



**Firmware Release Note**

## **ZyWALL 5**

**Release 3.64(XD.1)**

**Date:**  
**Author:**  
**Project Leader:**

**May 03, 2005**  
**Nash Fan**  
**Stanley Liu**

## **ZyXEL ZyWALL 5 Standard Version release 3.64(XD.1) Release Note**

**Date:** May 03, 2005

### **Supported Platforms:**

---

ZyXEL ZyWALL 5

### **Versions:**

---

ZyNOS Version: V3.64(XD.1) | 05/03/2005 10:49:34

Bootbase Version: V1.08 | 01/28/2005 14:47:16

Vantage Agent Version: 1.0.0

### **Note:**

---

1. Restore to Factory Defaults Setting Requirement: No.
2. The setting of ignore triangle route is on in default ROM FILE. 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. When firewall turns from "off" to "on", the firewall initialization procedure will disconnect all connections running through the ZyWALL.
5. 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.
6. In WLAN configuration, a switch for enable / disable WLAN is added. The default value is "**disable**" since WLAN without any security setting is vulnerable. Please configure MAC filter, WEP and 802.1X when you enable WLAN feature.
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. The default port roles for LAN/DMZ setting is: port 1 to port 4 are all LAN ports.
9. 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.
10. You must notice those metric values of WAN, Traffic-Redirect and Dial-backup. You

should better give those values, Dial-backup > Traffic-Redirect > WAN. For example, WAN (1), Traffic-Redirect(14), Dial-backup(15).

11. Under Bridge Mode, all LAN ports will behave as a hub, and all DMZ ports will also behave as another hub.
12. For users using the default ROMFILE in former release, please remove “ip nat session 1300” from autoexec.net by CI command “sys edit autoexec.net”.
13. The first entry for static route is reserved for creating WAN default routes and is READ-ONLY.
14. In previous 3.64 firmware, the VID value of DPD is not correct. VID change will cause current version doesn't work with the wrong value. Please be sure to connect with devices which has updated VID, or the DPD may not work correctly.

## **Known Issues:**

---

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.
3. On the SUA/ Address Mapping Edit page, the user can give the same local IP and global IP.
4. If the metric of dial-backup is smaller (has higher priority) than the metric of Traffic-Redirect, Traffic-Redirect can't be triggered any more.
5. Sometimes, modify an active IPsec rule (the VPN tunnel was created) will crash the system, if this tunnel is going the re-key process.
6. Bandwidth Management doesn't work on wireless LAN.
7. Symptom: LAN host can ping Internet while LAN host change cable from LAN port to DMZ port.  
Condition:
  - (1) Host connect to LAN port and get DHCP address from router.
  - (2) Unplug LAN host cable and plug it into DMZ port.
  - (3) The host can still ping Internet using LAN DHCP address
  - (4) The scenario will continue about 30secs.
8. The DMZ TxPkts counter increment at about 1 pkt/min even without any Ethernet cables ever connected.
9. At SMT24.1, the collisions for WAN, LAN and DMZ port are not really counted.
10. 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.
11. Bandwidth Management works abnormally when using Fairness/Priority scheduler and “borrow” is enabled on all classes.
12. Under PPTP encapsulation mode, we can not access some website like <http://www.kimo.com.tw/>
13. In eWC->Statistics, Tx data for Dial Backup is not correct.
14. Some limitations on Firewall CLI configuration:

## **ZyXEL Confidential**

- (1) User can not delete specific address or custom port entry from a rule.
- (2) CLI doesn't support Modify and Move for rules implemented in eWC.
- (3) eWC can not display firewall rule field correctly if rule is added by CI command and its type is port/address range.
- 15. Can't block ActiveX in some case. (Sometime the ActiveX block fail. 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.)
- 16. Don't use CI command "bridge rstp bridge enable" to enable RSTP, it will change the initial Path Cost value to an incorrect value.
- 17. G-100 WLAN card, does not support the fragment size below 800.
- 18. Bandwidth management H.323 service does not support Netmeeting H.323 application.
- 19. P2002 P-to-P cannot pass through router.
- 20. If you were using MSN Messenger Voice Communication through ZyWALL UPnP and found voice is blocked by firewall, we suggest you download MSN Messenger 7.0 and try again. This is because we found MSN Messenger 6.2 sometimes fails to detect UPnP status when it's starting voice invitation.
- 21. The domain name update timer for VPN sometimes can't work correctly. (GUI/VPN/Global Setting)
- 22. 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.
- 23. In BWM, subclass cannot borrow the remaining free bandwidth from parent class in Priority-Based mode.
- 24. 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.

## **Features:**

---

### **Modifications in V3.64(XD.1) | 05/03/2005**

Modify for formal release.

### **Modifications in V 3.64(XD.1)b2 | 04/27/2005**

- 1. [BUG FIX] 050201039
  - Symptom: "Gateway Domain Name Update Timer" in eWC --> VPN --> Global Setting didn't work.
  - Condition:
    - (1) Set one IKE rule which secured gateway address is domain name.
    - (2) Set "Gateway Domain Name Update Timer" to 15 minutes and apply.
    - (3) System will not update secured gateway domain name according to the setting unless system reboot.
- 2. [BUG FIX]
  - Symptom: LAN & WAN deathed when receive UDP packets which comes from TfGen.

Condition:

- (1) Restore default rom file.
  - (2) In WAN side, place a PC and open TfGen tool to send packets to router's WAN.
  - (3) The TfGen's setting in my PC is: Utilization: 4kbps, Destion: "DUT's WAN IP", Port: 500.
  - (4) After a period time, DUT's LAN & WAN both deathed that all traffic can't go out.
3. [BUG FIX] 050203206
- Symptom: In bridge mode, after device synchronized the defined NTP server, the result displayed failed.

Condition:

- (1) PC(192.168.1.33) --- DUT(192.168.1.254) --- NAT(192.168.12.106) --- Internet.
- (2) In eWC/Maintenance/Time and Date, get from Time Server: Time Protocol=NTP (RFC 1305), Time Server Address= a.ntp.alphazed.net, then clicked "Synchronize Now" button.
- (3) The result displayed failed. ("System Time and Date Synchronization Fail")
- (4) However, a successful log showed in eWC/LOGS.
- (5) Actually, the device was successful to synchronize the defined NTP server.

**Modifications in V 3.64(XD.1)b1 | 04/22/2005**

1. [ENHANCEMENT]  
Enlarge content filter web site, forbidden key word and trusted website size to 100.
2. [ENHANCEMENT]  
Add sequence number and SPI in log for ESP / AH packets
3. [ENHANCEMENT]  
Change DNS Address Record size from 8 to 30
4. [EHNANCEMENT] 050419889  
Add IP information for my IP address and Secure Gateway address. In CI command, "ipsec ikeDisp #" will show IKE rule configuration. When my IP address or secure gateway address is domain name, the resolved IP will show after domain name.
5. [BUG FIX] 050128770  
Symptom: When users remotely manage the ZyWALL via a PPTP connection, a strange firewall session (between PPTP server and PPTP client) timeout log may be observed.  
Condition:  
  - (1) Configure the ZyWALL's WAN port to use PPTP encapsulation.
  - (2) Remotely login eWC (http/https) via the PPTP connection.
  - (3) After a few minutes, check the centralized logs or syslogs, you will observe a sequence of firewall logs of http/https session timeout.
6. [BUG FIX] 040507153  
Symptom: Telnet function takes too much time.  
Condition:  
  - (1) Type the CI command "ip telnet host\_A".
  - (2) When telnet from router to non-exist server host\_A, it always takes about 40 seconds or more to connect. And users cannot interrupt the router and can do nothing.

7. [BUG FIX] 050420986  
Symptom: P2000W and P2000W can not talk to each other in P2P mode.  
Condition:  
(1) Topology:  
P2000W----DUT---Internat---DUT---P2000W  
(2) P2000W and P2000W can not talk to each other in P2P mode.
8. [BUG FIX] 050217478  
Symptom: Netbios packet cannot pass through VPN tunnel .  
Condition:  
(1) Configure a VPN tunnel as follows:  
1.1 local subnet mask is 192.168.1.1/255.255.0.0.  
1.2 remote subnet mask is 192.169.1.1/255.255.0.0.  
1.3 Enable "Netbois pass through" in local and remote gateway.  
1.4 PC A(Local)-----ZyWALLA-----ZyWALLB---PC B(Remote)192.168.1.1/24  
192.169.1.1/24  
(2) Establish the VPN tunnel.  
(3) In PC A, Search PC B's computer name.  
(4) PC A will send a broadcast packet to search PC B.  
(5) ZyWALL A will change destination IP address from 192.168.255.255 to 192.169.255.255 and send to ZyWALL B after encryption. Horever, ZyWALL A should adjust the UDP checksum but it didn't.  
(6) PCB will drop the received broadcast UDP pcket from PC A due to error UDP checksum.
9. [BUG FIX] 050214274  
Symptom: VPN My IP Addr will resolving fail  
Condition:  
(1) Add a VPN rule and My IP Address and Remote Gateway Address are domain type.  
(2) Click Dial button, it will fail to build tunnel first time (second time is ok)  
(3) Check log will display "Cannot resolve My IP Addr for rule xxx"
10. [BUG FIX] 050304284  
Symptom: There is no log for replay packets  
Condition:  
(1) Enable "Anti-Replay" function.  
(2) Sniffer an ESP packet and replay it.  
(3) This ESP packet will be dropped by there is no log.  
(4) There should be log to show this action.
11. [BUG FIX] 050316859  
Symptom: ZyWALL (3.64) crashes while remote VPN software (ZyWALL VPN Client) make a VPN connection  
Condition:  
(1) ZyWALL start negotiating with remote VPN software.  
(2) The remote VPN software sends too long VID size.  
(3)device will crash.
12. [BUG FIX] 050221575  
Symptom: Max. Concurrent Sessions Per Host problem.

Condition:

- (1) In eWC->NAT , change Max. Concurrent Sessions Per Host to 300
- (2) Use ipscan tool to make session
- (3) Log show “192.168.1.33 exceeds the max. number of session per host! “ when exceeds the max. number of session per host, but Max. Concurrent Sessions Per Host (Historical high since last startup: 286), it’s not reach 300.

13. [BUG FIX] 050407161

Symptom: PC cannot ping remote secure gateway's LAN IP via VPN tunnel

Condition:

PC A (1.33) – (1.1)ZW5 --- LAB ---- ZW70 (2.1) ----(2.33) PC B

- (1) Add a VPN rule(ZW5), and in IPsec rule Local Network select Subnet Address, Starting IP is 192.168.1.0 / 255.255.255.0. Remote Network select Subnet Address Starting IP is 192.168.2.0 / 255.255.255.0.
- (2) ZW70 had opposite setting.
- (3) Build up this tunnel, PC A can ping PC B, but PC A can’t ping 192.168.2.1(ZW70 gateway LAN IP)

14. [BUG FIX] 050302166

Symptom: Remote gateway Address can’t configure as domain type when ipsec Nail-Up option is on.

Condition:

- (1) Add a VPN rule(Static rule) with Remote gateway Address set as domain type.
- (2) In Ipsec rule, enable Nail-Up option.
- (3) Return to IKE rule page, change some fields and click Apply. The Status will show “This ipsec rule bounds to dynamic IKE rule. Please inactive nail up.” and it can’t be saved.

15. [BUG FIX] 050309435

Symptom: Router crash when recieve UDP packets which comes from TfGen.

Condition:

- (1) Restore default rom file.
- (2) In WAN side, place a PC and open TfGen tool to send packets to router's WAN.
- (3) The TfGen's setting in my PC is: Utilization: 4kbps, Destion: 192.168.70.34, Port: 500.

16. [BUG FIX] 050214258

Symptom: DNS inverse query causes system crash.

Condition:

- (1) Set A PC on the device LAN site.
- (2) The DNS server of the PC sets to the device.
- (3) The PC sends DNS inverse query continually, the device will crash sometimes.

17. [BUG FIX] 050204235

Symptom: Responder receive duplicate package when VPN tunnel established

Condition:

- (1) At Initiator edit one VPN rule and Extended Authentication=enable=client mode
- (2) At responder edit one VPN rule and Extended Authentication=enable=server mode
- (3) when VPN tunnel established ,Responder log show “Rule[IKE1] receives duplicate packet”

**ZyXEL Confidential**

18. [BUG FIX] 050412413  
Symptom: There is no "Ping of Dead" log message when performing "Consolidate every 10 seconds ( Attack: ping of death ) "  
Condition:  
(1) Dos command "ping 192.168.1.1 -l 2000"  
(2) User can not see "ping of death" consolidation log on eWC/LOGS page  
(3) Bridge mode only.
19. [BUG FIX] 050303203  
Symptom: DNS inverse query causes memory leak.  
Condition:  
(1) Set A PC on the ZyWALL LAN site.  
(2) The DNS server of the PC sets to the ZyWALL.  
(3) The PC sends DNS inverse query continually (ex: 140.113.23.1), the system will generate memory leak.
20. [BUG FIX] 050201041  
Symptom: "Gateway Domain Name Update Timer" in eWC --> VPN --> Global Setting didn't work.  
Condition:  
(1) Set one IKE rule which secured gateway address is domain name.  
(2) Set "Gateway Domain Name Update Timer" to 15 minutes and apply.  
(3) System will not update secured gateway domain name according to the setting unless system reboot.
21. [BUG FIX] 050415693  
Symptom: Resolving a domain name which start with number (for example 4youcard.com) will fail.  
Condition: CI command "ip ping 4youcard.com" and it will fail.
22. [BUG FIX] 050406055  
Symptom: ZyWALL VPN traffic will lose from time to time  
Condition:  
(1) To create tunnel from zw5 to peer.  
(2) To ping the LAN PC of peer VPN gateway fom the LAN PC of zw5 via the tunnel.  
(3) About 1 min, it will re-key again.  
(4) The tunnel loses packet.
23. [BUG FIX] 041201001  
Symptom: Router will crash when receive an unrecognizable DNS response  
Condition:  
Environment:  
PC(192.168.1.33)-----(192.168.1.1)ZW5---Internet  
(1) Set ZW5's system DNS server as "164.67.128.1"  
(2) From PC, send a DNS query to ZW5. The DNS format is as following:  
cf 07 01 00 00 01 00 00 00 00 00 04 75 63 6c  
61 03 65 64 75 00 00 ff 00 01  
(3) ZW5 will relay the DNS query to "164.67.128.1".  
(4) ZW5 will crash after receive DNS response from "164.67.128.1"
24. [BUG FIX] 050311685  
Symptom: Firewall WAN to DMZ Reject can't work.



Condition: PC A ---- (W)ZW5 (DMZ) 10.1.1.1 --- 10.1.1.100 ZW10W

- (1) In eWC Firewall Default Action WAN to DMZ select Reject. And enable Log
- (2) One ZW10W connect to ZW5 DMZ port and IP is 10.1.1.100
- (3) Add default server 10.1.1.100.
- (4) PC A also can ftp to DMZ ZW10W.
- (5) Check Picture [ZW5]Firewall W2D item 3->1

25. [BUG FIX] 050420986

Symptom: External content filter cannot work.

Condition

- (1) Enable external content filter.
- (2) Use external content filter for a long time.
- (3) System cannot create socket anymore and external content filter cannot work.
- (4) Use CI command "ip ping 168.95.1.1", there will be a message "Can't create socket" in console.
- (5) You can see there are many used sockets via CI command "sys socket".

26. [BUG FIX] 050201045

Symptom: For firewall ACL schedule, if two rules have the same policies except "schedule", only the first rule will work.

Condition:

1. Set two firewall rules have same policies except schedule.
2. Only the first rule will work.

27. [BUG FIX] 050301081

Symptom: Subclass(FTP service) can not borrow all rest of parent bandwidth in priority-base.

Condition:

1. Root bandwidth is 1000kbps
2. Add a FTP service subclass which bandwidth is 100kbps and can borrow from parent.
3. Add a Custom service subclass which bandwidth is 100kbps and can borrow from parent
4. Execute FTP , but FTP service bandwidth can not borrow all rest of parent bandwidth
5. Send lots of UDP packet , but Custom service bandwidth can not borrow all rest of parent bandwidth. Sometimes all traffic can not pass through DUT.

28. [BUG FIX] 050128718

Symptom: The VT6105 Ethernet port may fail to receive any packet.

Condition:

1. Connect ZyWALL5's LAN port (using VT6105 Ethernet chip) to an SMC hub and operate it in 100M/HALF mode.
2. Generate heavy traffic to go through the ZyWALL 5's LAN port.
3. After an indefinite period of time, the ZyWALL 5's LAN port may fail to receive any packet. When this hang condition happens, the console will show "enet0 stop NIC Rx never completed!"

29. [BUG FIX]

Symptom: DDNS failed to update when PPPoE redial.

Condition:

**ZyXEL Confidential**

1. Configure the DDNS host and enable it.
2. Configure WAN as PPPoE mode and idle timeout, and connected OK.
3. When the connection is doown, and connected again, IP is change, it failed to update DDNS server.

**Modifications in V3.64(XD.0) | 03/04/2005**

Modify for formal release.

**Modifications in V3.64(XD.0)b4 | 02/23/2005**

1. [BUG FIX]  
Symptom: In PPPoE/PPTP mode, BWM can not classify the traffic of FTP, H323, SIP.
2. [BUG FIX]  
Symptom: Bandwidth Management, Priority based, FTP transfer speed slow down until to disconnect .  
Condition:  
  - (1) Edit web eWC/BW MGMT , WAN/Active=enable, WAN1/Speed (kbps)=1000, Scheduler=Priority-Based
  - (2) Edit web eWC/BW MGMT/Class Setup, Interface=WAN1, Add Sub-Class, Class Name=FTP, Bandwidth Budget=200, Priority=3, Borrow bandwidth from parent class=enable , Enable Bandwidth Filter=enable, Service=FTP, Destination IP Address =192.168.10.0, Destination Subnet Mask=255.255.255.0
  - (3) FTP upload file from LAN to WAN
3. [BUG FIX]  
Symptom: Custom traffic will send over 100 kbps in bridge mode.  
Condition:  
  - (1) In bridge mode, set WAN as 1000 kbps with fairness mode.
  - (2) Create a custom class, budget=50, priority=2, no borrow.
  - (3) Create a ftp class, budget=200, priority=3, no borrow.
  - (4) Use tfggen to generate UDP traffic to match custom class.
  - (5) Use ftp to generate TCP traffic to match ftp class.
  - (6) In GUI statistics page, custom class will be over 100 kbps.
4. [BUG FIX]  
Symptom: VPN XAuth rule swap fail  
Condition:  
DUT1:  
  - (1) Edit web eWC/VPN, add gateway policy, Name=IKE1, Remote Gateway Address=192.168.11.101, Pre-Shared Key=12345678, Enable Extended Authentication=enable, Client Mode/User Name=dut1, Client Mode/Password=dut1
  - (2) Edit web eWC/VPN, add network policy for IKE1, Active=enable, Name=IPSec1, Local Network/Starting IP Address=192.168.1.33, Remote Network/Starting IP Address=192.168.2.33

DUT2:

- (1) Edit web eWC/AUTH SERVER/Local User Database, index1/Active=enable
  - (2) Edit web eWC/VPN, add gateway policy, Name=IKE1, Remote Gateway Address=192.168.12.100, Pre-Shared Key=12345678
  - (3) Edit web eWC/VPN, add gateway policy, Name=IKE2, Remote Gateway Address=0.0.0.0, Pre-Shared Key=12345678, Enable Extended Authentication=enable, Client Mode/User Name=dut1, Client Mode/Password=dut1
  - (4) Edit web eWC/VPN , add gateway policy, Name=IKE3, Remote Gateway Address=0.0.0.0, Pre-Shared Key=12345678, Enable Extended Authentication=enable, Server Mode=enable
  - (5) Edit web eWC/VPN, add network policy for IKE1, Active=enable, Name=IPSec1, Local Network/Starting IP Address=192.168.2.43, Remote Network/Starting IP Address=192.168.1.33
  - (6) Edit web eWC/VPN , add network policy for IKE2, Active=enable, Name=IPSec2, Local Network/Starting IP Address=192.168.2.53
  - (7) Edit web eWC/VPN , add network policy for IKE3, Active=enable, Name=IPSec3, Local Network/Starting IP Address=192.168.2.33
5. [BUG FIX]  
Symptom: In eWC->Wireless, When select WPA or WPA PSK, the Authentication Databases field always says: Local User first then RADIUS.  
Condition: Go to eWC>WLAN>Wireless, when select WPA or WPA PSK, the Authentication Databases field always says: "Local User first then RADIUS". But it shouldn't.
- (1) When selecting "WPA", we should show "Authentication Database = RADIUS" instead of "Authentication Databases Local User first then RADIUS"
  - (2) When selecting "WPA+PSK", "Authentication Databases" should be hidden.

### **Modifications in V3.64(XD.0)b3 | 02/03/2005**

1. [BUG FIX]  
Symptom: OpenPhone H.323 traffic will be blocked by Firewall if connection is initiated from WAN side to LAN side.  
Condition:  
PC1(OpenPhone)------(LAN) ZyWALL (WAN) ----- PC2(OpenPhone)  
192.168.1.33  
(1) Enable Firewall, setup a WAN2LAN firewall rule for H.323 service  
(2) Enable NAT port forwarding for port 1720(H.323) to PC 192.168.1.33  
(3) Enable H.323 ALG by "ip alg enable ALG\_H323"  
(4) PC1 and PC2 use OpenPhone, PC2 call PC1.  
(5) OpenPhone application traffic will be blocked by Firewall, you will see a lot of Firewall blocked log in Centralized LOG.
2. [BUG FIX]  
Symptom: DPD vendor ID is not correct.  
Condition: VID value of DPD is not compatible with RFC3706.

3. [FEATURE CHANGE]

WAS: The second datagram will use the last 8 octets of the first datagram as IV. This may cause IV "predictable".

IS: All datagrams will use random IV to make IV unpredictable.

**Modifications in V3.64(XD.0)b2 | 01/31/2005**

1. [BUG FIX]

Symptom: The name of Domain name does not check properly in SMT 1.

Condition:

(1) In SMT 1->Edit Dynamic DNS->Edit Host, fill the record 1's "domain name" with "xxx.dyndns.org". and record 2's "domain name" with "xxx.dyndns.org ". (the domain name of record 2 contains a space at the end)

(2) The domain should not contain space, we should have a filter to check this.

(3) Set record 1's "Update policy" with "Use WAN IP Addrsss" and record 2's "Update policy" with "Let DDNS Server Auto Detect".

(4) After the DDNS process updating, the domain name "xxx.dyndns.org" will be resolved by the policy "Let DDNS Server Auto Detect" not "Use WAN IP Addrsss". (the first DDNS query result was overwritten by the second executed, "xxx.dyndns.org" is the first, "xxx.dyndns.org " is the second)

2. [ENHANCEMENT] On eWC>BW MGMT>Class Setup, add a popup warning message "Delete Class : class name ?" before user delete a Class.

3. [ENHANCEMENT] Add a active checkbox for ipsec rule on VPN wizard.

4. [BUG FIX]

Symptom: The wording of Dial Backup in SMT is not consistent with GUI.

Condition:

(1) In "eWC->WAN->Dial Backup", one of the wordings in "Budget" is "Always On".

(2) In SMT, the wording is "Nailed-Up Connection".

5. [BUG FIX]

Symptom: While performing "Chariot 128 application 48 hours stress testing", ZyWALL crashed several .

Condition: Chariot Server<-----DUT----->Chariot end point

(1) DUT reset default romfile, and only configured WAN and LAN IP address.

(2) Traffic direction: Server to end point.

(3) Execute Chariot (automation.exe) after load stress file (stress-all.txt)

(4) After a while, DUT crashed

6. [BUG FIX]

Symptom: The traffic redirect should have higher priority than dial backup.

Condition:

(1) In eWC>WAN>Route, set Traffic Redirect priority smaller than Dial Backup, then click Apply.

(2) It can be saved.

7. [BUG FIX]

Symptom: Enter special url will cause device crash.

Condition: Form LAN site, enter

http://192.168.1.1/Forms/rpAuth\_1?ZyXEL%20ZyWALL%20Series<script>top.location.pathname=%20""</script> on browser, the device will crash.

8. [BUG FIX]

Symptom: The CI command "ip nat service irc" may display strange Enable state.

Condition:

(1) Execute "ip nat service irc he\_is\_good".

(2) Execute "ip nat service irc 0".

(3) Execute "ip nat service irc he\_is\_bad".

After Step 3, you will see that a strange Enable state, e.g., "IRC enable = 12".

9. [BUG FIX]

Symptom: The eWC>Firewall>Rule Summary>EDIT RULE page might be corrupted.

Condition:

(1) Go to eWC>Firewall>Rule Summary.

(2) Add or Edit a firewall rule.

(3) Try to delete a Source Address (or Destination Address) without first selecting an address.

(4) Or try to delete a Service without first selecting a service.

(5) With 3 or 4, you will see an error message on the status bar.

(6) Click on any button of this page, and then you will see that the values of some fields on this page are lost. Also you won't be able to escape this page by clicking on the Cancel button.

10. [ENHANCEMENT] Add SIP protocol in service list in firewall rule edit page.

11. [BUG FIX]

Symptom: In SMT 15.1 address mapping rule error message not correct.

Condition:

(1) In SMT 15.1, configure NAT address mapping many to many overloads(or many one to one).

(2) Configure local address from 0.0.0.0 to 255.255.255.255.

(3) Configure global address from 0.0.0.0 to 255.255.255.255.

(4) Save the configuration =>error message show "The end IP address must be great than the start IP address " not correct.

12 [BUG FIX]

Symptom: Configure WAN page, and WAN priority will become 1.

Condition:

(1) In "eWC->WAN->General", set WAN1 priority to 5.

(2) In "eWC->WAN->WAN"., set encapsulation type to PPTP or PPPoE.

(3) Go to "eWC->WAN->General", WAN's priority will become 1.

13 [ENHANCEMENT] Give a warning message when user configure FTP/SIP/H.323 filter on BWM but FTP/SIP/H.323 alg is not enabled.

GUI : Save the filter and show the warning message. Warning: This is a SIP(FTP, H.323) filter, you have to enable SIP(FTP, H.323) ALG by CI command "ip alg enable".

CI command : After running "bm config save", the router will save the configuration and check all filters in all interface. Then show a list of filters which are conflicted.

- 14 [ENHANCEMENT] NAT address mapping need prevent user configure local IP range and global IP range overlap.
- 15 [BUG FIX]  
Symptom: SIP WiFi-Phone's voice communication failed.  
Condition:  
(1) Use following topology to test.  
WiFi A--(L)ZW35(W)----Internet(SIP server)---(W)ZW5(L)----WiFi B  
(2) Both zyxwall reset to default romfile.  
(3) In SMT 24.8 CI command, both type "ip alg enable ALG\_SIP" to enable SIP ALG.  
(4) WiFi A make a phone call to WiFi B, voice communication works fine.  
(5) Terminate the phone call, then WiFi B make a phone call to WiFi A, voice communication fail.  
(6) Fail status: WiFi A can hear voice, but WiFi B can't.
- 16 [BUG FIX]  
Symptom: The device crashes while the user is changing the SNMP access right configuration.  
Condition:  
(1) Restore default romfile.  
(2) Set the SNMP Access = Disable.  
(3) Use MS-SOFT to query the device.  
(4) Before the query timeout, change Access = ALL, the device will crash.
- 17 [BUG FIX]  
Symptom: In authentication server, the local user database should check if the input user name is duplicate.  
Condition:  
(1) Restore to default romfile.  
(2) In record 1, active = yes, name = test, password = 1234 In record 2, active = yes, name = test, password = 5678  
(3) Press Save and this configuration will be accept by router.
- 18 [BUG FIX]  
Symptom: BWM linear search can not find first match filter.  
Condition:  
PC1 ----- (LAN) Router (WAN) ----- PC2  
(1) In router, enable BWM on WAN, setup two classes for WAN Root class:  
1000kbps  
|-----Class 1: 200kbps  
|-----Class 2: 200kbps  
Filters table:  
Class 1: FTP SrcIP = 192.168.1.0/24  
Class 2: FTP DstIP = 192.168.70.0/24  
(2) FTP upload file from PC1 to PC2.  
(3) In this case, BWM will match Class 2's filter. But it's wrong, in linear search algorithm, we should return the first match filter for traffic.
19. [BUG FIX]  
Symptom: When manual mode encapsulation is Tunnel, responder can't build up

tunnel.

Condition:

- (1) PC A – ZW70 ---- ZW5 – PC B
- (2) On eWC/VPN/Manual add two manual rules in ZW70 and ZW5. Rule 1 is inactive. Rule 2 is active and encapsulation is Tunnel.
- (3) PC A ping PC B, check SA Monitor, ZW70 tunnel had been built up but no tunnel is up in ZW5, vice versa.
- (4) If PC B ping PC A this time, tunnel can be built up in both sides and traffic can be transferred.

20. [BUG FIX]

Symptom: LAN static DHCP can save the same data.

Condition:

- (1) Restore default rom file.
- (2) In GUI>LAN>Static DHCP, add two record as MAC: 01:01:01:01:01:01, IP: 192.168.1.33 MAC: 02:02:02:02:02:02, IP: 192.168.1.66 and apply it.
- (3) Change these two record as MAC: 03:03:03:03:03:03, IP: 192.168.1.99 and apply it.
- (4) It can be saved and it is wrong.

21. [BUG FIX]

Symptom: Nail up warning message does not show correctly in eWC->WAN->WAN.

Condition:

- (1) Edit a VPN rule and enable nail up
- (2) In eWC->WAN->WAN, set encapsulation with PPPoE and no nailed-up enabled, click "apply" to save, the status will show "Warning: VPN Nailed-Up may trigger dial WAN links."
- (3) Click "apply" again, the status will show "Nothing changed; no need to perform save"

22. [BUG FIX]

Symptom: VPN tunnel cannot be disconnected.

Condition:

- (1) PC1—ZW5-----HUB-----ZW10W(V362WH7)--PC2
- (2) ZW5 has one IKE and two IPSec rules
- (3) ZW10W has two VPN rules
- (4) ZW10W initiates these two VPN rules
- (5) ZW10W delete these two VPN tunnels but one of ZW5 VPN tunnels can not be disconnected

23. [BUG FIX]

Symptom: When out of call schedule, the device still cannot send traffic out.

Condition:

- (1) Set WAN 1 encapsulation is Ethernet.
- (2) Edit SMT menu 24.10, Time Protocol = Manual, New Time (hh:mm:ss) = 10:00:00, New Date (yyyy-mm-dd) = 2004-06-01.
- (3) Edit SMT menu 26, enter Schedule Set Number to Configure = 1, Edit Name = FD-Once.
  - How often = Once
  - Once Date = 2004-06-01

**ZyXEL Confidential**

- Start Time = 10:05
  - Duration = 00:02
  - Action = Force Down
- (4) Edit SMT menu 11.1, schedule = 1.
- (5) However, when out of schedule about 5 minutes, device still cannot send traffic out.
24. [ENHANCEMENT] Add "Session Table is Full!" log message, when tos session is full.
25. [BUG FIX]  
Symptom: Wireless CI command "wlan active 100" can be save.(The value should be 1 or 0)  
Condition:  
(1) Plug in B120 and reboot router.  
(2) Use "wlan active 100" and it can be save.  
(3) Go to smt3-5, router will crash.
26. [BUG FIX]  
Symptom: The centralized log shows the strange DHCP entry with hex IP address.  
Condition:  
(1) The device enables LAN DHCP server.  
(2) A PC is set on device LAN site with dynamic IP and no system hostname.  
(3) The PC sends DHCP request to device.  
(4) The device will show the strange log message have the hex IP address. (ex: 101 01/15/ 2005 10:15:50 DHCP server assigns 0xa0a01e6 to 00:0E:08:AA:B6:B3)
27. [ENHANCEMENT] When router reset, console will display the reset date and time.  
For example, .\sys\_cmd.c:869 sysreset() ZyWALL 5 system reset at 01/18/2005 15:07:48
28. [BUG FIX]  
Symptom: VPN page cannot be configured.  
Condition:  
(1) Go to eWC>VPN>GATEWAY POLICY>EDIT to add a GATEWAY POLICY rule.  
(2) Go to eWC>VPN>NETWORK POLICY>EDIT to add 10 NETWORK POLICY rules and bind them with the GATEWAY POLICY rule which was added in Step1.  
(3) Delete the GATEWAY POLICY rule which was added in Step1 and 10 NETWORK POLICY rules will be put into the Recycle Bin  
(4) VPN page can't be configured anymore.
29. [BUG FIX]  
Symptom: Enhance the VPN error description  
Condition:  
(1) On eWC VPN, add a IKE rule Dynamic rule (Remote Gateway Address is 0.0.0.0)  
(2) Add an Ipsec rule, and fill some value instead of 0.0.0.0 in "Remote Network" fields.  
(3) Status will show "This policy cannot bound to the dynamic rule"  
(4) User may not know where is wrong.
30. [FEATURE CHANGE] Enhance Gateway Domain Name Update Timer. If Gateway



Domain Name Update Timer is enabled. The ZyWALL will resolve the IP from a VPN gateway policy whose IKE remote gateway is domain name type in every cycle. If the ZyWALL finds that the new remote gateway IP is different from the old one( which is used by tunnel now), the ZyWALL will delete this tunnel.

31. [BUG FIX]

Symptom: Save a legal VPN gateway policy but the ZyWALL shows an error message.

Condition:

- (1) GO to eWC>VPN>GATEWAY POLICY – EDIT
- (2) Save a GATEWAY POLICY whose name = GW, My Address = www.abc.com.tw, Remote Gateway Address = www.cde.com.tw and Pre-Shared Key = 12345678
- (3) GO to eWC>VPN>NETWORK POLICY - EDIT
- (4) Save a NETWORK POLICY whose name = NW, Active = Yes, Starting IP Address = 192.168.1.33, Starting IP Address = 192.168.2.33 and Pre-Shared Key = 12345678
- (5) Go back to eWC>VPN>Rules and edit rule "GW" and set its My Address as 0.0.0.0, then save
- (6) The ZyWALL shows an error message "This IKE rule has static policy rules.", but it should not.

32. [BUG FIX]

Symptom: There are no logs in eWC>Logs>Log Settings when SMTP authentication fail .

Condition:

- (1) Go to eWC>Logs>Log Settings. Configure a wrong Mail Server/Send Log to/Send Alerts to/ User Name of SMTP Authentication/Password of SMTP Authentication and save.
- (2) Go to eWC>Logs>View Log. There are no logs about SMTP Auth failures/SMTP failures.
- (3) If the configuration is correct. There is also no log to tell users that the result is successful.

33. [ENHANCEMENT] Add port information in centralized log message when a netbios packet was blocked.

34. [ENHANCEMENT] After the device rebooting, the system will synchronize Time server until any WAN is up or all WAN links are failed exceed 5 minutes. If NTP server is on LAN/DMZ subnet, DUT still won't sync when WAN interface is down.

35. [BUG FIX]

Symptom: VPN tunnel can be established but traffic cannot go through tunnel.

Condition: PC1 -- ZyWALL -- Any Router/Internet -- ZyWALL -- PC2

- (1) Configure corresponding VPN setting in both ZyWALLs.
- (2) Dial VPN tunnel
- (3) After tunnel established, PC1 cannot ping PC2 vice versa.

36. [BUG FIX]

Symptom: The router cannot flush correctly in eWC->LOGS->Reports.

Condition:

- (1) In Bridge Mode.

- (2) In eWC->LOGS->Reports, enable "Collect Statistics", interface = LAN, Report type= "Host IP Address".
  - (3) When pressing "Flush" button, there is still one record existing "192.168.70.123 Outgoing 3913 bytes". "192.168.70.123" is router's IP address.
  - (4) It has the same problem when changing interface from "LAN" to "DMZ" if we do the same action.
37. [BUG FIX]  
Symptom: In bridge mode, SIP traffic cannot be managed by BWM.  
Condition: SIP Phone1 ----- (LAN)ZyWALL(WAN) ----- SIP Phone2
- (1) Change router to Bridge Mode.
  - (2) Enable BWM, and add a SIP filter at WAN interface.
  - (3) SIP Phone1 call SIP Phone2.
  - (4) After connection is established, go to eWC->BW MGMT->Monitor, you will see SIP traffic falls into Default class, it's wrong.
38. [BUG FIX]  
Symptom: Packet still can send out through NAT router when there is no unused port for it.  
Condition:
- (1) Configure an active port forwarding rule with incoming port range 10000 to 29999.
  - (2) Send a packet out of NAT router.
  - (3) The packet can still send out.
39. [BUG FIX]  
Symptom: BWM highest priority class cannot borrow residual bandwidth from parent class (using tfgen tool)  
Condition:
- (1) In WAN interface. Enable Priority-based Scheduler.
  - (2) Class Setup on WAN.  
Root 100000 Kbps  
|-----WAN 2000 Kbps (No Borrow, No Filter, Priority = 3)  
|-----WAN1-1 500 Kbps (Borrow; Filter: SrcIP:0, DestIP:0, SrcPort:0, DestPort:90; Protocol: 17; Priority = 3 )  
|-----WAN1-2 300 Kbps (Borrow, Filter: SrcIP:0, DestIP: 192.168.70.0/24, SrcPort:0, DestPort:0, Protocol: 17; Priority= 6)
  - (3) From LAN host, use tfgen (UDP packet generator) to generate two session to match class WAN1-1 and WAN1-2.  
session 1: Utilization = 2000Kbps, Destination = WAN host (192.168.70.57), port=90. This will match WAN1-1 class.  
session 2: Utilization = 2000Kbps, Destination = WAN host(192.168.70.57), port = default. This will match WAN1-2 class
  - (4) From Monitor, WAN1-1 should be protected at 500Kbps, and WAN1-2 should borrow remaining bandwidth from parent class.  
But you will see WAN1-1 still borrow remaining bandwidth and WAN1-2 almost borrows nothing from parent class.
40. [BUG FIX]  
Symptom: There is no response from DMZ after set system name by SNMP.

Condition:

- (1) Reset to factory default setting.
- (2) Disable firewall.
- (3) Ping router's DMZ IP address continuity.
- (4) Set DUT's system name by SNMP tool "MG-SOFT MIB browser".
- (5) There is no response from DMZ anymore.

41. [BUG FIX]

Symptom: BM filter cannot be deleted via CI command.

Condition:

- (1) On eWC->BW MGMT->Class Setup, create 3 classes on LAN interface. all classes have filter enabled.
- (2) Go to SMT 24.8, delete the third filter by "bm filter lan del 3" and then save data by "bm config save"
- (3) By typing, "bm show filter", you will see the third filter still exists.

42. [BUG FIX]

Symptom: Device will crash.

Condition: Use IXIA to simulate 1012 ip address to access web site ( every ip has 10 sessions ), device will crash.

43. [BUG FIX]

Symptom: Memory leak in DNS query.

Condition:

- (1) Set the device as the network gateway.
- (2) Some PCs assign the DNS server to the device.
- (3) After some days, the DNS query will cause memory leak.

44. [BUG FIX]

Symptom: Executing CI command "ip nat service irc" will make the router crash.

Condition:

- (1) In SMT 24.8, type "ip nat service irc" then press enter.
- (2) The router crash.

45. [BUG FIX]

Symptom: NAT address mapping functionality fail.

Condition:

- (1) Restore to factory default.
- (2) In SMT4, set "Network Address Translation" as "Full Feature".
- (3) In SMT 15.1.1, insert a rule in rule 1. Take an example with my setting: Type: One to One. Local IP: 192.168.1.33 Global IP: 192.168.70.111 (FTP server in 192.168.70.8)
- (4) In PC/192.168.1.33, ftp to server/192.168.70.8.  
In FTP server, you can find the incoming IP is 192.168.70.111. (This is right)  
Then logout the ftp.
- (5) Repeat step 3 but change the Global IP: 192.168.70.123
- (6) Repeat step 4, you can find the incoming still 192.168.70.111. This is wrong, it should be 192.168.70.123.

46. [FEATURE CHANGE] Extend "devID" field to six hexadecimal numbers(12 characters) in syslog format.

47. [BUG FIX]

**ZyXEL Confidential**

Symptom: Netmeeting H.323 traffic will be blocked by Firewall if connection is initiated from WAN side to LAN side.

Condition:

PC1(Netmeeting)------(LAN) ZyWALL (WAN) ----- PC2(Netmeeting)

- (1) Enable Firewall, setup a WAN2LAN firewall rule for H.323 service
- (2) Enable NAT port forwarding for port 1720(H.323) to PC 192.168.1.33
- (3) PC1 and PC2 use Netmeeting, PC2 call PC1.
- (4) Netmeeting application traffic will be blocked by Firewall, you will see a lot of Firewall blocked log in Centralized LOG.

48. [BUG FIX]

Symptom: After VPN tunnel is established, user will see DPD packet while traffic still can be transferred through tunnel.

Condition:

PC1----- ZyWALL-A ===== ZyWALL-B ----- PC2 IPSec tunnel

- (1) Configure VPN tunnel between ZyWALL-A and ZyWALL-B.
  - (2) In ZyWALL-A eWC->VPN->Global Setting, set Output Idle Timer = 120.
  - (3) Reboot ZyWALL-A.
  - (4) PC1 ping PC2 to trigger tunnel.
  - (5) after tunnel is established, users will see ZyWALL-A's LOG show DPD packets.
49. [ENHANCEMENT] BWM children's bandwidth's sum will not exceed parent's. For example, the bandwidth of WAN interface is 50000 kbps. The sum of all children's bandwidth can not exceed 50000 kbps

**Modifications in V3.64(XD.0)b1 | 12/17/2004**

1. [ENHANCEMENT] Redesign IPSec mechanism to comply with ICSA Labs 1.1D IPSec Certification Testing.  
New feature added :
  - (1) Multiple Proposal.
  - (2) Support Nail Up, Dead Peer Detection, Control Ping.
  - (3) Separate IPSec SA (Phase 2) from IKE SA (Phase 1), multiple IPSec SAs can bind to one the same IKE SA. (Multiple policy)
  - (4) Add a "Global Setting" tab in eWC->VPN which contains some timer settings.
  - (5) IKE and manual key rules have their setting pages respectively in eWC->VPN.
  - (6) Remove the VPN setup page (SMT 27)
  - (7) Redesign lots of IPSec CI command.
2. [ENHANCEMENT] Support Port Restricted Cone NAT.
3. [ENHANCEMENT] Redesign eWC->BW MGMT->Class Setup page.
4. [ENHANCEMENT] Enable "ip alg" command in bridge mode.
5. [ENHANCEMENT] Add the eWC>CONTENT FILTER>Cache and eWC>DNS>Cache GUI.
  - (1) Add total cache entry number info.
  - (2) Remove the "Port" info in URL Cache Entry table.
  - (3) The "Action" in URL Cache Entry table shows "Blocked" first by default.
  - (4) The URL entry in URL Cache Entry table aligns to the left.

- (5) On the URL Cache Entry table, if the length of a URL entry is over 50, it will be truncated to 50 characters, with three trailing dots (...) appended.
- (6) To adjust the note font size in eWC>DNS>Cache GUI.
- 6. [ENHANCEMENT] Popup message improvement: "Delete this rule?" => "Delete entry #[number] ?"
- 7. [ENHANCEMENT] DNS adds CI command "ip dns system cache flush".
- 8. [ENHANCEMENT] eWC>LOGS>Reports>Report Type>"LAN IP Address" renamed as "Host IP Address"
- 9. [ENHANCEMENT] In eWC>DNS>System>Address Record, add Wildcard.
- 10. [ENHANCEMENT] Add length checking of DNS(Peer ID Type) content in VPN.
- 11. [ENHANCEMENT] Integration of TOS & NAT information
  - (1) Current concurrent sessions = max(TOS current concurrent sessions, NAT current concurrent sessions)
  - (2) Historical high since last startup = max(TOS historical high since last startup, NAT historical high since last startup)
- 12. [ENHANCEMENT] Add FQDN support in my IP address in IKE.
- 13. [ENHANCEMENT] IPSec GUI enhancements
  - (1) On eWC>VPN>Global Settings, add IPSec timers configuration.
  - (2) On eWC>VPN>Network Policy Edit page, add Netbios passthrough field.
  - (3) On eWC>VPN>Gateway Policy Edit page, add FQDN field for My ZyWALL.
- 14. [ENHANCEMENT] Enhance ZyWALL GUI.
  - (1) To allow more than two child windows open from multiple ZyWALLs, the second parameter (windowName) of the JavaScript function Window.open() will be the MAC address of the ZyWALL that is currently being managed. The child windows include the following.
    - 1) Wizards
    - 2) Help
    - 3) Show Statistics
    - 4) Show DHCP Table
    - 5) VPN Status
    - 6) BWM statistics
  - (2) For identification purpose, the title of the eWC parent window, as well as its child windows, will contain the system FQDN of the ZyWALL that is currently being managed.
- 15. [ENHANCEMENT]
  - (1) In eWC>Home>System Time, add GMT timezone + DST offset.
  - (2) In eWC>Date&Time>Current Time, GMT add timezone + DST offset.
- 16. [ENHANCEMENT] Add GUI for LAN DHCP Relay feature.
- 17. [ENHANCEMENT] Auth Server/Local User Database needs long time to save all entries, enhance the saving policy to speed up this action.
- 18. [ENHANCEMENT] In SMT 24.6, the menu adds the reminding message "You can enter ctrl-x to terminate operation any time."
- 19. [ENHANCEMENT] Add a API function to move rules for NAT address mapping table. CI command: ip nat acl move <set#> <rule# from> <rule# to>
- 20. [ENHANCEMENT] For Manual IPSec rule, the "My ZyWALL" and "Remote Gateway Address" should not have FQDN fields. (Remove My Domain Name and

change Secure Gateway Address into IP field)

21. [ENHANCEMENT]
  - (1) In eWC>MAINTENANCE>General, change the type of the "Administrator Inactivity Timer" field from ASCII to integer.
  - (2) Add a JavaScript Global function to avoid filling any character in the specific fields on both IE and Netscape. (allow number only)
22. [ENHANCEMENT] Add a "Log" check box for "VPN connectivity check". in eWC>VPN>NETWORK POLICY>EDIT.
23. [FEATURE CHANGE] Modify CI command "ip arp add" from hidden to visible.
24. [ENHANCEMENT] For single WAN, the WAN cannot receive an IP from DHCP server with the same subnet with other interfaces.
25. [ENHANCEMENT] The new DST feature allows user to know the start/end date. It will be nice if the ZyWALL shows what date '1st Sun in April' is ----. And there is some spare space on the screen on that line.
26. [ENHANCEMENT] User can use telnet/ping/ via VPN in SMT menu 24.8.
  - (1) If you telnet/ping/... from your ZyWALL to an IP on the VPN "remote network" and the ZyWALL's LAN IP (including alias IP) is on the VPN "local network", the ZyWALL uses LAN IP as source.
  - (2) If you telnet/ping/... from your ZyWALL to an IP on the VPN "remote network" and the ZyWALL's DMZ IP (including alias IP) is on the VPN "local network", the ZyWALL uses DMZ IP as source.
  - (3) (For future wireless enhancement) If you telnet/ping/... from your ZyWALL to an IP on the VPN "remote network" and the ZyWALL's WLAN IP (including alias IP) is on the VPN "local network", the ZyWALL uses WLAN IP as source.
  - (4) Otherwise the ZyWALL uses any appropriate interface IP as source depending on the routing table.

Note: If there are more than one appropriate local interfaces, router will use the first matched local interface IP address as the source IP address.
27. [ENHANCEMENT] In GUI>NAT>Port Forwarding, router will now check if the translated end port is out of 65535.
28. [ENHANCEMENT] On eWC>HOME>VPN wizard, My ZyWALL address support Domain name.
29. [ENHANCEMENT]
  - (1) In eWC>MAINTENANCE>F/W Upload, the warning message title should be red in order to be consistent with the style of other warning message.
  - (2) In eWC>MAINTENANCE>Restore Configuration, the warning message title should be red in order to be consistent with the style of other warning message.
30. [ENHANCEMENT] On eWC>NAT>AddressMapping, add dynamic display for "Go To Page". If there are less than 10 address mapping rules, then hide "Go To Page", else display "Go To Page".
31. [ENHANCEMENT] When we receive a non-encrypt initial content payload in IKE, we will ignore it.
32. [ENHANCEMENT] Add payload information in IKE LOG. Besides reason, we also show which payload caused the IKE LOG.
33. [ENHANCEMENT] HOME>Internet Access, the "First DNS Server", "Second DNS Server" is inconsistent with DNS>Name Server Record.

### **ZyXEL Confidential**

The specified "First DNS Server", "Second DNS Server" will be updated in eWC>DNS>Name Server Record.

34. [ENHANCEMENT] In GUI>WAN, add "Authentication Type" field.
35. [ENHANCEMENT] For DHCP server, if the requested client does not have a host name, the log will show MAC address instead of nothing.
36. [ENHANCEMENT]
  - (1) In eWC>CONTENT FILTER>Cache, if users click Action/URL/Remaining Time to sort the cache entries, the page will not jump to the top of this page before it refreshes.
  - (2) By using Firefox/Netscape in eWC>CONTENT FILTER>Cache, if users click Action/URL/Remaining Time to sort the cache entries, the page will refresh immediately.
37. [ENHANCEMENT] In the past, we can delete a tunnel in SMT 27 and can only do this in eWC. Now, Add a CI command "ipsec drop <policy index>" to delete a tunnel and "ipsec show\_runtime list" to list the active VPN tunnel.
38. [ENHANCEMENT] Consolidate "Receive IPSec packet, but no corresponding tunnel exists" logs.

### **Modifications in V3.62(XD.2) | 09/24/2004**

Modify for formal release.

### **Modifications in V3.62(XD.2)b3 | 09/21/2004**

1. [BUG FIX]

Symptom: LAN host will get wrong DNS server.

Condition:

  1. Set SMT 3.2 DNS first DNS server as user defined 1.1.1.1. Others are none.
  2. Unplug WAN port and reboot.
  3. LAN host get IP address and DNS server and the DNS server is LAN IP.

### **Modifications in V3.62(XD.2)b2 | 09/17/2004**

1. [BUG FIX]

Symptom: LAN host ping device LAN IP a period time, then PPPoE/PPTP will be triggered dial.

Condition:

  1. Set WAN 1 are PPPoE.
  2. LAN host ping device LAN IP a period time, then WAN 1 will be triggered dial.
2. [BUG FIX]

Symptom: Firewall sends TCP RST after it blocks traffic period of time.

Condition:

  1. Configure Firewall LAN to WAN blocked and enable log
  2. Generate one TCP SYN packet from LAN to WAN
  3. Firewall will block this packet and generate block log

4. After period of time (30 seconds), Firewall log shows it sent TCP RST to both client and server side
3. [BUG FIX]  
Symptom: System has a lot of long timeout UDP sessions.  
Condition:
  1. Enable firewall.
  2. Display TOS sessions.
  3. A lot of long timeout UDP sessions.
4. [BUG FIX]  
Symptom: ZyWALL crashes very often in bridge mode.  
Condition:
  1. Switch to bridge mode.
  2. Enable Firewall.
  3. ZyWALL crashes very often.
5. [ENHANCEMENT] Enhance "cnm keepalive" ci command. Add "cnm keepalive 0" command to stop sending of keepalive packet to Vantage.
6. [BUG FIX] Symptom: Symptom: FTP from WAN to LAN does not work.  
Condition:
  1. Set a FTP server on a host in the LAN side and configure a default server to this host.
  2. Using FTP from WAN to the default server with port mode.
  3. After typing username and password, "ls" command does not work.
7. [BUG FIX] Symptom: LAN host will get wrong DNS server.  
Condition:
  1. Set SMT 3.2 DNS first DNS server as user defined 1.1.1.1. Others are none.
  2. Unplug WAN port and reboot.
  3. LAN host get IP address and DNS server and the DNS server is LAN IP.
8. [BUG FIX] Symptom: System Crash when change encryption key in Vantage.  
Condition:
  1. Device register to Vantage in router mode under DES and PPPoE.
  2. configuration>>general>>system change the original encryption key and apply
  3. Device receives data but soon the system crash.
9. [BUG FIX] Symptom: WAN Gateway will be reset to 0.0.0.0.  
Condition:
  1. In Vantage CNM add a device (the device have a static IP),when it register to Vantage. Vantage set default value to device.
  2. After the device reset, WAN Gateway will be reset to 0.0.0.0.
10. [BUG FIX] Symptom: CNM agent accepts wrong CI command "cnm keepalive -323123122222222222222222".  
Condition:
  1. In SMT 24.8, type "cnm keep -323123122222222222222222".
  2. The system accepts it and saves with the value.
11. [BUG FIX] Symptom: CNM agent accepts wrong CI command "cnm encrymode 1231223".  
Condition:
  1. In SMT 24.8, type "cnm encrymode 1231223".



2. The system accepts it and read it as "65535".
12. [BUG FIX] Symptom: [Vantage] Configuration>>VPN: When delete a active VPN tunnel successfully. Device sends VPN tunnel status "Destroy" to vantage.  
Condition:
  1. Create and dial up a VPN tunnel via Vantage.
  2. Delete this active rule in Vantage.
  3. Vantage server will have exception.
13. [BUG FIX]  
Symptom: eWC will fill the "Connection ID/Name" field with "C:1" when the fetch data is empty.  
Condition:
  1. In eWC, set "Connection ID/Name" as empty in PPTP mode and apply it.
  2. Go go another page and go back the WAN page, the "Connection ID/Name" field is filled with "C:1" even we set the field as empty.

**Modifications in V3.62(XD.2)b1 | 08/16/2004**

1. [ENHANCEMENT]  
Add Unified ALG for SIP and H.323.
2. [ENHANCEMENT]  
Each unified ALG can be enabled/disabled. The default ALG setting for SIP and H.323 is disabled.
3. [ENHANCEMENT]  
Firewall can bypass AX.25 (protocol #93) & IPv6 (protocol #41) protocols.
4. [BUG FIX]  
Symptom: Bandwidth management with ALG\_H.323 cause system crash.  
Condition:
  1. Create a class with a Service-H.323 filter in WAN1 interface.
  2. Unplug all WAN's cable
  3. Launch the "Openphone" application that supports H.323 and make a call.
  4. Router crashes.
5. [BUG FIX]  
Symptom: Router block trusted web content.  
Condition:
  - 1). In "eWC->CONTENT FILTER->General", enable content filter.
  - 2). In "eWC->CONTENT FILTER->Customization", select check boxes of "Enable Web site customization" and "Disable all Web traffic except for trusted Web sites".
  - 3). In "eWC->CONTENT FILTER->Customization", set "www.hellowork.go.jp" as trusted web site.
  - 4). Open browser and access  
<http://www.hellowork.go.jp/kensaku/servlet/kensaku?pageid=001>
  - 5). In the new page, select third and fourth radio button and click "search" button.
  - 6). In the new page, click "next page" button.
  - 7). The new page will be blocked.
6. [BUG FIX]  
Symptom: External Content Filtering cannot block the URL belonging to restricted

category.

Condition:

- 1). In "eWC->CONTENT FILTER->Customization", unselect "Enable Web site customization".
- 2). Add a URL to "trusted web sites".
- 3). In "eWC->CONTENT FILTER-Customization", select "Block Web sites which contain these keywords".
- 4). In "eWC->CONTENT FILTER->Categories", select the category which the URL belongs to.
- 5). Access the trusted URL.
- 6). The URL will not be blocked.

7. [BUG FIX]

Symptom: System crash by memory leak.

Condition:

- 1). Enable bandwidth management.
- 2). Into eWC->Bandwidth Management->Monitor and wait for a period time.
- 3). System crash by memory leak.

8. [BUG FIX]

Symptom: Remote node CI command crashes.

Condition:

- 1). Goto SMT 24.8
- 2). Load dial backup remote node to working buffer.
- 3). Type CI command "sys rn accessblock 0".
- 4). Save this remote.
- 5). System crashes.

9. [BUG FIX]

Symptom: System crash when someone want to configure NAT mapping rules.

Condition:

1. Use the terminal program to login the console.
2. Enter SMT 15, NAT Setup
3. Select 1 to enter SMT 15.1, Address Mapping Sets.
4. The system crash

10. [BUG FIX]

Symptom: eWC>NAT>ADDRESS MAPPING edit page leaks memory.

Condition:

1. Log on to eWC.
2. Go to eWC>NAT>ADDRESS MAPPING edit page, and then click Cancel.
3. Repeat Step 2 for several times.
4. Check system memory info by the CI command: system memu ms You will observe abnormal increases of memory sections, indicating memory leaks.

11. [BUG FIX]

Symptom: Trigger port will disappear after system reboot.

Condition:

1. Configure Trigger port rule.
2. System reboot.
3. The configured Trigger port rule disappear.

12. [BUG FIX]

Symptom: The system might crash when enabling IPSec.

- Condition: During IKE negotiation the system might crash.
13. [BUG FIX]  
Symptom: MSN Messenger's "Ask for Remote Assistance" function causes system crash.  
Condition:  
1. Enable UPnP.  
2. Set PC(A) and router(B) in intranet and PC(C) connects to LAN port of router(B).  
3. Test MSN Messenger's "Ask for Remote Assistance" function from PC(A) to PC(C).  
4. After PC(C) accepts the PC(A) request by "Ask for Remote Assistance" then the device will crash.
14. [BUG FIX]  
Symptom: System out of memory.  
Condition:  
1. Let the ZyWALL be a DNS proxy for LAN hosts.  
2. Do a lot of DNS inverse queries by running IPScan tool continuously from LAN host.  
3. After a long time, the ZyWALL will out of memory.
15. [FEATURE CHANGE]  
Change UPnP device name for ZyWALL35 and ZyWALL5  
WAS: "ZyXEL ZyWALL 35 Internet Security Gateway"  
IS: "ZyXEL ZyWALL 35 Internet Security Appliance"
16. [BUG FIX]  
Symptom: Packets cannot pass through NAT router to LAN hosts.  
Condition:  
1. NAT default server is on  
2. Protocol of the packet is not TCP, UDP, ICMP, ESP, GRE.  
3. Packets from WAN to router.  
4. Packets cannot pass through NAT router to LAN hosts (NAT default server)
17. Symptom: External Content filtering cannot register.  
Condition:  
1. In "eWC->content filter->categories", click "register" to connect to ZSSW.  
2. Do the registration on ZSSW.  
3. The registration will fail in the final step.
18. [ENHANCEMENT]  
External content filtering support full URL checking.  
Was: External content filtering only take domain name or IP address of URL into category checking.  
Is: External content filtering put entire URL into category checking.
19. [ENHANCEMENT]  
CLI command to turn off triangle route log, multicast log and broadcast log.  
1. Add CLI commands:  
a. "sys logs switch".  
b. "sys logs switch display".  
c. Triangle route log switch: "sys logs switch bmlog <0:no|1:yes>"  
d. Broadcast/Multicast log switch: "sys logs switch trilog <0:no|1:yes>"
20. [BUG FIX]  
Symptom: System time problem.  
Condition:  
1. enter SMT24.10, configure time server.  
2. open daylight saving, configure the start time and end time so that current time is

within the daylight saving time.

3. after writing to rom file, router ask you to calibrate the system clock, answer yes.

4. If system failed to connect time server, system time will add one hour, every time you enter smt 24.1,system time add 1 hour automatically.

21. [FEATURE CHANGE]

Change external content filtering message on centralized log and blocked page for some error events.

22. [BUG FIX]

Symptom: Router will crash.

Condition: When user continuously accesses eWC and press "Apply" button, sometimes router will crash.

23. [BUG FIX]

Symptom: The system crashes after it receives a url that contains more than three "/"s behind the ip address (or domain name).

24. [BUG FIX]

Symptom: Sometimes when connect to router by TCP, FTP or HTTP will fail.

Condition:

1. One user connects to router by FTP, TELNET or HTTP.

2. In TCP handshake, client doesn't receive SYN ACK. i.e., router is in SYN RECEIVE state.

3. Client timeout and send RESET to router.

4. Related socket in router is still alive and other users can't login router until this socket timeout.

25. [BUG FIX]

Symptom: eWC spelling error: eWC->Firewall→Default Rule: Allow Asymmetrical should be "Asymmetric"

26. [BUG FIX]

Symptom: System out of memory and reboot when firewall enable.

Condition:

1. Enable firewall, then generate traffic.

2. The memory will slowly leak until it uses up all the memory, then reboot.

27. [BUG FIX]

Symptom: Generate a lot of TCP port 80 sessions to ZyWALL will cause device to hang and reboot by hardware watchdog.

Condition:

1. Use session.exe to generate a lot of TCP port 80 sessions to ZyWALL's LAN or WAN interface

2. After several hundreds of sessions are established, the ZyWALL will hang and finally reboot.

28. [ENHANCEMENT]

1. Support user config for SIP session timeout value.

2. Support SIP SDP multiple RTP port.

3. Delete unused ALG type.

4. Command for ALG enable/disable and sip timeout.

29. [BUG FIX]

Symptom: Sometimes the ZyWALL reboots by software watchdog.

Condition:

1.Put the ZyWALL on the network for a long time.

2.Sometimes the ZyWALL will reboot by software watchdog.

30. [BUG FIX]

**ZyXEL Confidential**

Symptom: XAUTH with rule swap doesn't work.

Condition:

1. In initiator, set up a VPN rule with XAUTH in client mode.
2. In responder, there are three VPN rules:
  - a. Rule 1 is XAUTH off.
  - b. Rule 2 is XAUTH with client mode.
  - c. Rule 3 is XAUTH with server mode (this rule corresponds to client rule).
3. Dial from initiator, and the tunnel will never be up.

31. [BUG FIX]

Symptom: Content filter timeout problem.

Condition:

1. A router is register the content filter (CF) server.
2. Enable the CF feature.
3. Enable the external database content filtering.
4. The router log often record "Waiting content filter server (server name) timeout!".
5. A PC in lan fetch web from internet often hang for a while.

**Modifications in V3.62(XD.1) | 06/25/2004**

1. Formal release.

**Modifications in V3.62(XD.1)b1 | 06/16/2004**

1. [ENHANCEMENT] Support Vantage CNM 2.0 (Vantage Centralized Network Management).

**Modifications in V3.62(XD.0) | 05/18/2004**

1. Formal release.

**Modifications in V3.62(XD.0)b5 | 05/14/2004**

1. [BUG FIX] Symptom: The ZyWALL might crash or hang when users browse eWC→Firewall→Rule Summary.

Condition:

- (1) Log on to eWC.
- (2) Browse Ewc→Firewall→Rule Summary
- (3) The ZyWALL might crash or hang.

**Modifications in V3.62(XD.0)b4 | 04/27/2004**

1. [FEATURE CHANGE]  
Remove Policy Route feature from ZyWALL 5 because Policy Route is not defined in

- product specification.
2. [FEATURE CHANGE]  
Maximum concurrent VPN tunnel number is changed from 5 to 10.
3. [FEATURE CHANGE]  
The following default settings is changed:  
(1) eWC→Firewall→Anti-Probing  
WAS: Anti-Probing Respond Ping to LAN  
IS: Anti-Probing Response Ping to LAN&WAN&DMZ  
(2) eWC→Firewall→Threshold  
WAS: TCP Maximum Incomplete Sessions = 10  
IS: TCP Maximum Incomplete Sessions = 30  
(3) eWC→WAN→Route  
WAS: WAN Priority = 2  
IS: WAN Priority = 1
4. [BUG FIX]  
Symptom: External Content Filtering cannot be registered.  
Condition:  
(1) In eWC→CONTENT FILTER→Categories", click "register" to connect to ZSSW.  
(2) Do the registration on ZSSW.  
(3) Browser display "Please wait....." and the page of "Register successfully" does not appear.
5. [BUG FIX]  
Symptom: Traffic Redirect does not work.  
Condition:

Internet ----- Router A ----- ZyWALL ----- gateway B ----- Internet  
WAN LAN

- (1) Let ZyWALL WAN port connect to another router A and A is connected to Internet.
  - (2) Setup Traffic Redirect to backup gateway B located at LAN side.
  - (3) Disconnect the connection between router A and Internet.
  - (4) The ZyWALL can not do Traffic Redirect to gateway B located at LAN side.
6. [BUG FIX]  
CI command “ip igmp” is lost.
7. [BUG FIX]  
Symptom: The behavior in priority-based Bandwidth Management is not correct.  
Condition:
- (1) In eWC→BW MGMT→Summary, activates WAN1 root class with Speed = 1500 kbps and Scheduler = Priority-Based
  - (2) In eWC→BW MGMT→Class Setup, Adds two sub-classes under WAN1 root class. Where WAN1-1 : Bandwidth Budget = 200, Priority = 7(higher than WAN1-2), and “Borrow bandwidth from parent class” is selected; WAN1-2 : Bandwidth Budget = 500, Priority = 1, “Borrow bandwidth from parent class” is also selected.
  - (3) First generates traffic that satisfies WAN1-2 class, users will find WAN1-2 borrow the whole available bandwidth from parent, and the traffic is bound at about 1500kbps.
  - (4) Then generates traffic that satisfies WAN1-1 class. Users will find WAN1-1 can not borrow bandwidth from parent class and bandwidth is bound at about 200kbps even

though WAN1-1 has higher priority than WAN1-2.

8. [BUG FIX]

Symptom: In eWC→MAINTENANCE→General, set a number which is bigger than 1000 for Administrator Inactivity Timer. The label string 'Administrator Inactivity Timer' will disappear.

Condition:

(1) Go to eWC→MAINTENANCE→General, set a number which is bigger than 1000 for Administrator Inactivity Timer.

(2) Click 'Apply'.

(3) The label string 'Administrator Inactivity Timer' will disappear.

9. [BUG FIX]

Symptom: ZyWALL ping sometimes fails.

Condition:

(1) Turn on Firewall.

(2) Go to SMT 24.8

(3) Ping to exist host, but it sometimes fails.

10. [BUG FIX]

Symptom: In SMT 3.2, the subnet of ZyWALL LAN IP can be different from the subnet of DHCP client ip and ZyWALL LAN IP can be set within DHCP Client IP pool range.

Condition:

First case:

(1) Go to SMT 3.2

(2) Set DHCP client IP Starting address to be 192.168.2.3

(3) Set LAN IP Address to be 192.168.1.1, then confirm to save.

(4) These setting can be saved and no error message.

Second case:

(1) In SMT 3.2, set DHCP client ip Starting address to be 192.168.1.3

(2) Set Size of Client IP Pool to be 10

(3) Set LAN IP Address to be 192.168.1.3, then confirm to save.

(4) These setting can be saved and no error message.

11. [BUG FIX]

Symptom: Remote access control cannot work properly.

Condition:

(1) Turn on bridge mode

(2) Configure telnet server access control from WAN only by SMT 24.11

(3) Telnet to device via WAN side

(4) The telnet connection fails.

12. [BUG FIX]

Symptom: System crashes.

Condition: Configure device by eWC sometimes cause crash.

13. [BUG FIX]

Symptom: In bridge mode ZyWALL at eWC→Bridge, Bridge IP address settings can not be saved successfully.

Condition:

(1) Switch the ZyWALL to bridge mode.

- (2) Go to eWC→Bridge page.
  - (3) Change "IP Address", "IP Subnet Mask", or "Gateway IP Address" then click "Apply"
  - (4) Status shows "Configuration updated successfully" but the changes was not really saved.
14. [BUG FIX]  
Symptom: In SMT 24.11, the setting of DNS Service is displayed under bridge mode  
Condition:  
(1) Go to SMT 1, change Device Mode to bridge mode.  
(2) After reboot, go to SMT 24.11, DNS Service incorrectly appear.

**Modifications in V3.62(XD.0)b3 | 04/04/2004**

1. [BUG FIX]  
Symptom: CI command error, ZyWALL will show some CI commands which don't belong to current command set.  
Condition:  
(1) Go to SMT 24.8, CI command mode.  
(2) Type "ip dns system", ZyWALL will correctly print two available commands, "edit" and "display".  
(3) Type "ip dns sys", ZyWALL will unexpectedly print nine available commands instead of two. Those extra seven commands are not under "ip dns system".
2. [BUG FIX]  
Symptom: DHCP client cannot get address from router.  
Condition:  
(1) In eWC→LAN→LAN, configure router as a DHCP server and set IP pool starting address as 192.168.1.33.  
(2) In eWC→LAN→Static DHCP, configure all rules in static DHCP table and the IP addresses are 192.168.1.33~192.168.1.40.  
(3) Use a PC which MAC address is not in the static DHCP table to get a IP address from router.  
(4) The PC cannot get the IP address.
3. [BUG FIX]  
Symptom: The ZyWALL will reset the current eWC HTTP session even when the LAN IP configuration is not successfully changed. Under this situation, users have to re-log in the ZyWALL.  
Condition:  
(1) Log in ZyWALL eWC, and go to eWC→LAN.  
(2) Deliberately configure the LAN IP address as within the WAN subnet.  
(3) Click Apply, then the status will show an error message indicating address conflict.  
(4) The ZyWALL will then automatically break the current eWC HTTP session. To access the ZyWALL, users have to log in again.
4. [BUG FIX]  
Symptom: Router will crash when entering SMT menu 3.5  
Condition:



- (1) Insert WLAN card.
- (2) In CI command, enter "wlan active 11" instead of "wlan active 1" to activate WLAN on router.
- (3) Enter SMT 3.5, router will crash.
5. [ENHANCEMENT]  
Supports Vantage CNM 2.0(Vantage Centralized Network Management)
6. [BUG FIX]  
Symptom: The Content Filtering blocks cookies even if it is not in the blocked schedule.  
Condition:
  - (1) In eWC→CONTENT FILTER→General, select "Block Cookies".
  - (2) In eWC→CONTENT FILTER→General, set "Schedule to Block" with a time period NOT including the current time.
  - (3) Access a web site which contains cookies.
  - (4) The cookies will be blocked by the Content Filtering.
7. [BUG FIX]  
Symptom: WAN status in SMT 24.1 shows wrong information in bridge mode.  
Condition:
  - (1) Configure Internet access as PPTP or PPPoE encapsulation in router mode.
  - (2) Switch ZyWALL to bridge mode.
  - (3) WAN status in SMT 24.1 shows idle and IP address is "0.0.0.0".
8. [BUG FIX]  
Symptom: Device cannot transfer Ethernet frame in bridge mode.  
Condition:
  - (1) ZyWALL enables bridge mode.
  - (2) The Internet connection is under DMZ port.
  - (3) Plug Ethernet cable between one host and ZyWALL DMZ port.
  - (4) This host starts to transfer packets to Internet.
  - (5) Unplug the Ethernet cable from DMZ port and plug in LAN port.
  - (6) This host cannot transfer packets to Internet anymore.
9. [BUG FIX]  
Symptom: PPPoE connection sometimes fails in France.  
Condition: Since France Telecom changes their core network setup to BRAS, ZyWALL PPPoE connection on authentication phase most of the time fails.
10. [ENHANCEMENT]  
Updates help pages for ZyWALL 5.
11. [BUG FIX]  
Symptom: On the eWC→WIZARD→Internet Access page, the System DNS Servers configuration is not available when the ZyWALL is not a DHCP server for its LAN hosts.  
Condition:
  - (1) Log onto eWC, and go to eWC→LAN. Uncheck the "DHCP Server" option to stop ZyWALL from being a DHCP server to its LAN hosts.
  - (2) Go to eWC→HOME→WIZARD→Internet Access. The System DNS Servers configuration is not available in the wizard.
12. [ENHANCEMENT]  
The ZyWALL 5 Firewall GUI are enhanced as follows.

## **ZyXEL Confidential**

- (1) On eWC→Firewall→Rule Summary→Edit Rule, a basic sanity check on the firewall rule is performed.
- (2) On eWC→Firewall→Rule Summary→Edit Rule, the selected service for a new rule is empty by default.
- (3) On eWC→Firewall→Rule Summary→Edit Rule, the useless headers "##### Source IP Address #####" and "##### Destination IP Address #####" are removed.
- (4) On eWC→Firewall→Rule Summary→Edit Rule, when a specific address is added to the Source/Destination Address list, the "Any" address will automatically be deleted.
- (5) On eWC→Firewall→Rule Summary→Edit Rule, the firewall action radio buttons are replaced by a dropdown list.
- (6) On eWC→Firewall→Threshold, the "Cancel" button is replaced by "Reset" button.
- (7) On eWC→Firewall→Default Rule, the wording "Default Rule Settings" is replaced by "Default Rule Setup".
- (8) On eWC→Firewall→Anti-Probing, the wording "Anti-Probing Settings" is replaced by "Anti-Probing Setup".
- (9) "ACCESS POLICY" is renamed as "FIREWALL".
- (10) "CUSTOM PORT" is renamed as "CUSTOM SERVICE".
- (11) Users can expand or collapse "Source Address", "Destination Address" and "Service Type" drop down lists by clicking the [+]/[-] icon at the beginning of each rule in Firewall Rule Summary Table.

### **Modifications in V3.62(XD.0)b2 | 03/26/2004**

1. [BUG FIX]  
Symptom: In eWC→FIREWALL→ACCESS POLICY→EDIT RULE, Action for Matched Packets can't be saved correctly.  
Condition:
  - (1) Go to eWC→FIREWALL→ACCESS POLICY→EDIT RULE
  - (2) Choose the type of Action for Matched Packets as Block, and then click Apply.
  - (3) Leave this page and then re-enter this page again, Action for Matched Packets always shows Forward.
2. [ENHANCEMENT]  
Supports Intel TE28F640 J3C120 Flash ROM.

### **Modifications in V3.62(XD.0)b1 | 03/11/2004**

First Release.

**ZyXEL Confidential**

## **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.

### **Note**

- (1) DNS Service is not available in Bridge Mode.

#### **Menu 24.11 - Remote Management Control**

```
TELNET Server:  Port = 23      Access = ALL
                  Secure Client IP = 0.0.0.0
FTP Server:     Port = 21      Access = ALL
                  Secure Client IP = 0.0.0.0
SSH Server:     Certificate = auto_generated_self_signed_cert
                  Port = 22     Access = ALL
                  Secure Client IP = 0.0.0.0
HTTPS Server:   Certificate = auto_generated_self_signed_cert
                  Authenticate Client Certificates = No
                  Port = 443    Access = ALL
                  Secure Client IP = 0.0.0.0
HTTP Server:    Port = 80      Access = ALL
                  Secure Client IP = 0.0.0.0
SNMP Service:   Port = 161     Access = ALL
                  Secure Client IP = 0.0.0.0
DNS Service:    Port = 53      Access = ALL
                  Secure 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.

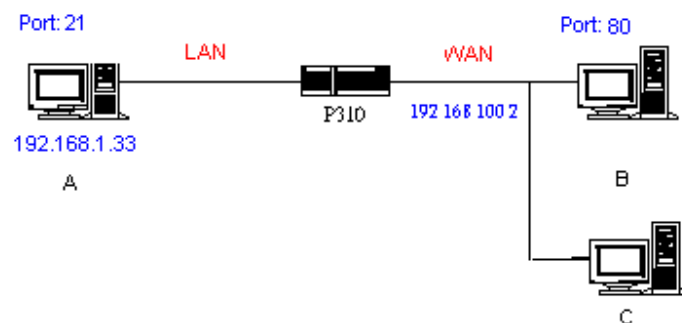
These triggered events can be timed so that they erase the port mapping as soon as they are done with the data transfer, so that the port mapping can be triggered by another Client computer. This gives the *illusion* that multiple computers can use the same port mapping at the same time, but the computers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

### How to use it

Following table is a configuration table.

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

### 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.

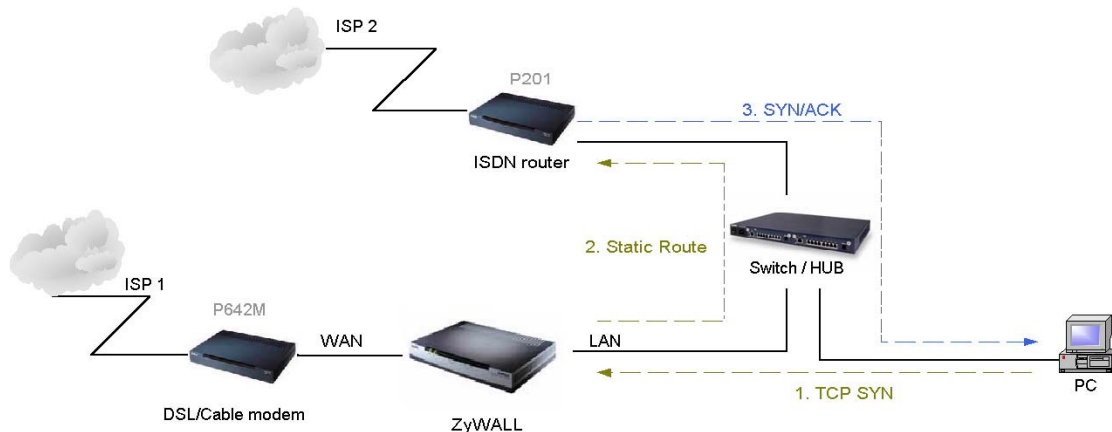


Figure 4-1 Triangle Route

Figure 4-1 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.



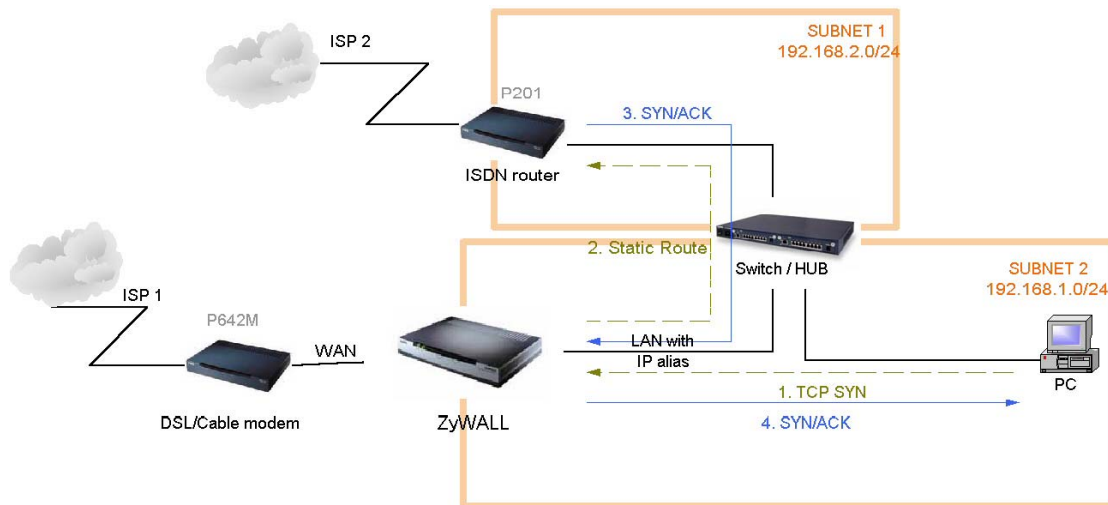


Figure 4-2 Gateway on alias IP network

## (2) Gateway on WAN side

A working topology is suggested as below.

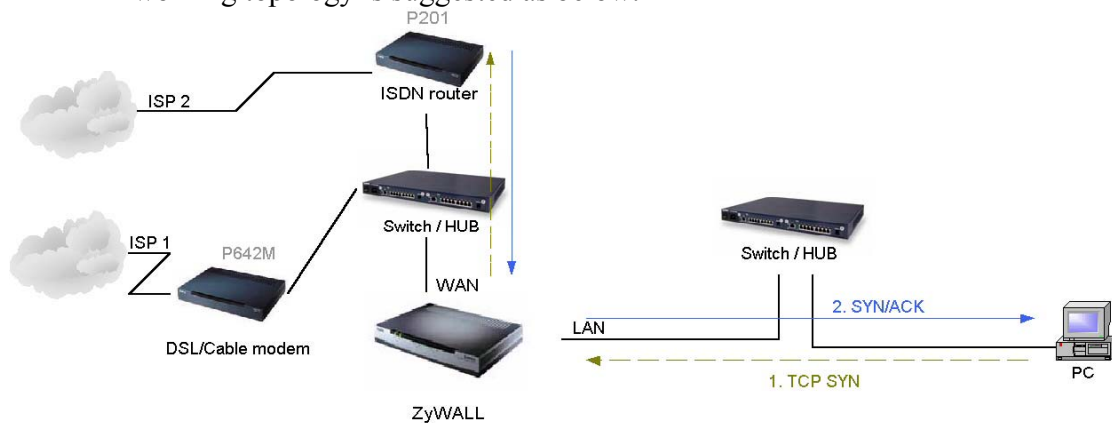


Figure 5-3 Gateway on WAN side

## 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                      | My WAN IP         | My WAN IP                                |
| 0.0.0.0               | a.b.c.d (it can be 0.0.0.0) | My WAN IP         | a.b.c.d ( 0.0.0.0, if user specified it) |
| a.b.c.d (not 0.0.0.0) | *blank                      | a.b.c.d           | a.b.c.d                                  |
| a.b.c.d (not 0.0.0.0) | e.f.g.h (or 0.0.0.0)        | a.b.c.d           | e.f.g.h (or 0.0.0.0)                     |

\*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           | 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         | System checks both type and content   |
| a.b.c.d             | blank           | 1. System will check the ID type and the content.<br>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.<br>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 which means user doesn't type anything here, 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, 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, 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 a such 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 Embedded HTTPS proxy server**

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a Web protocol developed by Netscape and built into its browser that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering.

The ZyWALL's embedded HTTPS proxy server is basically an SSL server which performs SSL transactions, on behalf of the embedded HTTP server, with an SSL client such as MSIE or Netscape. As depicted by the figure below, when receiving a secure HTTPS request from an SSL-aware Web browser, the HTTPS proxy server converts it into a non-secure HTTP request and sends it to the HTTP server. On the other hand, when receiving a non-secure HTTP response from the HTTP server, the HTTPS proxy server converts it into a secure HTTPS response and sends it to the SSL-aware Web browser.

By default, the HTTPS proxy server listens on port 443 instead of the HTTP default port 80. If the ZyWALL's HTTPS proxy server port is changed to a different number, say 8443, then the URL for accessing the ZyWALL's Web user interface should be changed to <https://hostname:8443/> accordingly.

**Annex A CI Command List**

Last Updated: 2004/04/27

| <b>Command Class List Table</b>          |  |  |
|--|--|--|
| <a href="#">System Related Command</a>   | <a href="#">Exit Command</a>                         | <a href="#">Device Related Command</a> |
| <a href="#">Ethernet Related Command</a> | <a href="#">POE Related Command</a>                  | <a href="#">PPTP Related Command</a>   |
| <a href="#">AUX Related Command</a>      | <a href="#">Configuration Related Command</a>        | <a href="#">IP Related Command</a>     |
| <a href="#">IPSec Related Command</a>    | <a href="#">Bridge Related Command</a>               | <a href="#">Bandwidth Management</a>   |
| <a href="#">Firewall Related Command</a> | <a href="#">Certificate Management (PKI) Command</a> |  |

Flag :

R: This command can be used in Router Mode

B: This command can be used in Bridge Mode

**System Related Command**[Home](#)

| 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 |  |

**ZyXEL Confidential**

|  |  |             |  |       |   |
|--|--|-------------|--|-------|---|
|  |  |             | access<br>[0:none/1:log/2:alert/3:both]  | R + B | record the access control logs  |
|  |  |             | attack<br>[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<br>[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<br>[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 java<br>blocked mten packetfilter pki tcp<br>reset 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<br>[0:full/1:hourly/2:daily/3:weekly/<br>4:none]   | R + B | mail schedule policy  |
|  |  |             | schedule week<br>[0:sun/1:mon/2:tue/3:wed/4:thu/5<br>: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  |

**ZyXEL Confidential**

|  |                |                               |       |   |
|--|----------------|-------------------------------|-------|---|
|  |                | 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                              |
|  | 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 |   |

**ZyXEL Confidential**

|  |            |             |  |       |  |
|--|------------|-------------|--|-------|--|
|  | 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><br><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><br><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<br>0: disable <default><br>1: enable |
|  |            | display     | <iface name>   | R     | display roadrunner information<br>iface-name: enif0, wanif0            |
|  |            | restart     | <iface name>   | R     | restart roadrunner   |
|  | ddns       |             |  | R + B |  |

**ZyXEL Confidential**

|  |      |          |                   |       |   |
|--|------|----------|-------------------|-------|---|
|  |      | 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 |         |      |                | Flag  | 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<br>level 0: disable debug log<br>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   |



**ZyXEL Confidential**

|  |             |       |               |       |   |
|--|-------------|-------|---------------|-------|---|
|  |             | 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  |        | [rfc3com]  | 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<br><yes/no> |  |  | Activate or deactivate the saved firewall settings |

**ZyXEL Confidential**

|          |                          |  |                              |  |   |
|----------|--------------------------|--|------------------------------|--|---|
|          | 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-service <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-service           |  |                              |  | Display all configured custom services.   |
|          | custom-service <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                    |  | Edit the mail address to send the alert   |

**ZyXEL Confidential**

|  |  |            |  |  |   |
|--|--|------------|--|--|---|
|  |  |            | <e-mail address>   |  |   |
|  |  |            | 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-minute <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 <0~255>   |  | The threshold to stop deleting the old half-opened 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                                      |

**ZyXEL Confidential**

|        |          |            |                 |  |  |
|--------|----------|------------|-----------------|--|--|
|        |          |            |                 |  | 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   |

**ZyXEL Confidential**

|        |          |            |              |  |  |
|--------|----------|------------|--------------|--|--|
|        |          |            |              |  | 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                            |
|         |          | siptimeout | <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><br><0:FQDN 1:wildcard> <0:from ISP<br>group 1:user defined> <isp group idx ip<br>address>                      |      | edit dns A record                              |
|         |          |            | editns <record idx> <*> domain name><br><0:from ISP 1:user defined(public) 2: user<br>defined(private)> <isp group idx dns server<br>ip> |      | edit dns NS record                             |

|  |          |              |   |       |  |
|--|----------|--------------|---|-------|--|
|  |          |              | inserta <before record idx -1:new> <name><br><0:FQDN 1:wildcard> <0:from ISP<br>group 1:user defined> <isp group idx ip<br>address>                     |       | insert dns A record                                  |
|  |          |              | insertns <before record idx -1:new><br><*<domain name> <0:from ISP 1:user<br>defined(public) 2: user defined(private)> <isp<br>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<br><0:none 1:name 2:type 3:IP 4:refCnt 5:ttl><br>[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                    |
|  |          |              | ttl <second(60 ~ 3600)>   |       | set positive cache maximum ttl                       |
|  | 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<br><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><br>[<metric>]  | R     | add route  |
|  |          | addiface     | <dest_addr default>[/<bits>] <gateway><br>[<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><br>[<metric>]  | R     | set static route destination address and<br>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                       |

**ZyXEL Confidential**

|  |           |            |   |       |  |
|--|-----------|------------|---|-------|--|
|  | telnet    |            | <host> [port]   | R + B | execute telnet client command  |
|  | tracert   |            | <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<br>[filterList/disableAllExceptTrusted/unblock<br>RWFTToTrusted/keywordBlock/fullPath/cas<br>eInsensitive/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 filter's general setting   |
|  |           |            | webFeature  | R + B | [block/nonblock]<br>[activex/java/cookei/webproxy]   |
|  |           |            | timeOfDay[always/hh:mm] [hh:mm]   | R + B | set block time   |
|  |           |            | exemptZone display  | R + B | display exemptzone information   |
|  |           |            | exemptZone actionFlags<br>[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<br>according the database on server or local<br>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<br>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<br>registered and write the original<br>license key to flash |
|  |           |            | zssw  | R + B | change the zssw's URL  |
|  | tredir    |            |   | R     |  |
|  |           | failcount  | <count>   | R     | set tredir failcount   |

**ZyXEL Confidential**

|  |          |            |                                      |       |   |
|--|----------|------------|--------------------------------------|-------|---|
|  |          | 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:dmz][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                     |



|  |      |            |                             |   |   |
|--|------|------------|-----------------------------|---|---|
|  |      | resetport  | aol [on/off]                | R | Turn on/off aol flag                            |
|  |      | incikeport | <iface>[on/off]             | R | reset all nat server table entries              |
|  |      | session    | [session per host]          | R | turn on/off increase ike port flag              |
|  |      | deleteslot | <iface> <slot>              | R | set nat session per host value                  |
|  |      | routing    | [0:LAN 1:DMZ] [0:no 1:yes]  | R | delete specific slot of iface                   |
|  | igmp |            |                             | R | set NAT routing attributes                      |
|  |      | debug      | [level]                     | R |   |
|  |      | forwardall | [on/off]                    | R | set igmp debug level                            |
|  |      | querier    | [on/off]                    | R | turn on/off igmp forward to all interfaces flag |
|  |      | iface      |                             | R | turn on/off igmp stop query flag                |
|  |      |            | <iface> grouptm <timeout>   | R |   |
|  |      |            | <iface> interval <interval> | R | set igmp group timeout                          |
|  |      |            | <iface> join <group>        | R | set igmp query interval                         |
|  |      |            | <iface> leave <group>       | R | join a group on iface                           |
|  |      |            | <iface> query               | R | leave a group on iface                          |
|  |      |            | <iface> rsptime [time]      | R | send query on iface                             |
|  |      |            | <iface> start               | R | set igmp response time                          |
|  |      |            | <iface> stop                | R | turn on of igmp on iface                        |
|  |      |            | <iface> ttl <threshold>     | R | turn off of igmp on iface                       |
|  |      |            | <iface> v1compat [on/off]   | R | set ttl threshold                               |
|  |      | robustness | <num>                       | R | turn on/off v1compat on iface                   |
|  |      | status     |                             | R | set igmp robustness variable                    |
|  |      |            |                             | R | dump igmp status                                |

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

[Home](#)

| Command |               |         |   | Description  |
|---------|---------------|---------|---|--|
| ipsec   | 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   |

**ZyXEL Confidential**

|  |              |                                |   |  |
|--|--------------|--------------------------------|---|--|
|  |              |                                |   | 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 minutes   |
|  |              |                                |   | - 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 minutes   |
|  |              |                                |   | - 0 means never timeout  |
|  | updatePeerIp |                                |   | Force system to update IPSec rules which use domain name as the secure gateway IP right away.  |
|  | dial         | <rule index><br><policy index> |   | Initiate IPSec rule <#> policy <#> from ZyWALL box   |
|  | ikeDisplay   | <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  |
|  |              | lclIdType                      | <0:IP   1:DNS   2:Email>  | Set local ID type  |
|  |              | lclIdContent                   | <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:RSASignature   2:preShare Key+XAUTH   3:RSASignature+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.  |

**ZyXEL Confidential**

|  |               |                 |                                      |  |
|--|---------------|-----------------|--------------------------------------|--|
|  |               | 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>         | Set radius username and password   |
|  | ipsecDisplay  | <rule #>        |                                      | Display IPSec rule #, if no rule number assigned, this command will show current working buffer.<br>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 antireplay 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 #  |

**ZyXEL Confidential**

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

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

**ZyXEL Confidential**

| Command |              |                 |                             |                       | Description   |
|---------|--------------|-----------------|-----------------------------|-----------------------|---|
| sys     | Firewa<br>ll |                 |                             |                       |   |
|         |              | 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.                                  |
|         |              | dynamicr<br>ule |                             |                       |   |
|         |              |                 | display                     |                       | Display firewall dynamic rules                            |
|         |              | tcprst          |                             |                       |   |
|         |              |                 | rst                         |                       | Set TCP reset sending on/off.                             |
|         |              |                 | rst113                      |                       | Set TCP reset sending for port 113 on/off.                |
|         |              |                 | display                     |                       | Display TCP reset sending setting.                        |
|         |              | 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<br>[on/off] | Set schedule on or off by day – Wednesday.                |
|         |              |                 |                             | thursday<br>[on/off]  | Set schedule on or off by day – Thursday.                 |
|         |              |                 |                             | friday [on/off]       | Set schedule on or off by day – Friday.                   |
|         |              |                 |                             | saturday<br>[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<br>[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_ce |  |  |             |

|  |    |                            |  |   |
|--|----|----------------------------|--|---|
|  | rt |                            |  |   |
|  |    | create                     |  |   |
|  |    |                            | selfsigned<br><name><br><subject> [key<br>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<br><name><br><subject> [key<br>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<br><name> <CA<br>addr> <CA<br>cert> <auth<br>key><br><subject> [key<br>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<br><name> <CA<br>addr> <CA<br>cert> <auth<br>key><br><subject> [key<br>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><br>[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>                   |  | Add a new directory service. <name> specifies a descriptive name   |

|  |                  |  |  |   |
|--|------------------|--|--|---|
|  |                  | <addr[:port]><br>[login:pswd]                |  | 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><br><addr[:port]><br>[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_m<br>anager |  |  |   |
|  |                  | 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  |
|         |           | dmz  | enable  | <bandwidth xxx> | Enable bandwidth management in DMZ 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 DMZ  |
|         |           | wlan | enable  | <bandwidth xxx> | Enable bandwidth management in WLAN with bandwidth xxx bps. If the user doesn't set the bandwidth, the default value is 100Mbps. |



**ZyXEL Confidential**

|  |       |     |         |                 |                 |  |
|--|-------|-----|---------|-----------------|-----------------|--|
|  |       |     |         | <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 WLAN   |
|  | 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.   |
|  |       | dmz | add #   | bandwidth xxx   | <name xxx>      | Add a class with bandwidth xxx bps in DMZ. 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 DMZ. 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 DMZ.   |

**ZyXEL Confidential**

|  |         |            |       |  |                 |  |
|--|---------|------------|-------|--|-----------------|--|
|  |         | wlan       | add # | bandwidth xxx  | <name xxx>      | Add a class with bandwidth xxx bps in WLAN. 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 WLAN. 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 WLAN.  |
|  | 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.   |
|  |         | dmz        | add # | Daddr <mask Dmask> Dport Saddr <mask Smask> Sport protocol |                 | Add a filter for class # in DMZ. 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 DMZ.   |
|  |         | wlan       | add # | Daddr <mask Dmask> Dport Saddr <mask Smask> Sport protocol |                 | Add a filter for class # in WLAN. 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 WLAN.  |
|  | show    | interface  | lan   |  |                 | Show the interface settings of LAN   |
|  |         |            | wan   |  |                 | Show the interface settings of WAN   |
|  |         |            | dmz   |  |                 | Show the interface settings of DMZ   |
|  |         |            | wlan  |  |                 | Show the interface settings of WLAN  |
|  |         | class      | lan   |  |                 | Show the classes settings of LAN   |
|  |         |            | wan   |  |                 | Show the classes settings of WAN   |
|  |         |            | dmz   |  |                 | Show the classes settings of DMZ   |
|  |         |            | wlan  |  |                 | Show the classes settings of WLAN  |
|  |         | filter     | lan   |  |                 | Show the filters settings of LAN   |
|  |         |            | wan   |  |                 | Show the filters settings of WAN   |
|  |         |            | dmz   |  |                 | Show the filters settings of DMZ   |
|  |         |            | wlan  |  |                 | Show the filters settings of WLAN  |
|  |         | statistics | lan   |  |                 | Show the statistics of the classes in LAN  |
|  |         |            | wan   |  |                 | Show the statistics of the classes in WAN  |
|  |         |            | dmz   |  |                 | Show the statistics of the classes in DMZ  |
|  |         |            | wlan  |  |                 | Show the statistics of the classes in WLAN   |
|  | monitor | lan        | <#>   |  |                 | Monitor the bandwidth of class # in LAN. If the class is not   |

|  |        |       |     |  |  |  |
|--|--------|-------|-----|--|--|--|
|  |        |       |     |  |  | specific, all the classes in LAN will be monitored.<br>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.<br>The first time you key the command will set it on; the second time you will set it off, and so on.   |
|  |        | dmz   | <#> |  |  | Monitor the bandwidth of class # in DMZ. If the class is not specific, all the classes in DMZ will be monitored.<br>The first time you key the command will set it on; the second time you will set it off, and so on.   |
|  |        | wlan  | <#> |  |  | Monitor the bandwidth of class # in WLAN. If the class is not specific, all the classes in WLAN will be monitored.<br>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         |