------|--------------------|--------------|
| 0 | LAN to WAN | Forward |
| 1 | WAN to LAN | Forward |
| 6 | IPSec pass through | Forward |
| 7 | Trigger dial | Disabled |

Example commands:

sys filter netbios config 0 on => block LAN to WAN NBT packets

sys filter netbios config 1 on => block WAN to LAN NBT packets

sys filter netbios config 6 on => block IPSec NBT packets

sys filter netbios config 7 off => disable trigger dial

Appendix 4 Traffic Redirect/Static Route Application Note

Why traffic redirect/static route be blocked by ZyWALL

ZyWALL is the ideal secure gateway for all data passing between the Internet and the LAN. For some reasons (load balance or backup line), users want traffics be re-routed to another Internet access devices while still be protected by ZyWALL. The network topology is the most important issue. Here is the common example that people misemploy the LAN traffic redirect and static route.

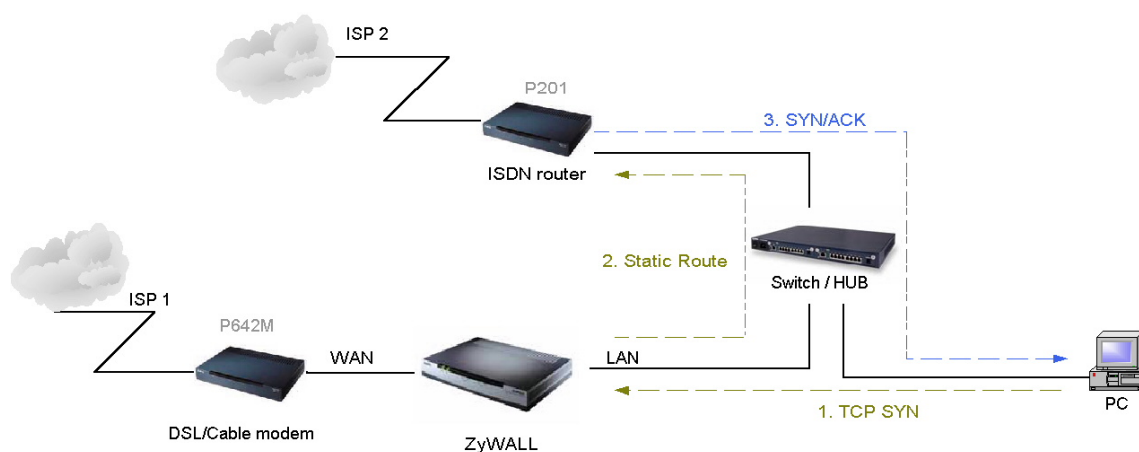


Figure 4-1 Triangle Route

Figure 5-1 indicates the triangle route topology. It works fine with turn off firewall. Let's take a look into the perspective toward this situation.

- Step 1. PC sends outgoing traffics through ZyWALL because default gateway assigned to it.
- Step 2. Then, ZyWALL will redirect the traffics to another gateway (ISDN/Router) as we expect.
- Step 3. But the return traffics do not go through ZyWALL because the gateway (say, P201) and the PC are on the same IP network. **Any traffic will easily inject into the protected network area through the unprotected gateway.**
- Step 4. When firewall turns on, it could be worse. ZyWALL will check the outgoing traffics by ACL and create dynamic sessions to allow legal return traffics. For Anti-DoS reason, ZyWALL will send RST packets to the PC and the peer because it never received TCP SYN/ACK packet.

That causes all of outgoing TCP traffics being reset!

How traffic redirect/static route works under protection - Solutions

(1) Gateway on alias IP network

IP alias allows you to partition a physical network into different logical IP networks over the same Ethernet interface. The ZyWALL supports three logical LAN interfaces via its single physical Ethernet interface with the ZyWALL itself as the gateway for each LAN network. Division of protected LAN and the other gateway into different subnets will trigger the incoming traffic back to ZyWALL and it can work as normal function.

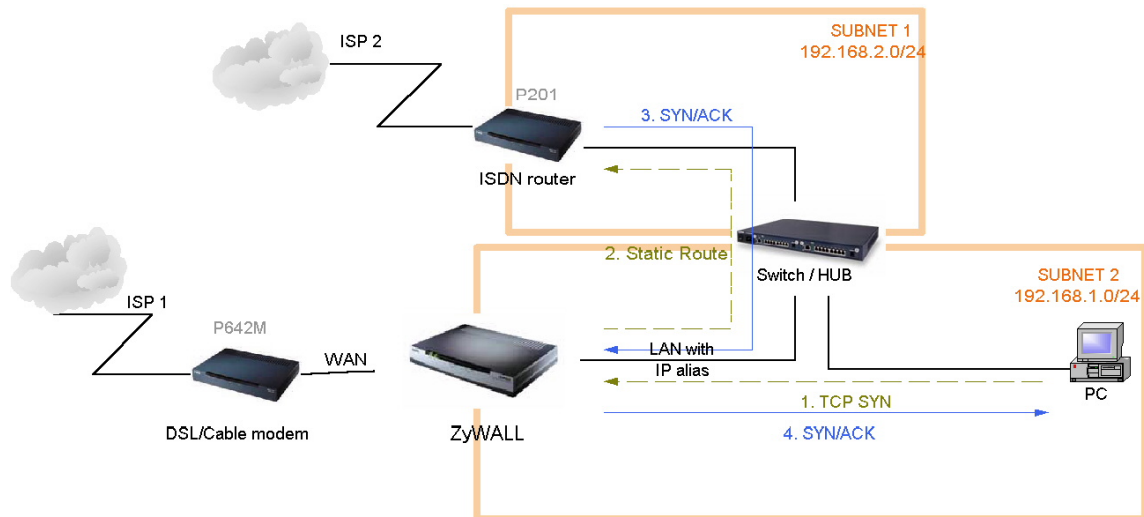


Figure 4-2 Gateway on alias IP network

(2) Gateway on WAN side

A working topology is suggested as below.

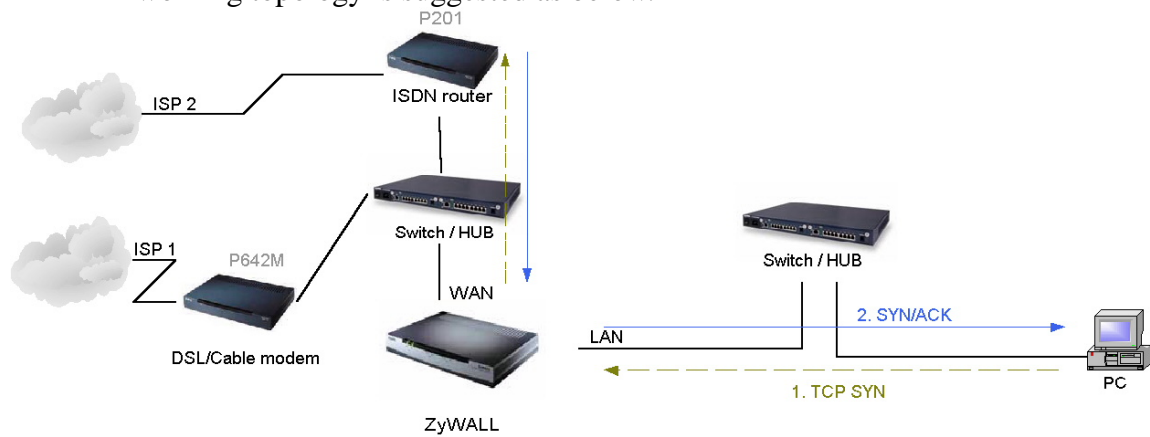


Figure 4-3 Gateway on WAN side

Appendix 5 IPSec FQDN support

ZyWALL A-----Router C (with NAT) -----ZyWALL B
 (WAN) (WAN) (LAN) (WAN)

If ZyWALL A wants to build a VPN tunnel with ZyWALL B by passing through Router C with NAT, A can not see B. It has to secure gateway as C. However, ZyWALL B will send it packet with its own IP and its ID to ZyWALL A. The IP will be NATed by Router C, but the ID will remain as ZyWALL B sent.

In FQDN design, all three types, IP, DNS, E-Mail, can set ID content. For ID type is DNS or E-mail, the behavior is simple. ZyWALL A and ZyWALL B only checks the ID contents are consistent and they can connect.

Basically the story is the same when ID type is IP. If user configures ID content, then ZyWALL will use it as a check. So the ID content also has to match each other. For example, ID type and ID content of incoming packets must match “Peer ID Type” and “Peer ID content”. Or ZyWALL will reject the connection.

However, user can leave “ID content” blank if the ID type is IP. ZyWALL will put proper value in it during IKE negotiation. This appendix describes all combinations and behaviors of ZyWALL.

We can put all combinations in to these two tables:

(Local ID Type is IP):

| Configuration | | **Run-time status | |
|-----------------------|-----------------------|-------------------|------------------|
| My IP Addr | Local ID Content | My IP Addr | Local ID Content |
| 0.0.0.0 | *blank or 0.0.0.0 | My WAN IP | My WAN IP |
| 0.0.0.0 | a.b.c.d (NOT 0.0.0.0) | My WAN IP | a.b.c.d |
| a.b.c.d (not 0.0.0.0) | *blank or 0.0.0.0 | a.b.c.d | a.b.c.d |
| a.b.c.d (not 0.0.0.0) | e.f.g.h (NOT 0.0.0.0) | a.b.c.d | e.f.g.h |

*Blank: User can leave this field as empty, doesn't put anything here.

**Runtime status: During IKE negotiation, ZyWALL will use “My IP Addr” field as source IP of IKE packets, and put “Local ID Content” in the ID payload.

(Peer ID Type is IP):

| Configuration | | *Run-time check |
|---------------------|------------------|--|
| Secure Gateway Addr | Peer ID Content | |
| 0.0.0.0 | Blank or 0.0.0.0 | Just check ID types of incoming packet and machine's peer ID type. If the peer's ID is |

| | | |
|---------|-------------------------------------|---|
| | | IP, then we accept it. |
| 0.0.0.0 | a.b.c.d (NOT 0.0.0.0) | System checks both type and content |
| a.b.c.d | Blank | 1. System will check the ID type and the content. 2. The contents will match only if the ID content of coming packet is a.b.c.d because system will put Secure Gateway Address as Peer ID content. |
| a.b.c.d | e.f.g.h | 1. System will check the ID type and the content. 2. The contents will match only if the ID content of coming packet is e.f.g.h. |

*Runtime Check: During IKE negotiation, we will check ID of incoming packet and see if it matches our setting of “Peer ID Type” and “Peer ID Content”.

Summary:

1. When Local ID Content is blank or 0.0.0.0, during IKE negotiation, my ID content will be “My IP Addr” (if it’s not 0.0.0.0) or local’s WAN IP.
2. When “Peer ID Content” is not blank or 0.0.0.0, ID of incoming packet has to match our setting. Or the connection request will be rejected.
3. When “Secure Gateway IP Addr” is 0.0.0.0 and “Peer ID Content” is blank or 0.0.0.0, system can only check ID type. This is a kind of “dynamic rule” which means it accepts incoming request from any IP, and these requests’ ID type is IP. So if user put such a kind of rule in top of rule list, it may be matched first. To avoid this problem, we will enhance it in the future.

Appendix 6 DNS servers for IPSec VPN Note

DNS Domain Names

DNS (Domain Name System), a system for naming computers and network services that is organized into hierarchy of domain. DNS services provided by the DNS server can resolve the name to other information associated with the name, such as an IP address. The ZyWALL can be configured as a DHCP server. For most cases, your computer connected to the LAN of the ZyWALL can get IP settings (IP address, network mask, gateway address and DNS server address) from the ZyWALL DHCP server automatically.

There are three ways the ZyWALL's DHCP server assigns DNS servers addressed to its DHCP client computers.

- (1) If the administrator has setup DNS servers on the ZyWALL's DHCP setting, the ZyWALL will tell the client those DNS server addresses.
- (2) If the DNS server has not been setup on the ZyWALL DHCP server, but the ZyWALL has gotten the public DNS servers from the ISP; the ZyWALL will assign those public DNS servers address.
- (3) The ZyWALL gives its own LAN IP address and acts as a DNS server proxy.

But the above are not enough for IPSec VPN applications.

How to access the private network by using domain names

On the IPSec VPN application, the user on the LAN of the ZyWALL, wants to access remote private networks. He must use the IP address to identify the remote site he wants to access. But at the modern intranet applications, we still want to have the DNS service for private network access. For example, there is a private Web server installed at the headquarters of your company. You can access this Web server inside your company, or from your home by way of the ZyWALL's IPSec tunnel. The IP address of the private Web server is also private. You can't use the Internet public DNS servers to resolve those domain names that belong to your company's private network. You must setup those private DNS servers on your computer manually if you want to access the private network by using domain names.

ZyWALL DNS Servers for IPSec VPN

The ZyWALL has added DNS Server on each IPSec policy setup. When you setup the IPSec rule, you can give the DNS server if there exists a DNS Server that provides DNS service for this private network. The DHCP client (on ZyWALL's LAN) requests the IP information from your ZyWALL, the ZyWALL assigns additional DNS servers for IPSec VPN to the client, if the assigned IP address belongs to the range of local addresses of the IPSec rule.

Annex A CI Command List

Last Updated: 2006/03/02

| Command Class List Table | | |
|--|--|--|
| System Related Command | Exit Command | Device Related Command |
| Ethernet Related Command | POE Related Command | PPTP Related Command |
| AUX Related Command | Configuration Related Command | IP Related Command |
| IPSec Related Command | Bridge Related Command | Bandwidth Management |
| Firewall Related Command | Certificate Management (PKI) Command | myZyXEL.com Command |
| Vantage Related Command | | |

Flag :

R: This command can be used in Router Mode

B: This command can be used in Bridge Mode

System Related Command

| Command | | | | Flag | Description |
|---------|-------------|----------|---|-------|--|
| sys | | | | | |
| | adjtime | | | R + B | retrieve date and time from Internet |
| | cbuf | | | | |
| | | cnt | | | cbuf static |
| | | | display | R + B | display cbuf static |
| | callhist | | | | |
| | | display | | R | display call history |
| | | remove | <index> | R | remove entry from call history |
| | countrycode | | [countrycode] | R + B | set country code |
| | date | | [year month date] | R + B | set/display date |
| | debug | | | R + B | |
| | | romfile | | R + B | |
| | | | cert [0:reserve/1:erase] | R + B | erase all the certificates |
| | | | display | R + B | display romfile debug settings |
| | | | isp [0:reserve/1:erase] | R | erase the account and password of ISP |
| | | | prekey [0:reserve/1:reset] | R | reset the system IPSec pre-shared key |
| | | | profile [0:reserve/1:erase] | R + B | erase the accounts and passwords of 802.1X and XAUTH |
| | | | pwd [0:reserve/1:reset] | R + B | reset system password |
| | | | radius | R + B | erase Authentication and Accounting keys |
| | | | update [0:reserve/1:erase] | R + B | update romfile depend on current configuration |
| | | | wep [0:reserve/1:erase] | R + B | erase all WEP encryption keys |
| | domainname | | | R + B | display domain name |
| | edit | | <filename> | R + B | edit a text file |
| | extraphnum | | | R | maintain extra phone numbers for outcalls |
| | | add | <set 1-3> <1st phone num> [2nd phone num] | R | add extra phone numbers |
| | | display | | R | display extra phone numbers |
| | | node | <num> | R | set all extend phone number to remote node <num> |
| | | remove | <set 1-3> | R | remove extra phone numbers |
| | | reset | | R | reset flag and mask |
| | feature | | | R + B | display feature bit |
| | hostname | | [hostname] | R + B | display system hostname |
| | logs | | | R + B | |
| | | category | | R + B | |
| | | | access [0:none/1:log/2:alert/3:both] | R + B | record the access control logs |

| | | | | | |
|--|--|-------------|--|-------|---|
| | | | attack [0:none/1:log/2:alert/3:both] | R + B | record and alert the firewall attack logs |
| | | | display | R + B | display the category setting |
| | | | error [0:none/1:log/2:alert/3:both] | R + B | record and alert the system error logs |
| | | | ipsec [0:none/1:log/2:alert/3:both] | R | record the access control logs |
| | | | ike [0:none/1:log/2:alert/3:both] | R | record the access control logs |
| | | | javablocked [0:none/1:log] | R + B | record the java etc. blocked logs |
| | | | mten [0:none/1:log] | R + B | record the system maintenance logs |
| | | | packetfilter [0:none/1:log] | R + B | record the packet filter logs |
| | | | pki [0:none/1:log/2:alert/3:both] | R | record the pki logs |
| | | | tcpreset [0:none/1:log] | R + B | record the tcp reset logs |
| | | | upnp [0:none/1:log] | R | record upnp logs |
| | | | urlblocked [0:none/1:log/2:alert/3:both] | R + B | record and alert the web blocked logs |
| | | | urlforward [0:none/1:log] | R + B | record web forward logs |
| | | clear | | R + B | clear log |
| | | display | [access attack error ipsec ike javab locked mten packetfilter pki tcpre set urlblocked urlforward] | R + B | display all logs or specify category logs |
| | | errlog | | R + B | |
| | | clear | | R + B | display log error |
| | | disp | | R + B | clear log error |
| | | online | | R + B | turn on/off error log online display |
| | | load | | R + B | load the log setting buffer |
| | | mail | | R + B | |
| | | | alertAddr [mail address] | R + B | send alerts to this mail address |
| | | | display | R + B | display mail setting |
| | | | logAddr [mail address] | R + B | send logs to this mail address |
| | | | schedule display | R + B | display mail schedule |
| | | | schedule hour [0-23] | R + B | hour time to send the logs |
| | | | schedule minute [0-59] | R + B | minute time to send the logs |
| | | | schedule policy [0:full/1:hourly/2:daily/3:weekly/ 4:none] | R + B | mail schedule policy |
| | | | schedule week [0:sun/1:mon/2:tue/3:wed/4:thu/5 :fri/6:sat] | R + B | weekly time to send the logs |
| | | | server [domainName/IP] | R + B | mail server to send the logs |
| | | | subject [mail subject] | R + B | mail subject |
| | | save | | R + B | save the log setting buffer |
| | | syslog | | R + B | |
| | | | active [0:no/1:yes] | R + B | active to enable unix syslog |
| | | | display | R + B | display syslog setting |
| | | | facility [Local ID(1-7)] | R + B | log the messages to different files |
| | | | server [domainName/IP] | R + B | syslog server to send the logs |
| | | updateSvrIP | <minute> | R + B | If there is one parameter <minute>, it will change the dns timer task timeout value. Otherwise, do dns resolve to find email log server and syslog server IP. |
| | | consolidate | | R + B | |
| | | | switch <0:on 1:off> | R + B | active to enable log consolidation |
| | | | period | R + B | consolidation period (seconds) |
| | | | msglist | R + B | display the consolidated messages |
| | | switch | | | |
| | | | bmlog <0:no 1:yes> | R + B | active to enable broadcast/multicast log |
| | | | display | R + B | display switch setting |
| | | | trilog <0:no 1:yes> | R + B | active to enable triangle route log |

| | | | | | |
|--|-----------|--------------------|-------------------------------|-------|---|
| | mbuf | | | R + B | |
| | | link | link | R + B | list system mbuf link |
| | | pool | <id> [type][num] | R + B | list system mbuf pool |
| | | status | | R + B | display system mbuf status |
| | | disp | <address>[1 0] | R + B | display mbuf status |
| | | cnt | | R + B | |
| | | | disp | R + B | display system mbuf count |
| | | | clear | R + B | clear system mbuf count |
| | | debug | [on off] | R + B | |
| | mode | <router/bridge> | | R + B | switch router and bridge mode |
| | pwderrtm | | [minute] | R + B | Set or display the password error blocking timeout value. |
| | rn | | | R | |
| | | load | <entry no.> | R | load remote node information |
| | | disp | <entry no.>(0:working buffer) | R | display remote node information |
| | | nat | <none sua full_feature> | R | config remote node nat |
| | | nailup | <no yes> | R | config remote node nailup |
| | | mtu | <value> | R | set remote node mtu |
| | | save | [entry no.] | R | save remote node information |
| | | pingcheck | [on off] | U + R | enable/disable WAN pingcheck |
| | smt | | | R + B | not support in this product |
| | stdio | | [second] | R + B | change terminal timeout value |
| | time | | [hour [min [sec]]] | R + B | display/set system time |
| | tos | | | R + B | |
| | | display | | R + B | display all runtime TOS |
| | | listPerHost | | R + B | display all host session count |
| | | debug | [on off] | R + B | turn on or off TOS debug message |
| | | sessPerHost | <number> | R + B | configure session per host value |
| | | timeout | | R + B | |
| | | | display | R + B | display all TOS timeout information |
| | | | icmp <idle timeout> | R + B | set idle timeout value |
| | | | igmp <idle timeout> | R + B | set idle timeout value |
| | | | tcpsyn <idle timeout> | R + B | set idle timeout value |
| | | | tcp <idle timeout> | R + B | set idle timeout value |
| | | | tcpfin <idle timeout> | R + B | set idle timeout value |
| | | | udp <idle timeout> | R + B | set idle timeout value |
| | | | gre <idle timeout> | R + B | set idle timeout value |
| | | | esp <idle timeout> | R + B | set idle timeout value |
| | | | ah <idle timeout> | R + B | set idle timeout value |
| | | | other <idle timeout> | R + B | set idle timeout value |
| | | tempTOSDisplay | | R + B | display temporal TOS records. |
| | | tempTOSTimeout | [timeout value] | R + B | set/display temporal timeout value |
| | trcdisp | parse, brief, disp | | R + B | monitor packets |
| | trclog | | | R + B | |
| | trcpacket | | | R + B | |
| | syslog | | | R + B | |
| | | server | [destIP] | R + B | set syslog server IP address |
| | | facility | <FacilityNo> | R + B | set syslog facility |
| | | type | [type] | R + B | set/display syslog type flag |
| | | mode | [on off] | R + B | set syslog mode |
| | version | | | R + B | display RAS code and driver version |
| | view | | <filename> | R + B | view a text file |
| | wdog | | | R + B | |
| | | switch | [on off] | R + B | set on/off wdog |
| | | cnt | [value] | R + B | display watchdog counts value: 0-34463 |

| | | | | | |
|--|------------|-------------|--|-------|--|
| | romreset | | | R + B | restore default romfile |
| | server | | | | |
| | | access | <telnet ftp web icmp snmp dns> <value> | R + B | set server access type |
| | | load | | R + B | load server information |
| | | disp | | R + B | display server information |
| | | port | <telnet ftp web snmp> <port> | R + B | set server port |
| | | save | | R + B | save server information |
| | | secureip | <telnet ftp web icmp snmp dns> <ip> | R + B | set server secure ip addr |
| | | certificate | <https ssh> [certificate name] | R + B | set server certificate |
| | | auth_client | <https> [on off] | R + B | specifies whether the server authenticates the client |
| | fwnotify | | | R + B | |
| | | load | | R + B | load fwnotify entry from spt |
| | | save | | R + B | save fwnotify entry to spt |
| | | url | <url> | R + B | set fwnotify url |
| | | days | <days> | R + B | set fwnotify days |
| | | active | <flag> | R + B | turn on/off fwnotify flag |
| | | disp | | R + B | display firmware notify information |
| | | check | | R + B | check firmware notify event |
| | | debug | <flag> | R + B | turn on/off firmware notify debug flag |
| | cmgr | | | R + B | |
| | | trace | | R + B | |
| | | | disp <ch-name> | R + B | show the connection trace of this channel |
| | | | clear <ch-name> | R + B | clear the connection trace of this channel |
| | | cnt | <ch-name> | R + B | show channel connection related counter |
| | socket | | | R + B | display system socket information |
| | filter | | | R + B | |
| | | netbios | | R + B | |
| | | | disp | R + B | display netbios filter status |
| | | | config <0:Between LAN and WAN, 1: Between LAN and DMZ, 2: Between WAN and DMZ, 3:IPSec passthrough, 4:Trigger Dial> <on off> | R + B | config netbios filter |
| | roadrunner | | | R | |
| | | debug | <level> | R | enable/disable roadrunner service 0: disable <default> 1: enable |
| | | display | <iface name> | R | display roadrunner information iface-name: enif0, wanif0 |
| | | restart | <iface name> | R | restart roadrunner |
| | ddns | | | R + B | |
| | | debug | <level> | R + B | enable/disable ddns service |
| | | display | <iface name> | R + B | display ddns information |
| | | restart | <iface name> | R + B | restart ddns |
| | | logout | <iface name> | R + B | logout ddns |
| | cpu | | | R + B | |
| | | display | | R + B | display CPU utilization |
| | upnp | | | R | |
| | | active | [0:no/1:yes] | R | Activate or deactivate the saved upnp settings |
| | | config | [0:deny/1:permit] | R | Allow users to make configuration changes. through UPnP |
| | | display | | R | display upnp information |
| | | firewall | [0:deny/1:pass] | R | Allow UPnP to pass through Firewall. |
| | | load | | R | save upnp information |

| | | | | | |
|--|--|---------|--------------|---|--|
| | | reserve | [0:no/1:yes] | R | Reserve UPnP NAT rules in flash after system bootup. |
| | | save | | R | save upnp information |

Exit Command

[Home](#)

| Command | | | | Flag | Description |
|---------|--|--|--|-------|---------------|
| exit | | | | R + B | exit smt menu |

Device Related Command

[Home](#)

| Command | | | | Description | |
|---------|---------|------|----------------|-------------|---------------------|
| dev | | | | | |
| | channel | | | | |
| | | drop | <channel_name> | R + B | drop channel |
| | dial | | <node#> | R + B | dial to remote node |

Ethernet Related Command

[Home](#)

| Command | | | | Flag | Description |
|---------|-------------|--------|---------------------|-------|--|
| ether | | | | R + B | |
| | config | | | R + B | display LAN configuration information |
| | driver | | | R + B | |
| | | cnt | | R + B | |
| | | | disp <name> | R + B | display ether driver counters |
| | | ioctl | <ch_name> | R + B | Useless in this stage. |
| | | status | <ch_name> | R + B | see LAN status |
| | version | | | R + B | see ethernet device type |
| | pkttest | | | | |
| | | disp | | | |
| | | | packet <level> | R + B | set ether test packet display level |
| | | | event <ch> [on/off] | R + B | turn on/off ether test event display |
| | | sap | [ch_name] | R + B | send sap packet |
| | | arp | <ch_name> <ip-addr> | R + B | send arp packet to ip-addr |
| | debug | | | | |
| | | disp | <ch_name> | R + B | display ethernet debug infomation |
| | | level | <ch_name> <level> | R + B | set the ethernet debug level level 0: disable debug log level 1:enable debug log (default) |
| | edit | | | R + B | |
| | | load | <ether no.> | R + B | load ether data from spt |
| | | mtu | <value> | R + B | set ether data mtu |
| | | speed | <speed> | R + B | set ether data speed |
| | | save | | R + B | save ether data to spt |
| | dynamicPort | | | | |
| | | dump | | U+R+B | display the relation between physical port and channel. |
| | | set | <port> <type> | U+R+B | set physical port belongs to which channel. |
| | | spt | | U+R+B | display channel setting stored in SPT. |

POE Related Command (All commands can only be used in Router Mode)

[Home](#)

| Command | | | | Description | |
|---------|--------|--|-----------|-------------|--------------------|
| poe | | | | | |
| | status | | [ch_name] | | see poe status |
| | dial | | <node> | | dial a remote node |
| | drop | | <node> | | drop a pppoe call |

| | | | | |
|--|-------|--------|------------|--|
| | ether | | [rfc 3com] | set /display pppoe ether type |
| | proxy | disp | | Display PPPoE proxy client session table |
| | | active | [on off] | Turn on / off PPPoE proxy function |
| | | debug | [on off] | Turn on / off PPPoE proxy debug function |
| | | time | <interval> | Set the time out interval, it's a count. Actual time is count * 5 seconds. |
| | | init | | Initialize PPPoE proxy client session table |
| | | flush | | Clear PPPoE proxy client session table |

PPTP Related Command (All commands can only be used in Router Mode)

[Home](#)

| Command | | | | Description |
|---------|--------|--|-------------|---------------------------------|
| pptp | | | | |
| | dial | | <rn-name> | dial a remote node |
| | drop | | <rn-name> | drop a remote node call |
| | tunnel | | <tunnel id> | display pptp tunnel information |

AUX Related Command (All commands can only be used in Router Mode)

[Home](#)

| Command | | | | Description |
|---------|----------|-------|---------------|---------------------------------------|
| aux | | | | |
| | atring | | <device name> | Command the AT command to the device. |
| | cnt | | | |
| | | disp | <device name> | display aux counter information |
| | | clear | <device name> | clear aux counter information |
| | drop | | <device name> | disconnect |
| | init | | <device name> | initialize aux channel |
| | mstatus | | <device name> | display modem last call status |
| | mtype | | <device name> | display modem type |
| | netstat | | <device name> | prints upper layer packet information |
| | rate | | <device name> | show tx rx rate |
| | redirect | | <device name> | invalid |
| | signal | | <device name> | show aux signal |

Configuration Related Command

(All commands can be used in both Router Mode and Bridge Mode)

[Home](#)

| Command | | | | | Description |
|---------|----------------------------|--|--|--|---|
| config | | | | | The parameters of config are listed below. |
| edit | firewall | active <yes no> | | | Activate or deactivate the saved firewall settings |
| | custom-service <entry#> | name <string> | | | Configure selected custom-service with name = <string> |
| | | ip-protocol < icmp tcp udp tcp/udp user-defined > | | | Configure IP Protocol Type for selected custom-service |
| | | port-range <start port> <end port> | | | When ip-protocol = "tcp udp tcp/udp ". configure port range for custom-service entry #. For single port configuration, start port equals to end port. |
| | | user-defined-ip <1~65535> | | | When ip-protocol = "user-defined". Configure user defined IP protocol. |
| | | icmp-type <0~255> | | | When ip-protocol = "icmp", configure ICMP type. |

| | | | | | |
|----------|------------------------------------|----------------------|--|--|---|
| | | icmp-code <0~255> | | | When ip-protocol = "icmp", configure ICMP code. This field is optional for ICMP. |
| retrieve | firewall | | | | Retrieve current saved firewall settings |
| save | firewall | | | | Save the current firewall settings |
| | custom-s ervice <entry#> | | | | Save the custom service entry specified by <entry#> |
| | all | | | | Save all working SPT buffer into flash. |
| display | firewall | | | | Displays all the firewall settings |
| | | set <set#> | | | Display current entries of a set configuration; including timeout values, name, default-permit, and number of rules in the set. |
| | | set <set#> | rule <rule#> | | Display current entries of a rule in a set. |
| | | attack | | | Display all the attack alert settings in PNC |
| | | e-mail | | | Display all the e-mail settings in PNC |
| | | ? | | | Display all the available sub commands |
| | custom-s ervice | | | | Display all configured custom services. |
| | custom-s ervice <entry #> | | | | Display custom service <entry #> |
| edit | firewall | e-mail | mail-server <mail server IP> | | Edit the mail server IP to send the alert |
| | | | return-addr <e-mail address> | | Edit the mail address for returning an email alert |
| | | | e-mail-to <e-mail address> | | Edit the mail address to send the alert |
| | | | policy <full hourly daily weekly> | | Edit email schedule when log is full or per hour, day, week. |
| | | | day <sunday monday tuesday wednesday thursday friday saturday> | | Edit the day to send the log when the email policy is set to Weekly |
| | | | hour <0~23> | | Edit the hour to send the log when the email policy is set to daily or weekly |
| | | | minute <0~59> | | Edit the minute to send to log when the email policy is set to daily or weekly |
| | | | Subject <mail subject> | | Edit the email subject |
| | | attack | send-alert <yes no> | | Activate or deactivate the firewall DoS attacks notification emails |
| | | | block <yes no> | | Yes: Block the traffic when exceeds the tcp-max-incomplete threshold |
| | | | | | No: Delete the oldest half-open session when exceeds the tcp-max-incomplete threshold |
| | | | block-minut e <0~255> | | Only valid when sets 'Block' to yes. The unit is minute |
| | | | minute-high <0~255> | | The threshold to start to delete the old half-opened sessions to minute-low |
| | | | minute-low | | The threshold to stop deleting the old half-opened |

| | | | | | |
|--|--|------------|-----------------------------------|---|--|
| | | | <0~255> | | session |
| | | | max-incomplete-high <0~255> | | The threshold to start to delete the old half-opened sessions to max-incomplete-low |
| | | | max-incomplete-low <0~255> | | The threshold to stop deleting the half-opened session |
| | | | tcp-max-incomplete <0~255> | | The threshold to start executing the block field |
| | | set <set#> | name <desired name> | | Edit the name for a set |
| | | | default-permit <forward block> | | Edit whether a packet is dropped or allowed when it does not match the default set |
| | | | icmp-timeout <seconds> | | Edit the timeout for an idle ICMP session before it is terminated |
| | | | udp-idle-timeout <seconds> | | Edit the timeout for an idle UDP session before it is terminated |
| | | | connection-timeout <seconds> | | Edit the wait time for the SYN TCP sessions before it is terminated |
| | | | fin-wait-timeout <seconds> | | Edit the wait time for FIN in concluding a TCP session before it is terminated |
| | | | tcp-idle-timeout <seconds> | | Edit the timeout for an idle TCP session before it is terminated |
| | | | pnc <yes no> | | PNC is allowed when 'yes' is set even there is a rule to block PNC |
| | | | log <yes no> | | Switch on/off sending the log for matching the default permit |
| | | | logone <yes no> | | Switch on/off for one packet that create just one log message. |
| | | | rule <rule#> | action <permit drop reject> | Edit whether a packet is permitted, dropped or rejected when it matches this rule |
| | | | | name <string> | Edit/Update rule name with <string> |
| | | | | active <yes no> | Edit whether a rule is enabled or not |
| | | | | protocol <0~255> | Edit the protocol number for a rule. 1=ICMP, 6=TCP, 17=UDP... |
| | | | | log <none match not-match both> | Sending a log for a rule when the packet none matches not match both the rule |
| | | | | | |
| | | | | alert <yes no> | Activate or deactivate the notification when a DoS attack occurs or there is a violation of any alert settings. In case of such instances, the function will send an email to the SMTP destination address and log an alert. |
| | | | | srcaddr-single <ip address> | Select and edit a source address of a packet which complies to this rule |
| | | | | srcaddr-subnet <ip address> <subnet mask> | Select and edit a source address and subnet mask if a packet which complies to this rule. |
| | | | | srcaddr-range <start ip address> <end ip address> | Select and edit a source address range of a packet which complies to this rule. |

| | | | | | |
|--------|----------|------------|--------------|--|---|
| | | | | destaddr-single <ip address> | Select and edit a destination address of a packet which complies to this rule |
| | | | | destaddr-subnet <ip address> <subnet mask> | Select and edit a destination address and subnet mask if a packet which complies to this rule. |
| | | | | destaddr-range <start ip address> <end ip address> | Select and edit a destination address range of a packet which complies to this rule. |
| | | | | tcp destport-single <port#> | Select and edit the destination port of a packet which comply to this rule. For non-consecutive port numbers, the user may repeat this command line to enter the multiple port numbers. |
| | | | | tcp destport-range <start port#> <end port#> | Select and edit a destination port range of a packet which comply to this rule. |
| | | | | udp destport-single <port#> | Select and edit the destination port of a packet which comply to this rule. For non-consecutive port numbers, users may repeat this command line to enter the multiple port numbers. |
| | | | | udp destport-range <start port#> <end port#> | Select and edit a destination port range of a packet which comply to this rule. |
| | | | | desport-custom <desired custom port name> | Type in the desired custom port name |
| | | | | custom-ip <desired custom service name> | Type in the desired User Defined IP Protocol custom service. |
| | | | | custom-icmp <desired custom service name> | Type in the desired ICMP custom service |
| delete | firewall | e-mail | | | Remove all email alert settings |
| | | attack | | | Reset all alert settings to defaults |
| | | set <set#> | | | Remove a specified set from the firewall configuration |
| | | set <set#> | rule <rule#> | | Remove a specified rule in a set from the firewall configuration |
| insert | firewall | e-mail | | | Insert email alert settings |
| | | attack | | | Insert attack alert settings |
| | | set <set#> | | | Insert a specified rule set to the firewall configuration |
| | | set <set#> | rule <rule#> | | Insert a specified rule in a set to the firewall configuration |
| cli | | | | | Display the choices of command list. |

IP Related Command

[Home](#)

| Command | | | | FLag | Description |
|---------|----------|-----------|---|------|--------------------------------|
| ip | | | | | |
| | address | | [addr] | | display host ip address |
| | alias | | <iface> | R | alias iface |
| | aliasdis | | <0 1> | R | disable alias |
| | alg | | | | |
| | | disp | | | Show ALG enable disable status |
| | | enable | <ALG_FTP ALG_H323 ALG_SIP> | | Enable ALG command |
| | | disable | <ALG_FTP ALG_H323 ALG_SIP> | | Disable ALG command |
| | | sitimeout | <timeout in second> or 0 for no timeout | | Configure SIP timeout command |
| | arp | | | | |
| | | status | <iface> | | display ip arp status |
| | dhcp | | <iface> | R | |

| | | | | | |
|--|----------|--------------|---|-------|--|
| | | client | | R | |
| | | | release | R | release DHCP client IP |
| | | | renew | R | renew DHCP client IP |
| | | | release <entry num> | R | release specific entry of the dhcp server pool |
| | | status | [option] | R | show dhcp status |
| | dns | | | R | |
| | | query | | R | |
| | | | address <ipaddr> [timeout] | R | resolve ip-addr to name |
| | | | Debug <num> | R | enable dns debug value |
| | | | Name <hostname> [timeout] | R | resolve name to multiple IP addresses |
| | | | Status | R | display dns query status |
| | | | Table | R | display dns query table |
| | | server | <primary> [secondary] [third] | R | set dns server |
| | | stats | | R | |
| | | | Clear | R | clear dns statistics |
| | | | Disp | R | display dns statistics |
| | | table | | R | display dns table |
| | | default | <ip> | R | Set default DNS server |
| | | system | | | |
| | | | display | | display dns system information |
| | | | edita <record idx> <name> <0:FQDN 1:wildcard> <0:from ISP group 1:user defined> <isp group idx ip address> | | edit dns A record |
| | | | editns <record idx> <*<domain name> <0:from ISP 1:user defined(public) 2: user defined(private)> <isp group idx dns server ip> | | edit dns NS record |
| | | | inserta <before record idx -1:new> <name> <0:FQDN 1:wildcard> <0:from ISP group 1:user defined> <isp group idx ip address> | | insert dns A record |
| | | | insertns <before record idx -1:new> <*<domain name> <0:from ISP 1:user defined(public) 2: user defined(private)> <isp group idx dns server ip> | | insert dns NS record |
| | | | movea <record idx> <record idx> | | move dns A record |
| | | | movens <record idx> <record idx> | | move dns NS record |
| | | | dela <record idx> | | delete DNS A record |
| | | | delns <record idx> | | delete DNS NS record |
| | | system cache | | | |
| | | | disp <0:none 1:name 2:type 3:IP 4:refCnt 5:tlt> [0:increase 1:decrease] | | display DNS cache table |
| | | | flush | | flush DNS cache |
| | | | negaperiod <second(60 ~ 3600)> | | set negative cache period |
| | | | negative <0: disable 1: enable> | | enable/disable dns negative cache |
| | | | positive <0: disable 1: enable> | | enable/disable dns positive cache |
| | | | tlt <second(60 ~ 3600)> | | set positive cache maximum tlt |
| | Httpd | | | R + B | |
| | | debug | [on off] | R + B | set http debug flag |
| | icmp | | | | |
| | | status | | R + B | display icmp statistic counter |
| | | discovery | <iface> [on off] | R + B | set icmp router discovery flag |
| | ifconfig | | [iface] [ipaddr] [broadcast <addr> mtu <value> dynamic] | R + B | configure network interface |

| | | | | | |
|--|------------|-----------|---|-------|--|
| | ping | | <hostid> | R + B | ping remote host |
| | route | | | R | |
| | | status | [if] | R | display routing table |
| | | add | <dest_addr default>[/<bits>] <gateway> [<metric>] | R | add route |
| | | addiface | <dest_addr default>[/<bits>] <gateway> [<metric>] | R | add an entry to the routing table to iface |
| | | drop | <host addr> [/<bits>] | R | drop a route |
| | status | | | R + B | display ip statistic counters |
| | stroute | | | R | |
| | | display | [rule # buf] | R | display rule index or detail message in rule. |
| | | load | <rule #> | R | load static route rule in buffer |
| | | save | | R | save rule from buffer to spt. |
| | | config | | R | |
| | | | name <site name> | R | set name for static route. |
| | | | destination <dest addr>[/<bits>] <gateway> [<metric>] | R | set static route destination address and gateway. |
| | | | mask <IP subnet mask> | R | set static route subnet mask. |
| | | | gateway <IP address> | R | set static route gateway address. |
| | | | metric <metric #> | R | set static route metric number. |
| | | | private <yes no> | R | set private mode. |
| | | | active <yes no> | R | set static route rule enable or disable. |
| | udp | | | R + B | |
| | | status | | R + B | display udp status |
| | tcp | | | R + B | |
| | | status | [tcb] [<interval>] | R + B | display TCP statistic counters |
| | telnet | | <host> [port] | R + B | execute telnet clinet command |
| | traceroute | | <host> [ttl] [wait] [queries] | R + B | send probes to trace route of a remote host |
| | xparent | | | R | |
| | | join | <iface1> [<iface2>] | R | join iface2 to iface1 group |
| | | break | <iface> | R | break iface to leave ipxparent group |
| | urlfilter | | | R + B | |
| | | customize | | R + B | |
| | | | display | R + B | display customize action flags |
| | | | actionFlags [filterList/disableAllExceptTrusted/unblock RWFTToTrusted/keywordBlock/fullPath/case Insensitive/fileName][enable/disable] | R + B | set action flags |
| | | | logFlags [type(1-3)][enable/disable] | R + B | set log flags |
| | | | add [string] [trust/untrust/keyword] | R + B | add url string |
| | | | delete [string] [trust/untrust/keyword] | R + B | delete url string |
| | | | reset | R + B | clear all information |
| | | general | | R + B | |
| | | | enable | R + B | enable/disable url filter function |
| | | | display | R + B | display content filer's general setting |
| | | | webFeature | R + B | [block/nonblock] [activex/java/cookei/webproxy] |
| | | | timeOfDay[always/hh:mm] [hh:mm] | R + B | set block time |
| | | | exemptZone display | R + B | display exemptzone information |
| | | | exemptZone actionFlags [type(1-3)][enable/disable] | R + B | set action flags |
| | | | exemptZone add [ip1] [ip2] | R + B | add exempt range |
| | | | exemptZone delete [ip1] [ip2] | R + B | delete exempt range |

| | | | | | |
|--|----------|------------|-----------------------------------|-------|--|
| | | | exemptZone reset | R + B | clear exemptzone information |
| | | | reset | R + B | reset content filter's general setting |
| | | webControl | | R + B | |
| | | | enable | R + B | enable cbr_filter |
| | | | display | R + B | display cbr_filter's setting |
| | | | logAndBlock [log/block/both] | R + B | set log or block on matched web site |
| | | | category | R + B | set blocked categories |
| | | | serverList display | R + B | display current cbr_filter servers |
| | | | serverList refresh | R + B | refresh cbr_filter servers |
| | | | queryURL [url][Server/localCache] | R + B | query url need to block or forward according the database on server or local cache |
| | | | cache display | R + B | display the local cache entries |
| | | | cache delete [entrynum/All] | R + B | delete the local cache entries |
| | | | cache timeout [hour] | R + B | Set timeout value of cache entries |
| | | | blockonerror [log/block][on/off] | R + B | choose log or block when server is unavailable |
| | | | unratedwebsite[block log][on/off] | | choose log or block for unrated web site |
| | | | waitingTime [sec] | R + B | set waiting time for server |
| | | | reginfo display | R + B | display the license key with cerberian |
| | | | reginfo refresh | R + B | Check whether device had been registered and write the original license key to flash |
| | | | zssw | R + B | change the zssw's URL |
| | tredir | | | R | |
| | | failcount | <count> | R | set tredir failcount |
| | | partner | <ipaddr> | R | set tredir partner |
| | | target | <ipaddr> | R | set tredir target |
| | | timeout | <timeout> | R | set tredir timeout |
| | | checktime | <period> | R | set tredir checktime |
| | | active | <on/off> | R | set tredir active |
| | | save | | R | save tredir information |
| | | disp | | R | display tredir information |
| | | debug | <value> | R | set tredir debug value |
| | rpt | | | R + B | |
| | | active | [0:lan][1:yes 0:no] | R + B | active report |
| | | start | | R + B | start report |
| | | stop | | R + B | stop report |
| | | url | [num] | R + B | top url hit list |
| | | ip | [num] | R + B | top ip addr list |
| | | srv | [num] | R + B | top service port list |
| | dropIcmp | | [0 1] | R + B | to drop ICMP fragment packets |
| | nat | | | R | |
| | | period | [period] | R | set nat timer period |
| | | port | [port] | R | set nat starting external port number |
| | | checkport | | R | verify all server tables are valid |
| | | timeout | | R | |
| | | | gre [timeout] | R | set nat gre timeout value |
| | | | iamt [timeout] | R | set nat iamt timeout value |
| | | | generic [timeout] | R | set nat generic timeout value |
| | | | reset [timeout] | R | set nat reset timeout value |
| | | | tcp [timeout] | R | set nat tcp timeout value |

| | | | | | |
|--|------|------------|--------------------------------------|---|---|
| | | | tcpother [timeout] | R | set nat tcp other timeout value |
| | | | udp [port] <value> | R | set nat udp timeout value of specific port |
| | | update | | R | create nat system information from spSysParam |
| | | iamt | <iface> | R | display nat iamt information |
| | | iface | <iface> | R | show nat status of an interface |
| | | lookup | <rule set> | R | display nat lookup rule |
| | | new-lookup | <rule set> | R | display new nat lookup rule |
| | | loopback | [on/off] | R | turn on/off nat loopback flag |
| | | reset | <iface> | R | reset nat table of an iface |
| | | server | | R | |
| | | | disp | R | display nat server table |
| | | | load <set id> | R | load nat server information from ROM |
| | | | save | R | save nat server information to ROM |
| | | | clear <set id> | R | clear nat server information |
| | | | edit active <yes/no> | R | set nat server edit active flag |
| | | | edit svrport <start port> [end port] | R | set nat server server port |
| | | | edit intport <start port> [end port] | R | set nat server forward port |
| | | | edit remotehost <start ip> [end ip] | R | set nat server remote host ip |
| | | | edit leasetime [time] | R | set nat server lease time |
| | | | edit rulename [name] | R | set nat server rule name |
| | | | edit forwardip [ip] | R | set nat server server ip |
| | | | edit protocol [protocol id] | R | set nat server protocol |
| | | | edit clear | R | clear one rule in the set |
| | | service | | R | |
| | | | irc [on/off] | R | turn on/off irc flag |
| | | | xboxlive [on/off] | R | turn on/off xboxlive flag |
| | | | aol [on/off] | R | Turn on/off aol flag |
| | | resetport | | R | reset all nat server table entries |
| | | incikeport | <iface>[on/off] | R | turn on/off increase ike port flag |
| | | session | [session per host] | R | set nat session per host value |
| | | deleteslot | <iface> <slot> | R | delete specific slot of iface |
| | | routing | [0:LAN] [0:no 1:yes] | R | set NAT routing attributes |
| | igmp | | | R | |
| | | debug | [level] | R | set igmp debug level |
| | | forwardall | [on/off] | R | turn on/off igmp forward to all interfaces flag |
| | | querier | [on/off] | R | turn on/off igmp stop query flag |
| | | iface | | R | |
| | | | <iface> grouptm <timeout> | R | set igmp group timeout |
| | | | <iface> interval <interval> | R | set igmp query interval |
| | | | <iface> join <group> | R | join a group on iface |
| | | | <iface> leave <group> | R | leave a group on iface |
| | | | <iface> query | R | send query on iface |
| | | | <iface> rsptime [time] | R | set igmp response time |
| | | | <iface> start | R | turn on of igmp on iface |
| | | | <iface> stop | R | turn off of igmp on iface |
| | | | <iface> ttl <threshold> | R | set ttl threshold |
| | | | <iface> v1compat [on/off] | R | turn on/off v1compat on iface |
| | | robustness | <num> | R | set igmp robustness variable |
| | | status | | R | dump igmp status |

IPSec Related Command (All commands can only be used in Router Mode)

[Home](#)

| Command | | | | Description |
|---------|------------------|--------------------------------|--|--|
| ipse | | | | |
| | debug | type | <0:Disable 1:Original on off 2:IKE on off 3: IPSec [SPI] on off 4:XAUTH on off 5:CERT on off 6: All> | Turn on off trace for IPsec debug information |
| | | level | <0:None 1:User 2:Low 3:High> | Set the debug level. Higher number means more detailed. |
| | | display | | Show debugging information, include type and level. |
| | route | dmz | <on off> | After a packet is IPSec processed and will be sent to DMZ side, this switch is to control if this packet can be applied IPSec again. |
| | | | | Remark: Only supported in ZyWALL100 |
| | | lan | <on off> | After a packet is IPSec processed and will be sent to LAN side, this switch is to control if this packet can be applied IPSec again. |
| | | | | Remark: Command available since 3.50(WA.3) |
| | | wan | <on off> | After a packet is IPSec processed and will be sent to WAN side, this switch is to control if this packet can be applied IPSec again. |
| | show_run time | sa | | display runtime phase 1 and phase 2 SA information |
| | | spd | | When a dynamic rule accepts a request and a tunnel is established, a runtime SPD is created according to peer local IP address. This command is to show these runtime SPD. |
| | | List | | Display brief runtime phase 1 and phase 2 SA information |
| | switch | <on off> | | As long as there exists one active IPSec rule, all packets will run into IPSec process to check SPD. This switch is to control if a packet should do this. If it is turned on, even there exists active IPSec rules, packets will not run IPSec process. |
| | timer | chk_conn. | <0~255> | - Adjust auto-timer to check if any IPsec connection has "only outbound traffic but no inbound traffic" for certain period. If yes, system will disconnect it. |
| | | | | - Interval is in minutes |
| | | | | - Default is 2 minuets |
| | | | | - 0 means never timeout |
| | | update_peer | <0~255> | - Adjust auto-timer to update IPSec rules which use domain name as the secure gateway IP. |
| | | | | - Interval is in minutes |
| | | | | - Default is 30 minutes |
| | | | | - 0 means never update |
| | | chk_input | <0~255> | - Adjust input timer to check if any IPsec connection has no inbound traffic for a certain period. If yes, system will disconnect it. |
| | | | | - Interval is in minutes |
| | | | | - Default is 2 minuets |
| | | | | - 0 means never timeout |
| | updatePe erIp | | | Force system to update IPSec rules which use domain name as the secure gateway IP right away. |
| | dial | <rule index> <policy index> | | Initiate IPSec rule <#> policy <#> from ZyWALL box |
| | ikeDispla y | <rule #> | | Display IKE rule #, if no rule number assigned, this command will show current working buffer. NOTE: If |

| | | | | |
|--|--------------|-----------------|---|---|
| | | | | working buffer is null, it will show error messages. Please ADD or EDIT an IKE rule before display. |
| | ikeAdd | | | Create a working buffer for IKE rule. |
| | ikeEdit | <rule #> | | Edit an existing IKE rule # |
| | ikeSave | | | Save working buffer of IKE rule to romfile. |
| | ikeList | | | List all IKE rules |
| | ikeDelete | <rule #> | | Delete IKE rule # |
| | ikeConfig | name | <string> | Set rule name (max length is 31) |
| | | negotiationMode | <0:Main 1:Aggressive> | Set negotiation mode |
| | | natTraversal | <Yes No> | Enable NAT traversal or not. |
| | | multiPro | <Yes No> | Enable multiple proposals in IKE or not |
| | | lclDType | <0:IP 1:DNS 2:Email> | Set local ID type |
| | | lclDContent | <string> | Set local ID content |
| | | myIpAddr | <IP address> | Set my IP address |
| | | peerIdType | <0:IP 1:DNS 2:Email> | Set peer ID type |
| | | peerIdContent | <string> | Set peer ID content |
| | | secureGwAddr | <IP address Domain name> | Set secure gateway address or domain name |
| | | authMethod | <0:PreSharedKey 1:RSA Signature 2:preShare Key+XAUTH 3:RSA Signature+XAUTH> | Set authentication method in phase 1 in IKE |
| | | preShareKey | <ASCII 0xHEX> | Set pre shared key in phase 1 in IKE |
| | | certificate | <certificate name> | Set certificate file if using RSA signature as authentication method. |
| | | encryAlgo | <0:DES 1:3DES 2:AES> | Set encryption algorithm in phase 1 in IKE |
| | | authAlgo | <0:MD5 1:SHA1> | Set authentication algorithm in phase 1 in IKE |
| | | saLifeTime | <seconds> | Set sa life time in phase 1 in IKE |
| | | keyGroup | <0:DH1 1:DH2> | Set key group in phase 1 in IKE |
| | | xauth | type <0:Client Mode 1:Server Mode> | Set client or server mode. |
| | | | username <name> | Set xauth user name |
| | | | password <password> | Set xauth password |
| | | | radius <username> <password> | Ser radius username and password |
| | ipsecDisplay | <rule #> | | Display IPSec rule #, if no rule number assigned, this command will show current working buffer. NOTE: If working buffer is null, it will show error messages. Please ADD or EDIT an IPSec rule before display. |
| | ipsecAdd | | | Create a working buffer for IPSec rule. |
| | ipsecEdit | <rule #> | | Edit IPSec rule # |
| | ipsecSave | | | Save working buffer of IPSec rule to romfile. |
| | ipsecList | | | List all IPSec rules |
| | ipsecDelete | <rule #> | | Delete IPSec rule # |
| | ipsecConfig | name | <string> | Set rule name. (max length is 31) |
| | | active | <Yes No> | Set active or not |
| | | saIndex | <index> | Bind to which IKE rule. |
| | | multiPro | <Yes No> | Enable multiple proposals in IPSec or not |
| | | nailUp | <Yes No> | Enable nailed-up or not |
| | | activeProtocol | <0:AH 1:ESP> | Set active protocol in IPSec |
| | | encryAlgo | <0:Null 1:DES 2:3DES 3:AES> | Set encryption algorithm in IPSec |
| | | encryKeyLen | <0:128 1:192 2:256> | Set encryption key length in IPSec |
| | | authAlgo | <0:MD5 1:SHA1> | Set authentication algorithm in IPSec |
| | | saLifeTime | <seconds> | Set sa life time in IPSec |
| | | encap | <0:Tunnel 1:Transport> | set encapsulation in IPSec |

| | | | | |
|--|---------------|-----------------|-------------------------------------|---|
| | | pfs | <0:None 1:DH1 2:DH2> | set pfs in phase 2 in IPSec |
| | | antiReplay | <Yes No> | Set anitreplay or not |
| | | controlPing | <Yes No> | Enable control ping or not |
| | | logControlPing | <Yes No> | Enable logging control ping events or not |
| | | controlPingAddr | <IP> | Set control ping address |
| | | protocol | <1:ICMP 6:TCP 17:UDP> | Set protocol |
| | | lcAddrType | <0:single 1:range 2:subnet> | Set local address type |
| | | lcAddrStart | <IP> | Set local start address |
| | | lcAddrEndMask | <IP> | Set local end address or mask |
| | | lcPortStart | <port> | Set local start port |
| | | lcPortEnd | <port> | Set local end port |
| | | rmAddrType | <0:single 1:range 2:subnet> | Set remote address type |
| | | rmAddrStart | <IP> | Set remote start address |
| | | rmAddrEndMask | <IP> | Set remote end address or mask |
| | | rmPortStart | <port> | Set remote start port |
| | | rmPortEnd | <port> | Set remote end port |
| | policyList | | | List all IPSec policies |
| | manualDisplay | <rule #> | | Display manual rule # |
| | manualAdd | | | Add manual rule |
| | manualEdit | <rule #> | | Edit manual rule # |
| | manualSave | | | Save IPSec rules |
| | manualList | | | List all IPSec rule |
| | manualDelete | <rule #> | | Delete IPSec rule # |
| | manualConfig | name | <string> | Set rule name |
| | | active | <Yes No> | Set active or not |
| | | myIpAddr | <IP address> | Set my IP address |
| | | secureGwAddr | <IP address> | Set secure gateway |
| | | protocol | <1:ICMP 6:TCP 17:UDP> | Set protocol |
| | | lcAddrType | <0:single 1:range 2:subnet> | Set local address type |
| | | lcAddrStart | <IP> | Set local start address |
| | | lcAddrEndMask | <IP> | Set local end address or mask |
| | | lcPortStart | <port> | Set local start port |
| | | lcPortEnd | <port> | Set local end port |
| | | rmAddrType | <0:single 1:range 2:subnet> | Set remote address type |
| | | rmAddrStart | <IP> | Set remote start address |
| | | rmAddrEndMask | <IP> | Set remote end address or mask |
| | | rmPortStart | <port> | Set remote start port |
| | | rmPortEnd | <port> | Set remote end port |
| | | activeProtocol | <0:AH 1:ESP> | Set active protocol in manual |
| | | ah | encap <0:Tunnel 1:Transport> | Set encapsulation in ah in manual |
| | | | spi <decimal> | Set spi in ah in manual |
| | | | authAlgo <0:MD5 1:SHA1> | Set authentication algorithm in ah in manual |
| | | | authKey <string> | Set authentication key in ah in manual |
| | | esp | encap <0:Tunnel 1:Transport> | Set encapsulation in esp in manual |
| | | | spi <decimal> | Set spi in esp in manual |
| | | | encryAlgo <0:Null 1:DES 2:3DES> | Set encryption algorithm in esp in manual |
| | | | encryKey <string> | Set encryption key in esp in manual |
| | | | authAlgo <0:MD5 1:SHA1> | Set authentication algorithm in esp in manual |

| | | | | |
|--|------------------|--|-------------------------------|---|
| | | | authKey < string> | Set authentication key in esp in manual |
| | manualPolicyList | | | List all manual policy |
| | swSkipOverlapIp | | <on/off> | <ul style="list-style-type: none"> - When a VPN rule with remote range overlaps with local range, the switch decides if a local to local packet should apply this rule. - Default value is “off” which means “no skip”. |
| | adjTcpMss | | <off auto user defined value> | <ul style="list-style-type: none"> - After a tunnel is established, system will automatically adjust TCP MSS. - After all tunnels are drops, the MSS will adjust to the original value. - The default value is auto. |
| | Drop | | <policy index> | Drop a active tunnel. |

Firewall Related Command (All command can be used in both Router Mode and Bridge Mode)[Home](#)

| Command | | | | | Description |
|---------|----------|-------------|--------------------------|--------------------|---|
| sys | Firewall | | | | |
| | | acl | | | |
| | | | disp | | Display specific ACL set # rule #, or all ACLs. |
| | | active | <yes/no> | | Active firewall or deactivate firewall |
| | | clear | | | Clear firewall log |
| | | cnt | | | |
| | | | disp | | Display firewall log type and count. |
| | | | clear | | Clear firewall log count. |
| | | disp | | | Display firewall log |
| | | online | | | Set firewall log online. |
| | | dynamicrule | | | |
| | | | display | | Display firewall dynamic rules |
| | | dos | | | |
| | | | smtp | | Set SMTP DoS defender on/off |
| | | | display | | Display SMTP DoS defender setting. |
| | | | ignore | | Set if firewall ignore DoS in lan/wan/dmz/wlan |
| | | ignore | | | |
| | | | triangle | | Set if firewall ignore triangle route in lan/wan/dmz/wlan |
| | | schedule | | | |
| | | | load [set # rule #] | | Load firewall ACL schedule by rule. |
| | | | display | | Display ACL schedule in buffer. |
| | | | save | | Save buffer date and update runtime firewall ACL rule. |
| | | | week | | |
| | | | | monday [on/off] | Set schedule on or off by day – Monday. |
| | | | | tuesday [on/off] | Set schedule on or off by day – Tuesday. |
| | | | | wednesday [on/off] | Set schedule on or off by day – Wednesday. |
| | | | | thursday [on/off] | Set schedule on or off by day – Thursday. |
| | | | | friday [on/off] | Set schedule on or off by day – Friday. |
| | | | | saturday [on/off] | Set schedule on or off by day – Saturday. |
| | | | | sunday [on/off] | Set schedule on or off by day – Sunday. |
| | | | | allweek [on/off] | Quick set schedule on or off by week. |
| | | | timeOfDay [always/hh:mm] | | Set firewall ACL schedule block time of day. |

Certificate Management (PKI) Command

(All commands can be used in both Router Mode and Bridge Mode)

[Home](#)

| Command | | | | Description |
|--------------|----------------|---------------|--|--|
| certificates | | | | |
| | my_certificate | | | |
| | | create | | |
| | | | selfsigned <name> <subject> [key size] | Create a self-signed local host certificate. <name> specifies a descriptive name for the generated certificate. <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn;{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits. |
| | | | request <name> <subject> [key size] | Create a certificate request and save it to the router for later manual enrollment. <name> specifies a descriptive name for the generated certification request. <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn;{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits. |
| | | | scep_enroll <name> <CA addr> <CA cert> <auth key> <subject> [key size] | Create a certificate request and enroll for a certificate immediately online using SCEP protocol. <name> specifies a descriptive name for the enrolled certificate. <CA addr> specifies the CA server address. <CA cert> specifies the name of the CA certificate. <auth key> specifies the key used for user authentication. If the key contains spaces, please put it in quotes. To leave it blank, type "". <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn;{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits. |
| | | | cmp_enroll <name> <CA addr> <CA cert> <auth key> <subject> [key size] | Create a certificate request and enroll for a certificate immediately online using CMP protocol. <name> specifies a descriptive name for the enrolled certificate. <CA addr> specifies the CA server address. <CA cert> specifies the name of the CA certificate. <auth key> specifies the id and key used for user authentication. The format is "id:key". To leave the id and key blank, type ":". <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn;{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits. |
| | | import [name] | | Import the PEM-encoded certificate from stdin. [name] specifies the descriptive name (optional) as which the imported certificate is to be saved. For my certificate importation to be successful, a certification request corresponding to the imported certificate must already |

| | | | | |
|--|----------------|----------------------------------|--|--|
| | | | | exist on ZyWALL. After the importation, the certification request will automatically be deleted. If a descriptive name is not specified for the imported certificate, the certificate will adopt the descriptive name of the certification request. |
| | | export <name> | | Export the PEM-encoded certificate to stdout for user to copy and paste. <name> specifies the name of the certificate to be exported. |
| | | view <name> | | View the information of the specified local host certificate. <name> specifies the name of the certificate to be viewed. |
| | | verify <name> [timeout] | | Verify the certification path of the specified local host certificate. <name> specifies the name of the certificate to be verified. [timeout] specifies the timeout value in seconds (optional). The default timeout value is 20 seconds. |
| | | delete <name> | | Delete the specified local host certificate. <name> specifies the name of the certificate to be deleted. |
| | | list | | List all my certificate names and basic information. |
| | | rename <old name> <new name> | | Rename the specified my certificate. <old name> specifies the name of the certificate to be renamed. <new name> specifies the new name as which the certificate is to be saved. |
| | | def_selfsigned [name] | | Set the specified self-signed certificate as the default self-signed certificate. [name] specifies the name of the certificate to be set as the default self-signed certificate. If [name] is not specified, the name of the current self-signed certificate is displayed. |
| | ca_trusted | | | |
| | | import <name> | | Import the PEM-encoded certificate from stdin. <name> specifies the name as which the imported CA certificate is to be saved. |
| | | export <name> | | Export the PEM-encoded certificate to stdout for user to copy and paste. <name> specifies the name of the certificate to be exported. |
| | | view <name> | | View the information of the specified trusted CA certificate. <name> specifies the name of the certificate to be viewed. |
| | | verify <name> [timeout] | | Verify the certification path of the specified trusted CA certificate. <name> specifies the name of the certificate to be verified. [timeout] specifies the timeout value in seconds (optional). The default timeout value is 20 seconds. |
| | | delete <name> | | Delete the specified trusted CA certificate. <name> specifies the name of the certificate to be deleted. |
| | | list | | List all trusted CA certificate names and basic information. |
| | | rename <old name> <new name> | | Rename the specified trusted CA certificate. <old name> specifies the name of the certificate to be renamed. <new name> specifies the new name as which the certificate is to be saved. |
| | | crl_issuer <name> [on/off] | | Specify whether or not the specified CA issues CRL. <name> specifies the name of the CA certificate. [on/off] specifies whether or not the CA issues CRL. If [on/off] is not specified, the current crl_issuer status of the CA. |
| | remote_trusted | | | |
| | | import <name> | | Import the PEM-encoded certificate from stdin. <name> specifies the name as which the imported remote host certificate is to be saved. |

| | | | | |
|--|--------------|--|--|--|
| | | export <name> | | Export the PEM-encoded certificate to stdout for user to copy and paste. <name> specifies the name of the certificate to be exported. |
| | | view <name> | | View the information of the specified trusted remote host certificate. <name> specifies the name of the certificate to be viewed. |
| | | verify <name> [timeout] | | Verify the certification path of the specified trusted remote host certificate. <name> specifies the name of the certificate to be verified. [timeout] specifies the timeout value in seconds (optional). The default timeout value is 20 seconds. |
| | | delete <name> | | Delete the specified trusted remote host certificate. <name> specifies the name of the certificate to be deleted. |
| | | list | | List all trusted remote host certificate names and basic information. |
| | | rename <old name> <new name> | | Rename the specified trusted remote host certificate. <old name> specifies the name of the certificate to be renamed. <new name> specifies the new name as which the certificate is to be saved. |
| | dir_service | | | |
| | | add <name> <addr[:port]> [login:pswd] | | Add a new directory service. <name> specifies a descriptive name as which the added directory server is to be saved. <addr[:port]> specifies the server address (required) and port (optional). The format is "server-address[:port]". The default port is 389. [login:pswd] specifies the login name and password, if required. The format is "[login:password]". |
| | | delete <name> | | Delete the specified directory service. <name> specifies the name of the directory server to be deleted. |
| | | view <name> | | View the specified directory service. <name> specifies the name of the directory server to be viewed. |
| | | edit <name> <addr[:port]> [login:pswd] | | Edit the specified directory service. <name> specifies the name of the directory server to be edited. <addr[:port]> specifies the server address (required) and port (optional). The format is "server-address[:port]". The default port is 389. [login:pswd] specifies the login name and password, if required. The format is "[login:password]". |
| | | list | | List all directory service names and basic information. |
| | | rename <old name> <new name> | | Rename the specified directory service. <old name> specifies the name of the directory server to be renamed. <new name> specifies the new name as which the directory server is to be saved. |
| | cert_manager | | | |
| | | reinit | | Reinitialize the certificate manager. |

Bandwidth management Related Command

(All commands can be used in both Router Mode and Bridge Mode)

[Home](#)

| Command | | | | | | Description |
|---------|-----------|-----|--------|-----------------|--|---|
| bm | | | | | | |
| | interface | lan | enable | <bandwidth xxx> | | Enable bandwidth management in LAN with bandwidth xxx bps. If the user doesn't set the bandwidth, the default value is 100Mbps. |
| | | | | <wrr pr> | | Select fairness-based(WRR) or priority-based(PRR) mechanism. the default value is fairness-based. |
| | | | | <efficient> | | Enable work-conserving feature. |

| | | | | | | |
|--|--------|-----------|---------|--|-----------------|---|
| | | | disable | | | Disable bandwidth management in LAN |
| | | wan | enable | <bandwidth xxx> | | Enable bandwidth management in WAN with bandwidth xxx bps. If the user doesn't set the bandwidth, the default value is 100Mbps. |
| | | | | <wrr pr> | | Select fairness-based(WRR) or priority-based(PRR) mechanism. the default value is fairness-based. |
| | | | | <efficient> | | Enable work-conserving feature. |
| | | | disable | | | Disable bandwidth management in WAN |
| | class | lan | add # | bandwidth xxx | <name xxx> | Add a class with bandwidth xxx bps in LAN. The name is for users' information. |
| | | | | | <priority x> | Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The default value is 3. |
| | | | | | <borrow on off> | The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The default value is off. |
| | | | mod # | <bandwidth xxx> | | Modify the parameters of the class in LAN. The bandwidth is unchanged if the user doesn't set a new value. |
| | | | | <name xxx> | | Set the class' name. |
| | | | | <priority x> | | Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The priority is unchanged if the user doesn't set a new value. |
| | | | | <borrow on off> | | The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The borrow is unchanged if the user doesn't set a new value. |
| | | | del # | | | Delete the class # and its filter and all its children class and their filters in LAN. |
| | | wan | add # | bandwidth xxx | <name xxx> | Add a class with bandwidth xxx bps in WAN. The name is for users' information. |
| | | | | | <priority x> | Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The default value is 3. |
| | | | | | <borrow on off> | The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The default value is off. |
| | | | mod # | <bandwidth xxx> | | Modify the parameters of the class in WAN. The bandwidth is unchanged if the user doesn't set a new value. |
| | | | | <name xxx> | | Set the class' name. |
| | | | | <priority x> | | Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The priority is unchanged if the user doesn't set a new value. |
| | | | | <borrow on off> | | The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The borrow is unchanged if the user doesn't set a new value. |
| | | | del # | | | Delete the class # and its filter and all its children class and their filters in WAN. |
| | filter | lan | add # | Daddr <mask Dmask> Dport Saddr <mask Smask> Sport protocol | | Add a filter for class # in LAN. The filter contains destination address (netmask), destination port, source address (netmask), source port and protocol. You may set the value as 0 if you do not care the item. |
| | | | del # | | | Delete a filter which belongs to class # in LAN. |
| | | wan | add # | Daddr <mask Dmask> Dport Saddr <mask Smask> Sport protocol | | Add a filter for class # in WAN. The filter contains destination address (netmask), destination port, source address (netmask), source port and protocol. You may set the value as 0 if you do not care the item. |
| | | | del # | | | Delete a filter which belongs to class # in WAN. |
| | show | interface | lan | | | Show the interface settings of LAN |
| | | | wan | | | Show the interface settings of WAN |
| | | class | lan | | | Show the classes settings of LAN |

| | | | | | | |
|--|---------|------------|-----|--|--|--|
| | | | wan | | | Show the classes settings of WAN |
| | | filter | lan | | | Show the filters settings of LAN |
| | | | wan | | | Show the filters settings of WAN |
| | | statistics | lan | | | Show the statistics of the classes in LAN |
| | | | wan | | | Show the statistics of the classes in WAN |
| | monitor | lan | <#> | | | Monitor the bandwidth of class # in LAN. If the class is not specific, all the classes in LAN will be monitored. The first time you key the command will set it on; the second time you will set it off, and so on. |
| | | wan | <#> | | | Monitor the bandwidth of class # in WAN. If the class is not specific, all the classes in WAN will be monitored. The first time you key the command will set it on; the second time you will set it off, and so on. |
| | config | save | | | | Save the configuration. |
| | | load | | | | Load the configuration. |
| | | clear | | | | Clear the configuration. |

Bridge Related Command

[Home](#)

| Command | | | | Flag | Description |
|---------|-------|---------|----------------|-------|---|
| bridge | | | | R + B | |
| | cnt | | | R + B | related to bridge routing statistic table |
| | | disp | | R + B | display bridge route counter |
| | | clear | | R + B | clear bridge route counter |
| | iface | | | R + B | Related to “bridge mode” access interface |
| | | active | <yes/no> | R + B | Active bridge mode iface or not |
| | | address | [ip] | B | Remote access IP address |
| | | dns1 | [ip] | B | First DNS server |
| | | dns2 | [ip] | B | Second DNS server |
| | | dns3 | [ip] | B | Third DNS server |
| | | mask | [network mask] | B | Network mask |
| | | gateway | [gateway ip] | B | Network gateway |
| | | display | | B | Display whole interface information |
| | stat | | | R + B | related to bridge packet statistic table |
| | | disp | | R + B | display bridge route packet counter |
| | | clear | | R + B | clear bridge route packet counter |

myZyXEL.com Command

[Home](#)

| Command | | | | Description | Flag |
|---------|------------|---------------|--|--|------|
| sys | | | | | U+R |
| | myZyxelCom | | | | U+R |
| | | checkUserName | <username> | Check the username exists or not | U+R |
| | | register | <username> <password> <email> <countryCode> | Input the registration information, include username, password, email, and country code. | U+R |
| | | trialService | <service>, 1 : CF, 2 : 3in1, 3 : CF + 3in1 | Input the service that to be tried. | U+R |

| | | | | | |
|--|--|----------------|---------------|---|-----|
| | | serviceUpgrade | <licence key> | Inout license key that you want to let service from trial to standard | U+R |
| | | serviceRefresh | NULL | Refresh the myZyXEL.com service status | U+R |
| | | display | NULL | Display all myZyXEL.com setting | U+R |
| | | serviceDisplay | NULL | Display all service status, include expired day. | U+R |

Vantage Related Command

[Home](#)

| Command | | | | Description |
|---------|-----------|-----------|--|--|
| cnm | active | [0/1] | | Display or set the CNM features to enable or disable . 0: disable 1: enable CNM features and communicate through WAN interface. |
| | sgid | [ID] | | Display or set sgid which is the unique ID of the device in Vantage. |
| | managerIP | [addr] | | Display or set the IP of Vantage server/COMServer which manage this device. [addr] specifies the IP of the Vantage serve/COMServer. |
| | Debug | [0/1] | | Display or set the way of outputting CNM debug messages. 0: disable debug messages. 1: output the debug messages to console and can accept SGMP inquire message only after the device is registered to Vantage server. |
| | version | | | Display the Vantage agent version. |
| | keepalive | [seconds] | | Display or set the keepalive report time. 10~655: Valid values, default 60 seconds. |