



Firmware Release Note

ZyWALL 35

Release 3.62(WZ.2)

Date:	June 28, 2004
Author:	Jason Chiang

ZyXEL ZyWALL 35 Standard Version release 3.62(WZ.2) Release Note

Date: June 28, 2004

Supported Platforms:

ZyXEL ZyWALL 35

Versions:

ZyNOS F/W Version : V 3.62(WZ.2) | 06/28/2004 09:01:09

BootBase : V1.07 | 03/23/2004 12:26:18

Note:

1. Restore to Factory Defaults Setting Requirement: No.
2. The secondary WAN interface, or WAN 2, is "Backup Line". It is the backup of the Primary WAN 1. By default WAN2 is active. WAN 2 will bring-up automatically when WAN 1 connection fails.
3. 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.
4. 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.
5. Using Web to configure VPN, the phase 1 algorithms have been fixed to DES + MD5. If other algorithms are preferred, please use ADVANCE page to configure them.
6. When firewall turns from "off" to "on", the firewall initialization procedure will disconnect all connections running through the ZyWALL.
7. 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.
8. 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.
9. 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.
10. The default roles for LAN/DMZ ports setting are: port 1 to 4 = LAN ports.
11. If the encapsulation type of WAN1 and WAN2 are both PPTP, The PPTP IP settings (My IP Addr, My IP Mask and Server IP Addr) on WAN1 and WAN2 must be different subnet.
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 two entries for static route are reserved for creating WAN1 and WAN2 default routes and are READ-ONLY.

Known Issues:

1. 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.
2. Sometimes on screen the “Local Area Connection” icon for UPnP disappears. The icon shows again when restarting PC.
3. 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..
4. On the SUA/ Address Mapping page, users can enter two or above same rules.
5. On the SUA/ Address Mapping Edit page, the user can give the same local IP and global IP.
6. SMT 15.1, if we try to edit the 11th rule then press ESC, the system returns some weird characters.
7. You must notice those metric values of WAN 1, WAN 2, Traffic-Redirect and Dial-backup. You should better give those values, Dial-backup > Traffic-Redirect > WAN 2 > WAN 1. For example, WAN 1(1), WAN 2(2), Traffic-Redirect(14), Dial-backup(15).
8. Bandwidth Management doesn't work on wireless LAN.
9. Sometimes, modify an active IPsec rule (the VPN tunnel was created) will crash the system, if this tunnel is going the re-key process.
10. Symptom: WAN2 port will duplicate received packet and modify source IP as WAN2's IP, then send out the copied packet.
Condition:
 - (1) Let WAN2 port, PC-A and PC-B connect to the same hub.
 - (2) PC-A ping PC-B
 - (3) PC-B will receive ICMP echo packet send from WAN2 port as well.
11. 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.
12. The DMZ TxPkts counter increment at about 1 pkt/min even without any Ethernet cables ever connected. This is because RIP on DMZ port is turned on by default.
13. At SMT24.1, the collisions for WAN2, LAN and DMZ port are not really counted.
14. AES doesn't work with key length 192 and 256.
15. If there are two sub-classes (under same parent) running with TCP services, and both of these two classes can borrow bandwidth by parent, their current bandwidth usage will

be very unstable.

16. BWM can not control a subnet :

- (1) Add a class (all filter item is 0) under root class (call rule A
- (2) Add a class under A for a subnet (call rule B) , the B never works

17. BWM out of control :

- (1) Add a class rule (all filter item is 0) under root class (call rule A) .
- (2) Add two class rules under A (rule B , C) , both of them can borrow bandwidth from parent class.
- (3) When B and C are running with UDP packets , sometimes one of them bandwidth is 0.

18. BWM bandwidth should not be smaller than the sum of children classes?

- (1) Add a class (call rule A) which bandwidth is 400.
- (2) Add a subclass (call rule B) which bandwidth is 100.
- (3) Add another subclass (call rule C) with bandwidth 400.
- (4) C still can be saved, this should not be allowed.

Features:

Modifications in V3.62(WZ.2) | 06/28/2004

Formal release.

Modifications in V3.62(WZ.2)b1 | 06/08/2004

1. [ENHANCEMENT] Support Vantage CNM 2.0 (Vantage Centralized Network Management).
2. [BUG FIX]
Symptom: Trigger port will disappear after system reboot.
Condition:
 - (1) Configure Trigger port rule.
 - (2) System reboots.
 - (3) The configured Trigger port rule disappeared.

Modifications in V3.62(WZ.1) | 05/25/2004

Formal release.

Modifications in V3.62(WZ.1)b1 | 05/13/2004

1. [BUG FIX] Symptom: TCP bandwidth usage is too low when the service is managed

ZyXEL Confidential

by Bandwidth management.

Condition: If there is a TCP service going through ZyWALL and is managed by router's bandwidth management mechanism, the bandwidth of this service is much slower than the limited bandwidth.

2. [BUG FIX] Symptom: Bandwidth management "barrow bandwidth" mechanism is not correct

Condition:

- (1) Set up a sub-class A under root. A's priority is 3.
- (2) Set up two sub-classes under A, call them B and C. Both B and C's priority is 3, too.
- (3) When B and C are running, they can't borrow bandwidth even their "Borrow bandwidth from parent class" is checked.

Modifications in V3.62(WZ.0) | 04/07/2004

1. Formal release.

Modifications in V3.62(WZ.0)b5 | 04/06/2004

1. [BUG FIX]

Symptom: NAT address mapping rule disappears after router reboots.

Condition:

- (1) In eWC→SUA/NAT→Address Mapping page
- (2) Adds 50 rules.
- (3) Reboots router, user can only see the first 22 rules and the other rules disappear.

2. [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.

Modifications in V3.62(WZ.0)b4 | 03/24/2004

1. [BUG FIX]

Symptom: When initiator receives wrong phase 1 ID from responder, it will jump to another rule.

Condition: During IKE negotiation in Main mode, if responder's "Local ID Content" mismatches initiator's "Peer ID Content", initiator will do rule swap and choose another rule to negotiate.

2. [BUG FIX]

Symptom: The daylight saving feature does not function normally. When leaving the daylight saving period, the system will not automatically adjust time.

Condition:

- (1) Configure current time in daylight saving.
- (2) After the current time leaves the end date of daylight saving, the system does not adjust to correct time.

3. [BUG FIX]

Symptom: Fixed a wording error "Use WAN IP Address" in SMT1.1.

Condition:

- (1) Go to SMT1.1 (Dynamic DNS).
- (2) The words "Use WAN IP Address" should be "Use IP Address".

4. [ENHANCEMENT]

In eWC→MAINTENANCE→Time and Date :

- (1) The original page is separated into three parts
 - (a) Current Time and Date only displays the information about the system time and date and it's read-only.
 - (b) Time and Date Setup includes:
 - Manual (None, use no time protocol)
 - Get from Time Server (Use protocol Daytime, Time or NTP)
 - (c) Time Zone Setup: users can configure the time zone and the daylight saving.
- (2) After pressing 'Synchronize Now' button, ZyWALL not only synchronizes with time server immediately but also stores the configurations. After pressing the synchronize button, a warning screen will appear.
- (3) There are two different behaviors when configuring the date and time.
 - (a) If users only change the time zone and daylight saving but don't change the original time and date. The new time and date will be updated based on the new time zone and if it is in the daylight saving period.
 - (b) If users change the time or date, no matter if users change the time zone and daylight saving, ZyWALL will store the new date and time directly, regardless of the time zone and daylight saving which were configured by the user.
- (4) In Daytime and Time protocol process, set the TCP connection timeout as 6 seconds.
- (5) In NTP protocol process, every time server in ZyWALL's default time server list is tried 3 times at most.

5. [ENHANCEMENT]

In eWC→HOME,

- (1) Let text boxes of 'current time' and 'current date' looked like labels.
- (2) Changed the wording from "NAT Session" to "NAT Concurrent Session".

6. [BUG FIX]

Symptom: Router will crash.

Condition: Use CI command "ip urlfilter webControl cache timeout"

7. [BUG FIX]

Symptom: SMT menu 25 shows 6 more policy route entries than predefined entry

number.

Condition:

- (1) Login SMT and go to menu 25
- (2) Press Next Page until the last page
- (3) Assume we define 24 as policy route rule number, we will see 30 rules on the last page.

8. [BUG FIX]

Symptom: Can't set wireless channel ID when country code is 219 (France).

Condition:

- (1) Set country code with 219.
- (2) Set channel ID with 6 - 13 via SMT or eWC.
- (3) After applying changes, the channel ID will restore to 1.

9. [ENHANCEMENT]

In eWC→MAINTENANCE→Time and Date:

- (1) Changed the warning message displayed when router is synchronizing with Time Server.
- (2) Removed the data format for current time and current date.
- (3) Added a note for reminding users of that "Time Server Address" is Optional. There is a pre-defined NTP time server list.

10. [ENHANCEMENT]

The ZyWALL now also records the time server address (domain name or IP address) in the time synchronization result (successful or failed) logs.

11. [BUG FIX]

Symptom: After successful time synchronization with LAN side NTP server, the "Destination" IP address for LOG message "Time initialized by NTP server" is WAN IP address.

Condition:

- (1) Go to eWC→MAINTENANCE→Time Setting
- (2) Choose "Time Protocol" as "NTP(RFC-1305)"
- (3) Setup "Time Server Address" as a server located at LAN side.
- (4) Click Apply and then press "Synchronize Now".
- (5) Go to eWC→LOGS→View Log, will see a log "Time initialized by NTP server" where the "Destination" address is router's WAN IP address, it should be router's LAN IP address.

12. [FEATURE CHANGE]

Was: When user access web sites which is in LAN IP alias or DMZ, content filter will check these traffic need to block or not.

Is: Content filter does not block web traffic if the web site is in router's LAN/LAN IP Alias/DMZ.

13. [BUG FIX]

Symptom: Some trusted web sites' pictures cannot be seen.

Condition:

- (1) In "eWC→CONTENT FILTER→Customization", select "Disable all Web traffic except for trusted Web sites" and "Don't block Java/ActiveX/Cookies/Web proxy to trusted Web sites".
- (2) At the same page, add "kobeoffshore.com" to "Trusted Web Sites".

- (3) Open web browser to access "kobeoffshore.com".
- (4) All the pictures cannot be seen.
- 14. [BUG FIX]
Symptom: The router crashes after the user configures the log setting.
Condition:
 - (1) Go to eWC→LOGS→Log settings page.
 - (2) Configure Mail Server, Mail Subject, Send log to, Active Syslog Logging fields and choose all check boxes under "Send Immediate Alert".
 - (3) Connect WAN1 to network.
 - (4) The system will crash after getting DHCP address.
- 15. [BUG FIX]
Symptom: Responder will jump to wrong VPN rule when current rule's phase 2 parameter is wrong.
Condition:
 - Initiator -----NAT router ----- Responder
 - (1) Initiator has one VPN rule in which NAT traversal is on.
 - (2) In responder, there are two VPN rules.
 - Rule 1: NAT traversal is on, and phase 2 parameters are wrong.
 - Rule 2: NAT traversal is off, and all other parameters are correct.
 - (3) Trigger tunnel from initiator, and responder will use rule 1 to negotiate.
 - (4) When phase 2 negotiation starts, responder found rule 1's parameters are wrong, and will jump to rule 2.
 - (5) Negotiation will keep going and tunnel will be up.
- 16. [ENHANCEMENT]
If the Local/Remote Address Type is "Subnet Mask", the "Local/Remote IP Address" in VPN summary table must be like "1.1.1.1 / 255.0.0.0".
WAS: "1.1.1.1 - 255.0.0.0"
IS: "1.1.1.1 / 255.0.0.0"
- 17. [BUG FIX]
Symptom: In SSH connection, if users paste a large number data into CI command then the system will crash.
Condition:
 - (1) Create SSH connection.
 - (2) Enter the CI command mode.
 - (3) Paste a large number data as command.
 - (4) The system will crash.
- 18. [BUG FIX]
Symptom: NAT loopback fail.
Condition:
 - (1) Host A runs FTP server in ZyWALL's LAN side.
 - (2) Turn on SUA and NAT loopback on ZyWALL.
 - (3) Configure default server to host A.
 - (4) Turn on Firewall.
 - (5) Host A runs FTP client and connect to ZyWALL's WAN IP.
 - (6) Connection fails.
- 19. [FEATURE CHANGE]

Add more information about content filter's error events in centralized log and block message. When the packet was blocked because of error happens.

For centralized log:

Was: The blocked log displays "domain" in the message filed.

Is: The blocked log display <domain>: <reason> in the message files. The wording of reasons contains:

- (1) "Waiting content filter server timeout"
- (2) "DNS resolving failed"
- (3) "Creating socket failed"
- (4) "Connecting to content filter server fail"
- (5) "License key is invalid"

For block message:

Was: The blocked page only shows a deny message if the license key of external content filter is invalid.

Is: The blocked page will show <Deny message> : "License key is invalid" in this case.

20. [FEATURE CHANGE]

Give different returned error message between timeout and invalid license in
eWC→CONTENT FILTER→Categories→Test Against Internet Server

Was: It returns "Request error" if the license key of external content filtering is invalid or the request is timeout.

Is:

- (1) It returns "Request timeout" if the request is timeout
- (2) It returns "License key is invalid" if the license key is invalid.

21. [BUG FIX]

Symptom: Router will crash.

Condition:

- (1) In eWC→CONTENT FILTER→General, select "Enable Content Filter" and click "Apply"
- (2) In eWC→CONTENT FILTER→Categories, select "Enable External Database Content Filtering" and at least one category in "Select Categories". Click "Apply" after selection.
- (3) Open web browser and access a web site which belongs to the category you select in step 2.
- (4) In eWC→CONTENT FILTER→Categories, un-select the category selected in step 2 and keep at least one category is selected. Click "Apply" after selection.
- (5) Repeat step 3 immediately after step 4.
- (6) Router will crash or hang.

22. [BUG FIX]

Symptom: No firewall checking when using dial backup connection.

Condition:

- (1) Setup dial backup environment.
- (2) Enable firewall and block WAN to WAN traffic.
- (3) Pull out the WAN line and make dial backup turn on.
- (4) Try to FTP to firewall WAN ip address from outside workstation.
- (5) Firewall will not block the ftp connection.

Note: to enable Firewall checking for Dial Backup, please re-configure and save Dial

Backup configuration again.

23. [BUG FIX]

Symptom: Content filter cannot work under traffic redirect.

Condition:

- (1) Set router's traffic redirect check point as a PC or router in LAN or DMZ
- (2) Force router to traffic redirect.
- (3) All web traffic will bypass content filter.

24. [BUG FIX]

Symptom: In VPN negotiation, if responder jumps to a new rule which has empty phase 1 peer ID content, tunnel will not be up.

Condition: There are two rules in responder and one rule in initiator. All rules in initiator and responder are in aggressive mode.

Responder: Rule 1: dynamic rule (Secure gateway IP is 0.0.0.0).

Rule 2: static rule with wrong phase 2 ID.

Both rule 1 and rule 2 has empty phase 1 peer ID (i.e., in SMT menu 27.1.1, "Peer ID Content" is empty).

When trigger tunnel from initiator, negotiation will fail.

25. Symptom: Responder will jump to wrong rule when phase 1 parameter of current rule is wrong.

Condition: There is one rule in initiator and three rules in responder.

Initiator:

Rule 1==> Negotiation mode = pre-shared key. Encapsulation mode = Tunnel mode.

Responder:

Rule 1==> Negotiation mode = Certificate. Encapsulation mode = Tunnel mode.

Phase 2 local ID is wrong.

Rule 2==> Negotiation mode = pre-shared key. Encapsulation mode = Transport mode.

Phase 2 local ID is wrong.

Rule 3==> Negotiation mode = pre-shared key. Encapsulation mode = Tunnel mode.

Phase 2 ID is correct. (This rule should be chosen eventually).

When trigger tunnel from initiator, responder will use Rule 1 to negotiate and then jump to Rule 2. And eventually tunnel won't be up because initiator ID mismatches during phase 2 negotiation.

26. [BUG FIX]

Symptom: Firewall eWC available service only shows max 60 entries, including predefined ports(services) and custom ports. Currently there are 43 predefined ports. If user defines more than eighteen custom ports, some of the predefined ports will not be on the eWC list.

Condition:

- (1) There are 43 predefined ports on the firewall eWC available services.
- (2) Add more than 18 custom ports. Some of the predefined ports will not be on the eWC list.

27. [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.

ZyXEL Confidential

- (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".
28. [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.
29. [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.
30. [ENHANCEMENT]
Support Intel 16Mbytes Flash ROM.
31. [ENHANCEMENT]
In WC→LAN→Port Roles and eWC→DMZ→Port Roles :
(1) When users change port roles. ZyWALL needn't be rebooted.
(2) Add a waiting page to warn users that the ZyWALL is re-configuring its hardware, and during this period, users might not access ZyWALL momentarily.

Modifications in V3.62(WZ.0)b3 | 02/16/2004

1. [FEATURE CHANGE] Extend eWC→static route number from 30 to 50
2. [FEATURE CHANGE] Change eWC→policy route number from 72 to 48
3. [FEATURE CHANGE] Extend rule number in eWC→SUA/NAT→SUA Server from 30 to 50.
4. [FEATURE CHANGE] Extend NAT session number from 2,048 to 10,000
5. [FEATURE CHANGE] Extend Firewall max rule number from 100 to 200
6. [FEATURE CHANGE] Extend Cerberian content filter max connection number from 20 to 50
7. [FEATURE CHANGE] Extend number of classes from 20 to 50 for Bandwidth Management
8. [FEATURE CHANGE] Extend number of filters from 20 to 50 for Bandwidth

Management

9. [FEATURE CHANGE] Extend max depth of classes in the tree from 1 to 3 for Bandwidth Management
10. [FEATURE CHANGE] Extend Certificate buffer size from 32K to 64K
11. [ENHANCEMENT]
Support wireless driver B100+B120+G100
12. [ENHANCEMENT]
Content filter supports to block two kinds of special URL.
(1) URL has the '@' sign. For example, <http://zyxel@209.247.228.201>
(2) IP address is transferred to decimal. For example, <http://209.247.228.201> ==> <http://3522684105>
13. [ENHANCEMENT]
Enhance fatal error log. When a fatal error occurs, system will reboot. In the past, there is no useful information before rebooting. Now, there will be some error logs shown on console before system reboots.
14. [BUG FIX]
Symptom: SMT Menu 27.1.1 "Peer ID Type" behavior is wrong when authentication method is pre-shared key.
Condition:
(1) In Menu 27.1.1, change "Peer ID Type". For example, change "Peer ID Type" from IP to DNS.
(2) Go to Menu 27.1.1.1
(3) Go back to Menu 27.1.1 by pressing "Esc" button.
(4) "Peer ID Type" is still "IP" , which should be "DNS" in this case.
15. [BUG FIX]
Symptom: SSH can't restrict server access.
Condition: In eWC-->Remote Management-->SSH: Whatever users choose in "Server Access", users can always access server in any interface.
16. [ENHANCEMENT]
The centralized log mechanism will merge repeated content filter license error logs into a single log, instead of showing the log repeatedly.
Note: System will count the number of repeated content filter license error logs, and append this information to the log message.
17. [BUG FIX]
Symptom: If there are more than 10 VPN tunnels, the 10th tunnel in Current IPSec Security Associations table (eWC>Home>VPN Status) will be covered by the bottom frame.
Condition:
(1) Open eWC.
(2) Go to "Home" page.
(3) Click VPN Status button.
(4) If there are more than 10 VPN tunnels, the 10th tunnel in Current IPSec Security Associations table will be covered by the bottom frame.
18. [BUG FIX]
Symptom: IKE negotiation will success when PFS parameter is different between Initiator and Responder.

Condition:

- (1) Initiator has only one rule without PFS.
- (2) Responder has only one rule with PFS parameter is DH1.
- (3) Initiator dial to Responder.
- (4) Tunnel establishment will success, but should fail in this case.

19. [BUG FIX]

Symptom: EWC wording error.

Condition: In eWC -> "Login" page -> "Replace Factory Default Certificate" page: wording "Ingore" spelling error.

20. [BUG FIX]

Symptom: EWC wording error.

Condition: In eWC -> "MAINTENANCE" page -> "Time Setting" page: wording "Dalight" spelling error.

21. [BUG FIX]

Symptom: EWC cannot show correct NAT session usage in "HOME" page of backup line mode.

Condition:

- (1) Switch active WAN to WAN2 or Dial Backup in backup line mode.
- (2) In eWC -> "HOME" page, the NAT session usage is incorrect.

22. [BUG FIX]

Symptom: Router will reply the ping packet on behave of the NAT default server located on LAN.

Condition:

- (1) Set NAT default server IP address to an address on LAN.
- (2) Ping from WAN side to the NAT default server IP address.
- (3) Router will reply the ping on behave of the NAT default server, which then never receives the ping packet and thus never replies it.

23. [BUG FIX]

Symptom: In ZW35 eWC home page, the NAT session is always 2048.

Condition: When ZW35 boots up, the NAT session number is always 2048.

24. [BUG FIX]

Symptom: In eWC, the system cannot display the login page when the eWC connection has timed out (or disconnected) and the user clicks on an eWC button.

Condition:

- (1) Log in eWC.
- (2) Enter console mode to disconnect eWC.
- (3) Click buttons, such as Apply and Refresh, in eWC.
- (4) The browser will show "Object Not Found".

25. [BUG FIX]

Symptom: In the SMT menu 11 and eWC, the user cannot assign the Ethernet static IP of the WAN2.

Condition:

- (1) Log in SMT.
- (2) Enter menu 11 to configure WAN2.
- (3) Configure a Ethernet static IP in the menu 11.3
- (4) The router cannot store this configuration.

26. [BUG FIX]

Symptom: PC can't setup TCP connections via ZyWall to the internet when ZyWALL's WAN encapsulation is PPTP.

Condition:

- (1) Set WAN encapsulation with PPTP.
- (2) Setup a TCP connection to the internet. For example : Use browser to create an HTTP connection.
- (3) Browser won't retrieve any information because ZyWALL always resets TCP connections.

27. [BUG FIX]

Symptom: Traceroute or PingPlotter are not able to discover ZyWALL's LAN interface.

Condition:

- (1) Running Traceroute or PingPlotter on desktop.
- (2) Both applications can not discover ZyWALL's LAN interface.
- (3) Firewall log shows "Unsupported/out-of-order ICMP: ICMP(type:11, code:0)".

28. [ENHANCEMENT]

- (1) Re-layout the zw35 Port Roles pages to fix the out of alignment problem when users set Windows OS font size to "Large".
- (2) Modify the CSS by adding IP field width to fix the problem that the IP Address field will become two lines when users set Windows OS font size to "Large".

29. [BUG FIX]

Symptom: X-Auth behavior in VPN rule setting page isn't correct.

Condition:

- (1) eWC-->VPN-->Extended Authentication: Do not select "Enable Extended Authentication" (X-Auth is disabled).
- (2) Select "Client mode" and keep "User name" and "Password" empty.
- (3) VPN rule can't be saved and message "Both User Name and Password are required" shows on "Status".

30. [BUG FIX]

Symptom: On IE, the BWM (Bandwidth Management) tree view can be expanded and collapsed. But on Mozilla, BWM tree can't be expanded or collapsed.

Condition:

- (1) Go to eWC>BW MGMT>Class Setup
- (2) If there is no any sub-class, use the 'Add Sub-Class' button to add one.
- (3) Go back to eWC>BW MGMT>Class Setup, click the hyperlink in BWM tree, the tree can't be expanded.

31. [ENHANCEMENT]

- (1) After the ZyWALL sends an update request to DDNS server and receives a return code from DDNS server, the ZyWALL will record the return code in centralized log.
- (2) The IP address of the last update request will be recorded in centralized log.
- (3) Once the user changes the hostname in the SMT menu 1.1 or Web, ZyWALL will send an update request to DDNS.
- (4) When the ZyWALL receives an error code from the DDNS server, ex: "badauth", "nohost", "abuse", it will stop updating.
- (5) When the user chooses the option (Let the DNS server auto detect the IP Address) to use CheckIP (Server Auto Detect) to determine the current IP address, the request

string to checkip.dyndns.org sent by the ZyWALL is ended with "CRLF CRLF".

(6) By DyDNS.org's abuse policy, the force update period is changed from 5 days to 28 days.

(7) Let wordings in SMT1.1 and the DDNS web page to be consistent.

32. [BUG FIX]

Symptom: The ZyWALL will send updates when the user has not entered a userid or password or all host names.

Condition: Set a userid or password or host names as empty one in the SMT menu 1.1 or Web.

33. [BUG FIX]

Symptom: Fixed a wording error "domian name" in eWC>CONTENT FILTER>Categories.

Condition:

(1) Go to eWC>CONTENT FILTER>Categories>Test Web Site Attribute>Test Web Site Attribute (an edit box).

(2) The words next to the edit box is mis-spelled as "Domian name".

34. [BUG FIX]

Symptom: Fixed a wording error "DNS Server" in eWC>WAN>DDNS.

Condition:

(1) Go to eWC>WAN>DDNS>IP Address Update Policy> DNS server auto detect IP Address(a radio button). Or go to SMT1.1>DNS Server Auto Detect IP Address.

(2) The words "DNS server" in "DNS server auto detect IP Address" should be "DDNS server".

35. [BUG FIX]

Symptom: Router will crash.

Condition:

(1) A host connects to router.

(2) User accesses website then disconnect.

(3) After 2 hours, user accesses website again.

36. [BUG FIX]

Symptom: In eWC->UPnP->UPnP Setup, the "Note: For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP." is missing, the <HR> is missing, the Apply and Reset buttons are aligned left.

Condition:

(1) Go to eWC->UPnP->UPnP Setup page.

(2) "Note: For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP." is missing.

(3) <HR> HTML line is missing.

(4) Apply and Reset buttons are aligned left on this page.

37. [BUG FIX]

Symptom: LAN host cannot access Internet.

Condition: When one host continuously tries to setup a new connection, sometimes it fails and the host never can access Internet.

38. [ENHANCEMENT]

Pause console display when the NAT session information fills a console screen.

39. [BUG FIX]

Symptom: Console hangs when editing VPN rule at SMT menu 27.1

Condition:

- (1) Go to SMT menu 27.1 and edit a new rule.
- (2) Leave "Name" field blank, enter "Edit IKE Management Setup" directly.
- (3) Press ESC return to previous menu.
- (4) Console hangs.

40. [BUG FIX]

Symptom: System memory leak and eventually causing the reboot.

Condition:

- (1) Start collecting data in eWC->LOGS->Reports or using CI command "ip rpt start".
- (2) Run for a very long time.
- (3) System will run out of memory and become very unstable.

41. [BUG FIX]

Symptom: Warning message of the SMT11 and WAN web page is wrong.

Condition:

- (1) Configure WAN1 IP address to be a static IP address in the SMT11.3 or WAN web page.
- (2) Continue to configure WAN2 IP address to be a static IP address that is in the same network with LAN or DMZ or WAN1.
- (3) The warning message of the SMT or WEB will keep appearing "WAN must not be on same subnet as LAN" even it may be in the same network with WAN1 or DMZ.

42. [BUG FIX]

Symptom: Internet access wizard is always opened in the Ethernet mode.

Condition:

- (1) Go to eWC>Home>Internet Access Wizard or eWC>WAN>WAN1 and configure settings as the PPTP or PPPoE mode.
- (2) Go back to eWC>Home>Wizard and click the Internet Access button.
- (3) Wizard always display in Ethernet mode no matter ZyWALL is in PPTP/PPPoE.

43. [BUG FIX]

Symptom: Internet access wizard displays the wrong value of remote IP/subnet mask in PPTP/PPPoE mode.

Condition:

- (1) Go to eWC>Home>Internet Access Wizard or eWC>WAN>WAN1 and configure PPTP's My IP Address.
- (2) Go back to eWC>Home>Wizard and click the Internet Access button.
- (3) Change to PPTP mode.
- (4) Remote IP/subnet mask of PPTP/PPPoE mode are different from eWC>WAN>WAN1 and SMT11.1.

44. [BUG FIX]

Symptom: eWC>LOGS>Log Settings, E-mail Log Settings, if Log Schedule = None, the "Day for Sending Log" option is not grayed out.

Condition:

- (1) Go to eWC>LOGS>Log Settings>E-mail Log Settings on Netscape, Mozilla or Firebird.
- (2) The checkbox 'Day for Sending Log' needs to be grayed out when the checkbox 'Log Schedule' is not chosen as 'weekly'.

45. [BUG FIX]
Symptom: Router crashed and reboot when editing SMT menu 3.5
Condition:
(1) Insert WLAN card, then restart router.
(2) In CI command, enter "wlan active 11" instead of "wlan active 1" to active WLAN on router.
(3) Enter SMT 3.5, router crashed and reboot.
46. [BUG FIX]
Symptom: ZyWALL cannot establish IPSec connection to SSH Sentinel.
Condition: When ZyWALL and Sentinel both enable XAUTH, the IKE negotiation will fail.
47. [BUG FIX]
Symptom: IPSec XAUTH cannot work with SoftRemote version 8.0.0
Condition:
(1) Configure corresponding IPSec rule with XAUTH on SoftRemote and ZyWALL.
(2) Trigger SoftRemote IPSec rule.
(3) SoftRemote log shows "no proposal chosen" and connection fails.
48. [FEATURE CHANGE]
Modify wireless channel ID mapping table with Country code setting.
49. [FEATURE CHANGE]
Modify the Time & Date setting policy.
(1) Wording in SMT menu 24.10: Time Protocol= None -> Manual.
(2) Only under Manual mode, users can set the New Time & New Date.
(3) If users change the Time Zone without modifying the New Time or New Date, the system time will automatically be shifted according to new Time Zone.
(4) If users change the Time Zone and also modify the New Time or New Date, the system time will be updated to the New Time and New Date, disregarding the new Time Zone.
Note: This enhancement only works in SMT24.10 now.
50. [BUG FIX]
Symptom: Router will crash.
Condition: When using "ip nat hash" command, router will crash.
51. [BUG FIX]
Symptom: When the Ethernet chip VT6105 operates under Half Duplex mode, its TX functionality might hang permanently due to severe collisions.
Condition:
(1) Connect the ZW35 WAN1 (or LAN port) to a 10M Hub so that the port will operate in 10M/Half-Duplex mode.
(2) Generate a lot of traffic over the 10M Hub.
(3) Have the ZW35 WAN1 port (or LAN port) continuously transmit a lot of packets.
(4) After an indefinite time period, the ZW35 WAN1 port (or LAN port) might permanently fail to transmit packets, as a result of too severe collisions.
52. [BUG FIX]
Symptom: IPsec NAT-Traversal can not work.
Condition:
(1) Setup NAT-Traversal rule at Initiator and Responder, both sides are Tunnel

encapsulation mode.

(2) Connect from Initiator side.

(3) Tunnel can not be established.

53. [BUG FIX]

Symptom: Rule swap failed when NAT-Traversal is on.

Condition:

(1) Initiator setup one NAT-Traversal rule and transport encapsulation mode.

(2) Responder setup two NAT-Traversal rules, the first is tunnel mode, and the second is transport mode.

(3) Initiator starts to establish connection for the transport mode rule.

(4) IKE negotiation will fail.

54. [BUG FIX]

Symptom: IPSec rule swap is fail with NAT traversal.

Condition:

Initiator -----NAT Router -----Responder

(1) Initiator has one rule with NAT Traversal on.

(2) Responder has two rules:

- Rule 1: NAT Traversal is on, and phase 2 ID is wrong.

- Rule 2: NAT Traversal is off, and phase 2 ID is correct.

- All other parameters in rule 1 and rule 2 are correct.

(3) Dial tunnel from initiator. Responder will use rule 1 to start negotiate.

(4) In phase 2, since phase 2 ID is wrong, responder will swap to rule 2 and eventually tunnel will be up because system won't check NAT Traversal flag when swapping the rule.

55. [BUG FIX]

Symptom: ICMP packet of NAT loopback will be blocked by Firewall.

Condition:

(1) Enable Firewall.

(2) NAT default server is set to host A.

(3) Turn on NAT loopback.

(4) Host A pings router's WAN IP address.

(5) Host A does not receive echo reply packet and Firewall log shows "Land Attack".

56. [FEATURE CHANGE]

Change behavior when router detects that the external content filter's license key is invalid.

Was: Disable external content filter and add a centralized log "Content filter's license key expired! disable web control."

Is: Don't disable external content filter and add a centralized log "External content filtering's license key is invalid."

57. [FEATURE CHANGE]

When user registers external content filter, the traffic will not be blocked by "blocking JAVA" option.

Was: When user registers external content filtering and content filter's "blocking JAVA" option is selected, the traffic will be block by content filtering.

Is: The web traffic to content filter's registration site is always forwarded by content filtering.

Note: The protection does not work when system's DNS servers are not set properly.

58. [ENHANCEMENT]

Implement the timeout mechanism on content filter's local cache. Once the cache entry is timeout, it will be delete.

Note: User can set the cache time via CI command "ip urlfilter webControl cache timeout". The unit of setting is hour. Router checks whether there are timeout entries every 30 minutes.

Modifications in V3.62(WZ.0)b2 | 01/13/2004

1. [BUG FIX]

Symptom: Configure VPN rule at eWC fails

Condition:

(1) Edit an VPN rule, choose Certificate authentication method and E-mail as Peer ID Type.

(2) Fill in the Content field with peer's E-Mail ID Content value generated by default certificate.

(3) eWC will show "The maximum ID Content length of DNS or E-Mail is 32 characters" at Status bar.

2. [ENHANCEMENT] On Log Settings page (Send Log - Time for Sending Log), added range check for time format.

3. [BUG FIX] In eWC Firewall->Threshold, the field 'Deny new connection request for ... minutes' can't store the value 256. And also added a range checking in the fix.

4. [ENHANCEMENT] Added a blank space in Perfect Forward Secrecy(PFS) of VPN - VPN RULE - EDIT - ADVANCED.

5. [BUG FIX]

Symptom: Nat incikeport command can not work in autoexec.net.

Condition:

(1) Goto SMT 24.8

(2) Type "sys edit autoexec.net" and add "ip nat incikeport enifl on" after "ip nat lookback on" .

(3) Reboot ZyWall

(4) After reboot, the error message "The nat table of iface enifl is not allocated" will pop up.

6. [ENHANCEMENT] Add a new firewall service type - Roadrunner(TCP/UDP:1026)

7. [BUG FIX]

Symptom: Content filter cannot block cookie content for some web sites.

Condition:

(1) Enable "block cookie" in eWC.

(2) Access <http://www.tomshardware.com> from PC.

(3) PC has cookie contents which are written from the web site. The cookie contents should be blocked by router.

8. [BUG FIX]

Symptom: When system's WAN mac is changed to any PC's mac attached on LAN, LAN traffic will be blocked and can not access Internet for a period of time.

Condition:

- (1) Change system's WAN mac to any PC's mac attached on LAN.
- (2) PC ping system's LAN IP.

9. [BUG FIX]

Symptom: HOME/Internet Access , the Ethernet service type is always “Standard”, and can not set other service type

Condition:

- (1) In eWC, HOME->Internet Access
- (2) Choose Ethernet encapsulation and change service type
- (3) After refreshing page, service type was not be changed

10. [BUG FIX]

Symptom: In eWC, HOME->Internet Access , the ethernet fixed ip address is always 0.0.0.0

Condition:

- (1) Goto eWC->WAN, setup a fixed up with Ethernet Encapsulation
- (2) Goto HOME->Internet Access, Press Next
- (3) IP address is always 0.0.0.0, it should be IP address configured in step 1

11. [BUG FIX]

Symptom: In eWC, HOME->Internet Access , the default Login Server IP Address of Ethernet service type RR-Toshiba / RR-Manager / RR-Telstra is “0.1.0.0”

Condition:

- (1) Goto eWC->HOME->Internet Access.
- (2) Choose Ethernet nncapsulation and service type RR-Toshiba / RR-Manager / RR-Telstra
- (3) The default Login Server IP is 0.1.0.0

12. [BUG FIX]

Symptom: The “Show Statistics” button is missing on eWC->HOME page

Condition:

- (1) Goto eWC->HOME
- (2) “Show Statistics” button is missing.

13. [BUG FIX]

Symptom: Router will display “File size is changing: done“ everytime the router is rebooting.

Condition:

- (1) Reboot system.
- (2) Router will display “File size is changing: done” even without processing rom convert.
- (3) It happens everytime when rebooting system.

14. [ENHANCEMENT]

Add GUI for the new feature of configurable port setting. Using this new feature, users can dynamically set LAN/DMZ port roles.

Modifications in V3.62(WZ.0)b1 | 12/29/2003

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.

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.

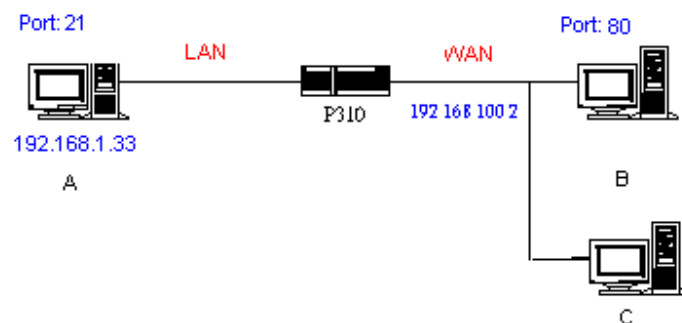
These triggered events can be timed so that they erase the port mapping as soon as they are done with the data transfer, so that the port mapping can be triggered by another Client computer. This gives the *illusion* that multiple computers can use the same port mapping at the same time, but the computers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

How to use it

Following table is a configuration table.

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

How it works



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

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

internal table for this port. (This behavior is the same as we did for port forwarding.)

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

Notes

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

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

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

There are two CI commands:

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

Example output:

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

- (2) "sys filter netbios config <type> {on|off}": To configure the filter mode for each type. Current filter types and their description are:

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

Example commands:

```
sys filter netbios config 0 on  => block LAN to WAN NBT packets  
sys filter netbios config 1 on  => block WAN to LAN NBT packets  
sys filter netbios config 6 on  => block IPSec NBT packets  
sys filter netbios config 7 off => disable trigger dial
```

Appendix 4 Traffic Redirect/Static Route Application Note

Why traffic redirect/static route be blocked by ZyWALL

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

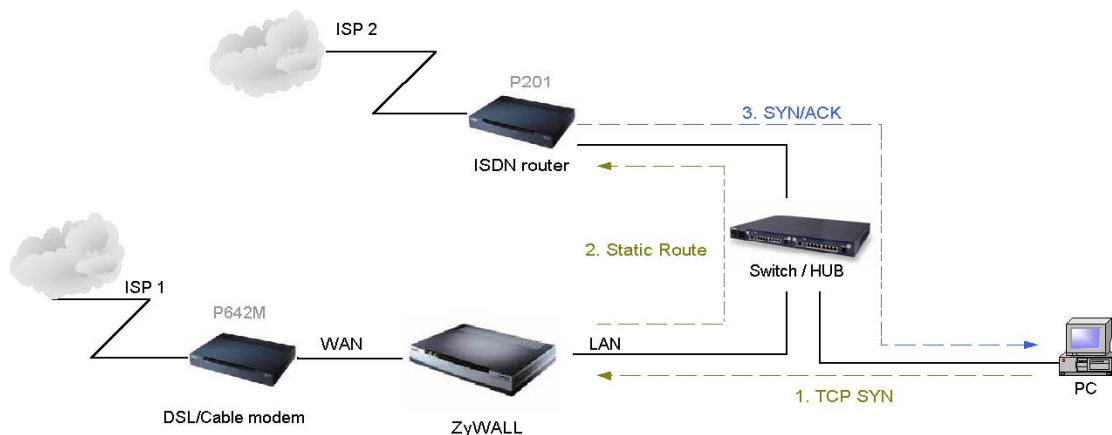


Figure 5-1 Triangle Route

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

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

That causes all of outgoing TCP traffics being reset!

How traffic redirect/static route works under protection - Solutions

(1) Gateway on alias IP network

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

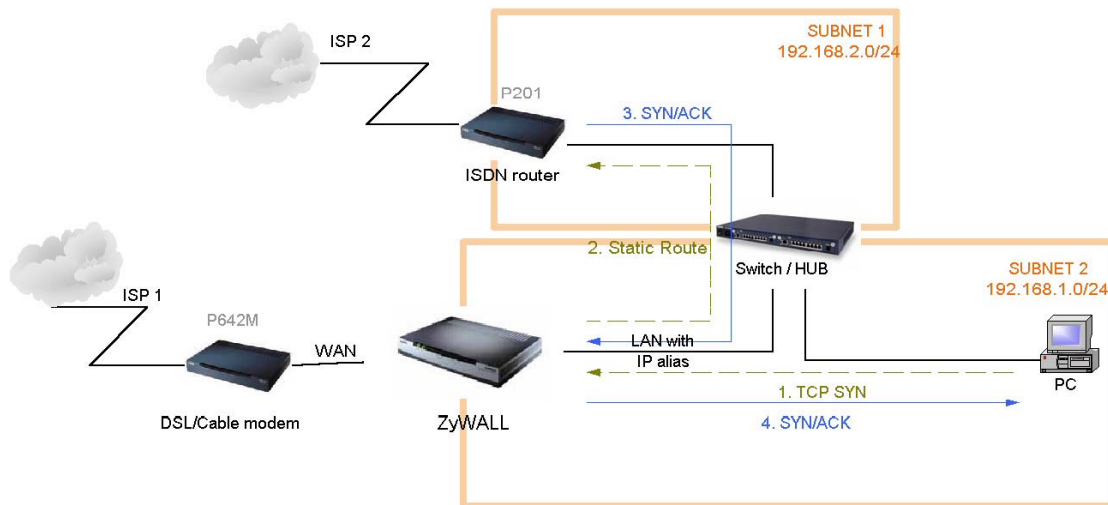


Figure 5-2 Gateway on alias IP network

(2) Gateway on WAN side

A working topology is suggested as below.

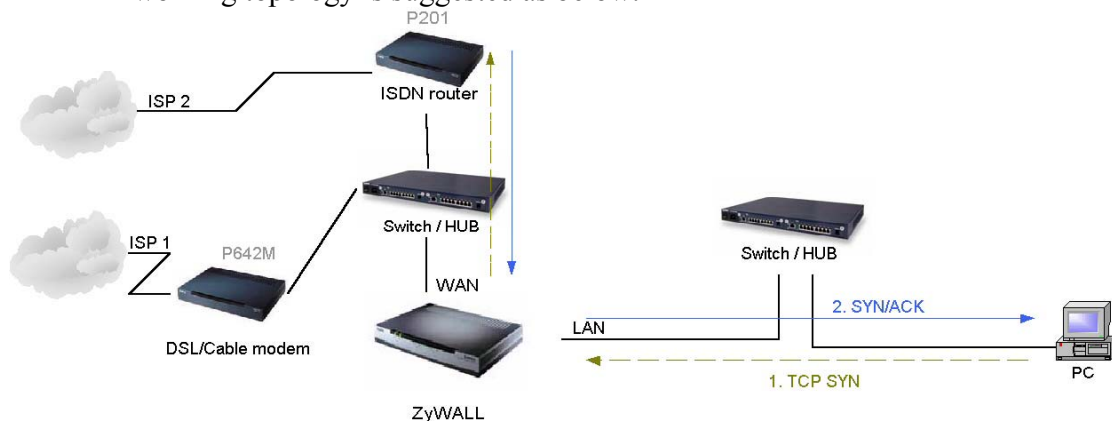


Figure 5-3 Gateway on WAN side

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.

ZyXEL Confidential

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. 2. The contents will match only if the ID content of coming packet is a.b.c.d because system will put Secure Gateway Address as Peer ID content.
a.b.c.d	e.f.g.h	1. System will check the ID type and the content. 2. The contents will match only if the ID content of coming packet is e.f.g.h.

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

Summary:

1. When Local ID Content is blank 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: 2003/11/03

Command Class List Table		
System Related Command	Exit Command	Device Related Command
Ethernet Related Command	POE Related Command	PPTP Related Command
AUX Related Command	Configuration Related Command	IP Related Command
IPSec Related Command	PPP Related Command	Bandwidth Management
Firewall Related Command	Certificate Management (PKI) Command	

System Related Command				Home
Command				Description
sys				
	adjtime			retrive date and time from Internet
	cbuf			
		display	[a f u]	display cbuf a: all f: free u: used
		cnt		cbuf static
			display	display cbuf static
			clear	clear cbuf static
	baud		<1..5>	change console speed
	callhist			
		add	<phone dir [rate] [upTime]>	add entry to call history
		display		display call history
		remove	<index>	remove entry from call history
	clear			clear the counters in GUI status menu
	clock			
		display		display system clock
	countrycode		[countrycode]	set country code
	date		[year month date]	set/display date
	debug			
		romfile		
			cert [0:reserve/1:erase]	erase all the certificates
			display	display romfile debug settings
			isp [0:reserve/1:erase]	erase the account and password of ISP
			prekey [0:reserve/1:reset]	reset the system IPSec pre-shared key
			profile [0:reserve/1:erase]	erase the accounts and passwords of 802.1X and XAUTH
			pwd [0:reserve/1:reset]	reset system password
			radius	erase Authentication and Accounting keys
			update [0:reserve/1:erase]	update romfile depend on current configuration
			wep [0:reserve/1:erase]	erase all WEP encryption keys
	dir			display file directory
	domainname			display domain name
	edit		<filename>	edit a text file
	enhanced			return OK if commands are supported for PWC purposes
	errctl		[level]	set the error control level 0:crash no save,not in debug mode (default) 1:crash no save,in debug mode 2:crash save,not in debug mode 3:crash save,in debug mode

ZyXEL Confidential

	event			
		display		display tag flags information
		trace		display system event information
			display	display trace event
			clear <num>	clear trace event
	extraphnum			maintain extra phone numbers for outcalls
		add	<set 1-3> <1st phone num> [2nd phone num]	add extra phone numbers
		display		display extra phone numbers
		node	<num>	set all extend phone number to remote node <num>
		remove	<set 1-3>	remove extra phone numbers
		reset		reset flag and mask
	feature			display feature bit
	fid			
		display		display function id list
	firmware			display ISDN firmware type
	hostname		[hostname]	display system hostname
	iface			
		disp	[#]	display iface list
	isr		[all used free]	display interrupt service routine
	interrupt			display interrupt status
	logs			
		category		
			access [0:none/1:log/2:alert/3:both]	record the access control logs
			attack [0:none/1:log/2:alert/3:both]	record and alert the firewall attack logs
			display	display the category setting
			error [0:none/1:log/2:alert/3:both]	record and alert the system error logs
			ipsec [0:none/1:log/2:alert/3:both]	record the access control logs
			ike [0:none/1:log/2:alert/3:both]	record the access control logs
			javablocked [0:none/1:log]	record the java etc. blocked logs
			mten [0:none/1:log]	record the system maintenance logs
			packetfilter [0:none/1:log]	record the packet filter logs
			pki [0:none/1:log/2:alert/3:both]	record the pki logs
			tcpreset [0:none/1:log]	record the tcp reset logs
			upnp [0:none/1:log]	record upnp logs
			urlblocked [0:none/1:log/2:alert/3:both]	record and alert the web blocked logs
			urlforward [0:none/1:log]	record web forward logs
		clear		clear log
		display	[access attack error ipsec ike javablocked mten packetfilter pki tcpreset urlblocked urlforward]	display all logs or specify category logs
		dispSvrIP		Display the IP address of email log server and syslog server
		errlog		
			clear	display log error
			disp	clear log error
			online	turn on/off error log online display
		load		load the log setting buffer
		mail		
			alertAddr [mail address]	send alerts to this mail address
			display	display mail setting
			logAddr [mail address]	send logs to this mail address
			schedule display	display mail schedule

ZyXEL Confidential

			schedule hour [0-23]	hour time to send the logs
			schedule minute [0-59]	minute time to send the logs
			schedule policy [0:full/1:hourly/2:daily/3:weekly/4:none]	mail schedule policy
			schedule week [0:sun/1:mon/2:tue/3:wed/4:thu/5:fri/6:sat]	weekly time to send the logs
			server [domainName/IP]	mail server to send the logs
			subject [mail subject]	mail subject
		save		save the log setting buffer
		syslog		
			active [0:no/1:yes]	active to enable unix syslog
			display	display syslog setting
			facility [Local ID(1-7)]	log the messages to different files
			server [domainName/IP]	syslog server to send the logs
		updateSvrIP	<minute>	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.
	map			display whole memory map content
	mbuf			
		link	link	list system mbuf link
		pool	<id> [type][num]	list system mbuf pool
		status		display system mbuf status
		disp	<address>[1/0]	display mbuf status
		cnt		
			disp	display system mbuf count
			clear	clear system mbuf count
		debug	[on/off]	
	memory		<address> <length>	display memory content
	memwrite		<address> <len> [data list ...]	write some data to memory at <address>
	memutil			
		usage		display memory allocate and heap status
		mqueue	<address> <len>	display memory queues
		mcell	mid [fu]	display memory cells by given ID
		msecs	[a fu]	display memory sections
		mtstart	<n-mcell>	start memory test
		mtstop		stop memory test
		mtalloc	<size> [n-mcell]	allocate memory for testing
		mtfree	<start-idx> [end-idx]	free the test memory
	model			display server model name
	proc			
		display		display all process information
		stack	[tag]	display process's stack by a give TAG
		pstatus		display process's status by a give TAG
	pwc			sends information to PWC via telnet
	pwderrtm		[minute]	Set or display the password error blocking timeout value.
	queue			
		display	[a fu] [start#] [end#]	display queue by given status and range numbers
		ndisp	[qid]	display a queue by a given number
	quit			quit CI command mode

ZyXEL Confidential

	reboot		[code]	reboot system code = 0 cold boot, = 1 immediately boot = 2 bootModule debug mode
	reslog			
		disp		display resources trace
		clear		clear resources trace
	rn			
		load	<entry no.>	load remote node information
		disp	<entry no.>(0:working buffer)	display remote node information
		nat	<none sua full feature>	config remote node nat
		nailup	<no yes>	config remote node nailup
		mtu	<value>	set remote node mtu
		save	[entry no.]	save remote node information
	smt			not support in this product
	stdio		[second]	change terminal timeout value
	support			not support in this product
	time		[hour [min [sec]]]	display/set system time
	timer			
		disp		display timer cell
		trace	[on off]	set/display timer information online
		start	[tmValue]	start a timer
		stop	<ID>	stop a timer
	tos			
		display		display all runtime TOS
		listPerHost		display all host session count
		debug	[on off]	turn on or off TOS debug message
		dump	<session>	dump session information
		sessPerHost	<number>	configure session per host value
		tcprst	<session>	send TCP RST to both source and dest IP
		timeout		
			display	display all TOS timeout information
			icmp <idle timeout>	set idle timeout value
			igmp <idle timeout>	set idle timeout value
			tcpsyn <idle timeout>	set idle timeout value
			tcp <idle timeout>	set idle timeout value
			tcpfin <idle timeout>	set idle timeout value
			udp <idle timeout>	set idle timeout value
			gre <idle timeout>	set idle timeout value
			esp <idle timeout>	set idle timeout value
			ah <idle timeout>	set idle timeout value
			other <idle timeout>	set idle timeout value
	trcdisp	parse, brief, disp		monitor packets
	trclog			
		switch	[on off]	set system trace log
		online	[on off]	set on/off trace log online
		level	[level]	set trace level of trace log #:1-10
		type	<bitmap>	set trace type of trace log
		disp		display trace log
		clear		clear trace
		call		display call event
		encapmask	[mask]	set/display tracelog encapsulation mask
	trcpacket			

ZyXEL Confidential

		create	<entry> <size>	create packet trace buffer
		destroy		packet trace related commands
		channel	<name> [none incoming outgoing bothway]	<channel name>=enet0,sdsl00, fr0 set packet trace direction for a given channel
		string		enable smt trace log
		switch	[on off]	turn on/off the packet trace
		disp		display packet trace
		udp		send packet trace to other system
			switch [on off]	set tracepacket upd switch
			addr <addr>	send trace packet to remote udp address
			port <port>	set tracepacket udp port
		parse	[[start_idx], end_idx]	parse packet content
		brief		display packet content briefly
	syslog			
		server	[destIP]	set syslog server IP address
		facility	<FacilityNo>	set syslog facility
		type	[type]	set/display syslog type flag
		mode	[on off]	set syslog mode
	version			display RAS code and driver version
	view		<filename>	view a text file
	wdog			
		switch	[on off]	set on/off wdog
		cnt	[value]	display watchdog counts value: 0-34463
		dead		let watch dog take place using while loop
	romreset			restore default romfile
	mrd			
		atwe	<mac> [country code] [debug flag] [featurebit]	configure mac, country code, debug flag, featurebit in the boot module
		atse		generate the engineering debug flag password seed
		aten	<password>	enter the engineering debug flag password
		atfl	<0:1>	set engineering debug flag
		atsh		show mrd setting
	server			
		access	<telnet ftp web icmp snmp dns> <value>	set server access type
		load		load server information
		disp		display server information
		port	<telnet ftp web snmp> <port>	set server port
		save		save server information
		secureip	<telnet ftp web icmp snmp dns> <ip>	set server secure ip addr
		certificate	<https ssh> [certificate name]	set server certificate
		auth_client	<https> [on off]	specifies whether the server authenticates the client
	fwnotify			
		load		load fwnotify entry from spt
		save		save fwnotify entry to spt
		url	<url>	set fwnotify url
		days	<days>	set fwnotify days
		active	<flag>	turn on/off fwnotify flag
		disp		display firmware notify information
		check		check firmware notify event
		debug	<flag>	turn on/off firmware notify debug flag
	spt			

ZyXEL Confidential

		dump		dump spt raw data
			root	dump spt root data
			rn	dump spt remote node data
			user	dump spt user data
			slot	dump spt slot data
		set	<offset> <len> <value...>	set spt value in memory address
		save		save spt data
		size		display spt record size
		clear		clear spt data
	cmgr			
		trace		
			disp <ch-name>	show the connection trace of this channel
			clear <ch-name>	clear the connection trace of this channel
		data	<ch-name>	show channel connection related data
		cnt	<ch-name>	show channel connection related counter
	socket			display system socket information
	filter			
		clear		clear filter statistic counter
		disp		display filter statistic counters
		sw	[on off]	set filter status switch
		rule	<iface>	display iface filter flag
		set	<set>	display filter rule
		addNetBios		add netbios filter
		removeNetBios		remove netbios filter
		netbios		
			disp	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>	config netbios filter
		blockbc	[on off]	set/display broadcast filter mode
	roadrunner			
		debug	<level>	enable/disable roadrunner service 0: diable <default> 1: enable
		display	<iface name>	display roadrunner information iface-name: enif0, wanif0
		restart	<iface name>	restart roadrunner
		logout	<iface name>	logout roadrunner
		set	<iface name>	set roadrunner
	ddns			
		debug	<level>	enable/disable ddns service
		display	<iface name>	display ddns information
		restart	<iface name>	restart ddns
		logout	<iface name>	logout ddns
	cpu			
		display		display CPU utilization
	upnp			
		active	[0:no/1:yes]	Activate or deactivate the saved upnp settings
		config	[0.deny/1:permit]	Allow users to make configuration changes. through UPnP
		display		display upnp information
		firewall	[0:deny/1:pass]	Allow UPnP to pass through Firewall.
		load		save upnp information

ZyXEL Confidential

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

Exit Command

[Home](#)

Command				Description
exit				exit smt menu

Device Related Command

[Home](#)

Command				Description
dev				
	channel			
		name	<all use>	list channel name
		drop	<channel_name>	drop channel
		disp	<channel_name> [level]	display channel
		threshold	<channel_name> [number]	set channel threshold
	dial		<node#>	dial to remote node

Ethernet Related Command

[Home](#)

Command				Description
ether				
	config			display LAN configuration information
	driver			
		cnt		
		disp <name>		display ether driver counters
		clear <name>		clear ether driver counters
		iface	<ch_name> <num>	send driver iface
		ioctl	<ch_name>	Useless in this stage.
		mac	<ch_name> <mac_addr>	Set LAN Mac address
		reg	<ch_name>	display LAN hardware related registers
		rxmod	<ch_name> <mode>	set LAN receive mode. mode: 1: turn off receiving 2: receive only packets of this interface 3: mode 2+ broadcast 5: mode 2 + multicast 6: all packets
		status	<ch_name>	see LAN status
		init	<ch_name>	initialize LAN
	version			see ethernet device type
	pkttest			
		disp		
		packet <level>		set ether test packet display level
		event <ch> [on off]		turn on/off ether test event display
		sap	[ch_name]	send sap packet
		arp	<ch_name> <ip-addr>	send arp packet to ip-addr
		mem	<addr> <data> [type]	write memory data in address
	test		<ch_id> <test_id> [arg3] [arg4]	do LAN test
	ipmul		<num>	only receive ip multicast and broadcast packet
	pncconfig		<ch_name>	do pnc config
	mac		<src_ch> <dest_ch> <ipaddr>	fake mac address
	debug			
		disp	<ch_name>	display ethernet debug infomation

ZyXEL Confidential

		reset	<ch_name>	reset ethernet debug state
		create	<ch_name> <num>	create ethernet debug state
		destory	<ch_name>	destory ethernet debug state
		level	<ch_name> <level>	set the ethernet debug level level 0: disable debug log level 1:enable debug log (default)
	edit			
		load	<ether no.>	load ether data from spt
		mtu	<value>	set ether data mtu
		speed	<speed>	set ether data speed
		save		save ether data to spt

POE Related Command

[Home](#)

Command				Description
poe				
	debug		[on off]	switch poe debug
	retry			
		count	[count]	set/display poe retry count
		interval	[interval]	set/display poe retry interval
	status		[ch_name]	see poe status
	master			
		promiscuous	[on off]	provide pppoe server list to client
		easy	[on off]	response for no service name request
	service			
		add	<service-name>	add poe service
		show		show poe service
	dial		<node>	dial a remote node
	drop		<node>	drop a pppoe call
	channel			
		enable	<channel>	enable a channel to carry pppoe traffic
		disable	<channel>	disable a pppoe channel
		show		show pppoe channel
	padt		[limit]	set/display pppoe PADT limit
	inout		<node name>	set call direction to both
	ippool		[ip] [cnt]	set/display pppoe ippool information
	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

[Home](#)

Command				Description
pptp				
	debug		[on off]	switch pptp debug flag
	dial		<rn-name>	dial a remote node
	drop		<rn-name>	drop a remote node call
	tunnel		<tunnel id>	display pptp tunnel information
	window		[size]	set pptp data rx-window-size
	rxTimeout		[timeout]	set pptp data rx-timeout
	queue		[size]	set pptp data tx-queue-size

	enqueue		[size]	set pptp max en-queued size
--	---------	--	--------	-----------------------------

AUX Related Command

[Home](#)

Command				Description
aux				
	atring		<device name>	Command the AT command to the device.
	clearstat		<device name>	reset channel statistics
	cnt			
		disp	<device name>	display aux counter information
		clear	<device name>	clear aux counter information
	cond			
		disp	<device name>	display aux condition information
		clear	<device name>	clear aux condition information
	config			display aux config, board, line, channel information
	data			
		disp		display TX session information
		send	<device name> <pkt size> <interval(ms)> <count>	start TX session
		stat	<device name>	display data statistic from TX session
		stop	<session>	stop a TX session
	dial		<device name> <phone number>	begin dialing
	disp		<device name>	displays ndis's copy of a channel's spt profile
	dqtest		<device name> <command>	send AT command
	drop		<device name>	disconnect
	dump		<start#> <display#>	dump aux debug information
	st		<start#> <display#>	dump aux state
	event			
		disp		aux event trace display
		clear		aux event trace clear
	init		<device name>	initialize aux channel
	is		<device name>	send event to in-service
	mbuf		<index>	dump mbuf information
	mem		<addr> <data> [type]	write data at addr in memory
	mode		<device name> [mode]	set mode
	mstatus		<device name>	display modem last call status
	mttype		<device name>	display modem type
	netstat		<device name>	prints upper layer packet information
	oos		<device name>	send event to out-of-service
	prtl		<device name> <level>	set display level
	rate		<device name>	show tx rx rate
	read		<device name>	read spt from ROM and copy to ndis's copy
	redirect		<device name>	invalid
	ringbuf			
		cmd		
			clear <device name>	clear ringbuffer
			disp <device name>	display ringbuffer
		data		
			clear	clear command ringbuffer
			disp <start> <len>	display command ringbuffer
	save		<device name>	save aux information
	set		<device name> <field> <value>	set aux information
	signal		<device name>	show aux signal

	speed		<device name> <type> [value]	display/set aux speed
	test		<device name> <type>	test aux channel
	version			invalid

Configuration Related Command

[Home](#)

Command					Description
config					The parameters of config are listed below.
edit	firewall	active <yes no>			Activate or deactivate the saved firewall settings
retrieve	firewall				Retrieve current saved firewall settings
save	firewall				Save the current firewall settings
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
		e-mail	mail-server <mail server IP>		Edit the mail server IP to send the alert
			return-addr <e-mail address>		Edit the mail address for returning an email alert
			e-mail-to <e-mail address>		Edit the mail address to send the alert
			policy <full hourly daily weekly>		Edit email schedule when log is full or per hour, day, week.
			day <sunday monday tuesday wednesday thursday friday saturday>		Edit the day to send the log when the email policy is set to Weekly
			hour <0~23>		Edit the hour to send the log when the email policy is set to daily or weekly
			minute <0~59>		Edit the minute to send to log when the email policy is set to daily or weekly
			Subject <mail subject>		Edit the email subject
		attack	send-alert <yes no>		Activate or deactivate the firewall DoS attacks notification emails
			block <yes no>		Yes: Block the traffic when exceeds the tcp-max-incomplete threshold
					No: Delete the oldest half-open session when exceeds the tcp-max-incomplete threshold
			block-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-		The threshold to stop deleting the half-opened

ZyXEL Confidential

			low <0~255>		session
			tcp-max-incomplete <0~255>		The threshold to start executing the block field
		set <set#>	name <desired name>		Edit the name for a set
			default-permit <forward block>		Edit whether a packet is dropped or allowed when it does not match the default set
			icmp-timeout <seconds>		Edit the timeout for an idle ICMP session before it is terminated
			udp-idle-timeout <seconds>		Edit the timeout for an idle UDP session before it is terminated
			connection-timeout <seconds>		Edit the wait time for the SYN TCP sessions before it is terminated
			fin-wait-timeout <seconds>		Edit the wait time for FIN in concluding a TCP session before it is terminated
			tcp-idle-timeout <seconds>		Edit the timeout for an idle TCP session before it is terminated
			pnc <yes no>		PNC is allowed when 'yes' is set even there is a rule to block PNC
			log <yes no>		Switch on/off sending the log for matching the default permit
			logone <yes no>		Switch on/off for one packet that create just one log message.
			rule <rule#>	permit <forward block>	Edit whether a packet is dropped or allowed when it matches this rule
				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
delete	firewall	e-mail			Remove all email alert settings
		attack			Reset all alert settings to defaults
		set <set#>			Remove a specified set from the firewall configuration
		set <set#>	rule <rule#>		Remove a specified rule in a set from the firewall configuration
insert	firewall	e-mail			Insert email alert settings
		attack			Insert attack alert settings
		set <set#>			Insert a specified rule set to the firewall configuration
		set <set#>	rule <rule#>		Insert a specified rule in a set to the firewall configuration
cli					Display the choices of command list.
debug	<1 0>				Turn on/off trace for firewall debug information.

IP Related Command

[Home](#)

Command				Description
ip				
	address		[addr]	display host ip address
	alias		<iface>	alias iface
	aliasdis		<0 1>	disable alias
	arp			
		status	<iface>	display ip arp status
		add	<hostid> ether <ether addr>	add arp information
		resolve	<hostid>	resolve ip-addr
		replydif	[<0:No 1:yes>]	reply different interface ip-addr's arp request
		drop	<hostid> [hardware]	drop arp
		flush		flush arp table
		publish		add proxy arp
	dhcp		<iface>	
		client		
			release	release DHCP client IP
			renew	renew DHCP client IP
		mode	<server relay none client>	set dhcp mode
		relay	server <serverIP>	set dhcp relay server ip-addr
		reset		reset dhcp table
		server		
			probecount <num>	set dhcp probe count
			dnsserver <IP1> [IP2] [IP3]	set dns server ip-addr
			winsserver <winsIP1> [<winsIP2>]	set wins server ip-addr
			gateway <gatewayIP>	set gateway
			hostname <hostname>	set hostname
			initialize	fills in DHCP parameters and initializes (for PWC purposes)
			leasetime <period>	set dhcp leasetime
			netmask <netmask>	set dhcp netmask

ZyXEL Confidential

			pool <startIP> <numIP>	set dhcp ip pool
			renewaltime <period>	set dhcp renew time
			rebindtime <period>	set dhcp rebind time
			reset	reset dhcp table
			server <serverIP>	set dhcp server ip for relay
			dnsorder [router isp]	set dhcp dns order
			release <entry num>	release specific entry of the dhcp server pool
		status	[option]	show dhcp status
		static		
			Delete <num> all	delete static dhcp mac table
			display	display static dhcp mac table
			update <num> <mac> <ip>	update static dhcp mac table
	dns			
		query		
			address <ipaddr> [timeout]	resolve ip-addr to name
			Debug <num>	enable dns debug value
			Name <hostname> [timeout]	resolve name to multiple IP addresses
			Status	display dns query status
			Table	display dns query table
		server	<primary> [secondary] [third]	set dns server
		stats		
			Clear	clear dns statistics
			Disp	display dns statistics
		table		display dns table
		default	<ip>	Set default DNS server
	Httpd			
		debug	[on off]	set http debug flag
	icmp			
		echo	[on off]	set icmp echo response flag
		data	<option>	select general data type
		check		
			cmd [on off]	check icmp echo reply command data
			rsp [on off]	check icmp response
			indication [i r l p]	set icmp indication
		status		display icmp statistic counter
		trace	[on off]	turn on/off trace for debugging
		discovery	<iface> [on off]	set icmp router discovery flag
	ifconfig		[iface] [ipaddr] [broadcast <addr> mtu <value> dynamic]	configure network interface
	ping		<hostid>	ping remote host
	pong		<hostid> [<size> <time-interval>]	pong remote host
	route			
		status	[if]	display routing table
		add	<dest_addr default>[/<bits>] <gateway> [<metric>]	add route
		addiface	<dest_addr default>[/<bits>] <gateway> [<metric>]	add an entry to the routing table to iface
		addprivate	<dest_addr default>[/<bits>] <gateway> [<metric>]	add private route
		drop	<host addr> [/<bits>]	drop a route
		flush		flush route table
		lookup	<addr>	find a route to the destination
		errcnt		
			disp	display routing statistic counters

ZyXEL Confidential

		clear	clear routing statistic counters
smtp			
	server	[addr]	set smtp server
	destmail	[addr]	set destination mail addr
	srcmail	[addr]	set source mail addr
	sendmail		send mail
	addrlist		list smtp server, dest, return addr
	addrreset		reset smtp server, dest, return addr
status			display ip statistic counters
stroute			
	display	[rule # buf]	display rule index or detail message in rule.
	load	<rule #>	load static route rule in buffer
	save		save rule from buffer to spt.
	config		
		name <site name>	set name for static route.
		destination <dest addr>[/<bits>] <gateway> [<metric>]	set static route destination address and gateway.
		mask <IP subnet mask>	set static route subnet mask.
		gateway <IP address>	set static route gateway address.
		metric <metric #>	set static route metric number.
		private <yes no>	set private mode.
		active <yes no>	set static route rule enable or disable.
adjTcp		<iface> [<mss>]	adjust the TCP mss of iface
adjmss		[mss]	adjust all system TCP mss of iface
udp			
	status		display udp status
rip			
	accept	<gateway>	drop an entry from the RIP refuse list
	activate		enable rip
	merge	[on/off]	set RIP merge flag
	refuse	<gateway>	add an entry to the rip refuse list
	request	<addr> [port]	send rip request to some address and port
	reverse	[on/off]	RIP Poisoned Reverse
	status		display rip statistic counters
	trace		enable debug rip trace
	mode		
		<iface> in [mode]	set rip in mode
		<iface> out [mode]	set rip out mode
	dialin_user	[show in out both none]	show dialin user rip direction
sidepath			
	clear		clear side path
	disp		display side path
	set	<iface> <gateway>	set side path
tcp			
	ceiling	[value]	TCP maximum round trip time
	floor	[value]	TCP minimum rtt
	irtt	[value]	TCP default init rtt
	kick	<tc>	kick tcb
	limit	[value]	set tcp output window limit
	max-incomplete	[number]	Set the maximum number of TCP incomplete connection.
	mss	[value]	TCP input MSS
	reset	<tc>	reset tcb
	rtt	<tc> <value>	set round trip time for tcb

ZyXEL Confidential

		status	[tcb] [<interval>]	display TCP statistic counters
		syndata	[on/off]	TCP syndata piggyback
		trace	[on/off]	turn on/off trace for debugging
		window	[tcb]	TCP input window size
	samenet		<iface1> [<iface2>]	display the ifaces that in the same net
	uninet		<iface>	set the iface to uninet
	telnet		<host> [port]	execute telnet clinet command
	tftp			
		support		pritr if tfpt is support
		stats		display tftp status
	tracroute		<host> [ttl] [wait] [queries]	send probes to trace route of a remote host
	xparent			
		join	<iface1> [<iface2>]	join iface2 to iface1 group
		break	<iface>	break iface to leave ipxparent group
	anitprobe		<0 1> 1:yes 0:no	set ip anti-probe flag
	forceproxy		<display/set> [on/off] [servicePort] [proxyIp] [proxyport]	enable TCP forceproxy
	ave			anti-virus enforce
	urlfilter			
		enable		enable/disable url filter function
		reginfo		
			display	display urlfilter registration information
			name	set urlfilter registration name
			eMail <size>	set urlfilter registration email addr
			country <size>	set urlfilter registration country
			clearAll	clear urlfilter register information
		category		
			display	display urlfilter category
			webFeature [block/nonblock] [activex/java/cookei/webproxy]	block or unblock webfeature
			logAndBlock [log/logAndBlock]	set log only or log and block
			blockCategory [block/nonblock] [all/type(1-14)]	block or unblock type
			timeOfDay [always/hh:mm] [hh:mm]	set block time
			clearAll	clear all category information
		listUpdate		
			display	display listupdate status
			actionFlags [yes/no]	set listupdate or not
			scheduleFlag [pending]	set schedule flag
			dayFlag [pending]	set day flag
			time [pending]	set time
			clearAll	clear all listupdate information
		exemptZone		
			display	display exemptzone information
			actionFlags [type(1-3)][enable/disable]	set action flags
			add [ip1] [ip2]	add exempt range
			delete [ip1] [ip2]	delete exempt range
			reset	clear exemptzone information
		customize		
			display	display customize action flags
			actionFlags [filterList/disableAllExceptTrusted/	set action flags

ZyXEL Confidential

			unblockRWFTToTrusted/keywordBlock/fullPath/caseInsensitive/fileName][enable/disable]	
			logFlags [type(1-3)][enable/disable]	set log flags
			add [string] [trust/untrust/keyword]	add url string
			delete [string] [trust/untrust/keyword]	delete url string
			reset	clear all information
		logDisplay		display cyber log
		ftplist		update cyber list data
		listServerIP	<ipaddr>	set list server ip
		listServerName	<name>	set list server name
		general		
			enable	enable/disable url filter function
			display	display content filter's general setting
			webFeature	[block/nonblock] [activex/java/cookei/webproxy]
			timeOfDay[always/hh:mm] [hh:mm]	set block time
			exemptZone display	display exemptzone information
			exemptZone actionFlags [type(1-3)][enable/disable]	set action flags
			exemptZone add [ip1] [ip2]	add exempt range
			exemptZone delete [ip1] [ip2]	delete exempt range
			exemptZone reset	clear exemptzone information
			reset	reset content filter's general setting
		webControl		
			enable	enable cbr filter
			display	display cbr filter's setting
			logAndBlock [log/block/both]	set log or block on matched web site
			category	set blocked categories
			serverList display	display current cbr filter servers
			serverList refresh	refresh cbr filter servers
			queryURL [url][Server/localCache]	query url need to block or forward according the database on server or local cache
			cache display	display the local cache entries
			cache delete [entrynum/All]	delete the local cache entries
			blockonerror [log/block][on/off]	choose log or block when server is unavailable
			waitingTime [sec]	set waiting time for server
			reginfo display	display the license key with cerberian
			reginfo	No used
			zssw	change the zssw's URL
	tredir			
		failcount	<count>	set tredir failcount
		partner	<ipaddr>	set tredir partner
		target	<ipaddr>	set tredir target
		timeout	<timeout>	set tredir timeout
		checktime	<period>	set tredir checktime
		active	<on/off>	set tredir active
		save		save tredir information
		disp		display tredir information
		debug	<value>	set tredir debug value
	rpt			
		start		start report
		stop		stop report

ZyXEL Confidential

		url	[num]	top url hit list
		ip	[num]	top ip addr list
		srv	[num]	top service port list
	dropIcmp		[0 1]	to drop ICMP fragment packets
	nat			
		period	[period]	set nat timer period
		port	[port]	set nat starting external port number
		checkport		verify all server tables are valid
		timeout		
			gre [timeout]	set nat gre timeout value
			iamt [timeout]	set nat iamt timeout value
			generic [timeout]	set nat generic timeout value
			reset [timeout]	set nat reset timeout value
			tcp [timeout]	set nat tcp timeout value
			tcpother [timeout]	set nat tcp other timeout value
			udp [port] <value>	set nat udp timeout value of specific port
		update		create nat system information from spSysParam
		iamt	<iface>	display nat iamt information
		iface	<iface>	show nat status of an interface
		lookup	<rule set>	display nat lookup rule
		new-lookup	<rule set>	display new nat lookup rule
		loopback	[on off]	turn on/off nat loopback flag
		reset	<iface>	reset nat table of an iface
		server		
			disp	display nat server table
			load <set id>	load nat server information from ROM
			save	save nat server information to ROM
			clear <set id>	clear nat server information
			edit active <yes no>	set nat server edit active flag
			edit svrport <start port> [end port]	set nat server server port
			edit intport <start port> [end port]	set nat server forward port
			edit remotehost <start ip> [end ip]	set nat server remote host ip
			edit leasetime [time]	set nat server lease time
			edit rulename [name]	set nat server rule name
			edit forwardip [ip]	set nat server server ip
			edit protocol [protocol id]	set nat server protocol
			edit clear	clear one rule in the set
		service		
			irc [on off]	turn on/off irc flag
			xboxlive [on off]	turn on/off xboxlive flag
		resetport		reset all nat server table entries
		incikeport	<iface>[on off]	turn on/off increase ike port flag
		session	[session per host]	set nat session per host value
		deleteslot	<iface> <slot>	delete specific slot of iface
		debug		
			natTraversal [on off]	set NAT traversal debug flag
			hash [on off]	set NAT hash table debug flag
			session [on off]	set NAT session debug flag
		hashtable	<enifX, X=0, 1, 2, ...>	show the NAT hash table of enifX
	igmp			
		debug	[level]	set igmp debug level
		forwardall	[on off]	turn on/off igmp forward to all interfaces flag
		querier	[on off]	turn on/off igmp stop query flag
		iface		

			<iface> group tm <timeout>	set igmp group timeout
			<iface> interval <interval>	set igmp query interval
			<iface> join <group>	join a group on iface
			<iface> leave <group>	leave a group on iface
			<iface> query	send query on iface
			<iface> rsptime [time]	set igmp response time
			<iface> start	turn on of igmp on iface
			<iface> stop	turn off of igmp on iface
			<iface> ttl <threshold>	set ttl threshold
			<iface> v1compat [on/off]	turn on/off v1compat on iface
		robustness	<num>	set igmp robustness variable
		status		dump igmp status
	pr			
		clear		clear ip pr table counter information
		disp		display policy route set and rule information
		move		move specific policy route rule to another rule
		dispCnt		dump ip pr table counter information
		switch		turn on/off ip pr table counter flag

IPSec Related Command

[Home](#)

Command				Description
ipsec				
	debug	<1 0>		turn on/off trace for IPsec debug information
	ipsec_log_disp			show IPsec log, same as menu 27.3
	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.
				Remark: Command available since 3.50(WA.3)
	show_runtime	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.
	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_my_ip	<1~3600>	- Adjust timer to check if WAN IP in menu is changed
				- Interval is in seconds
				- Default is 10 seconds
				- 0 is not a valid value
		chk_conn.	<0~255>	- Adjust auto-timer to check if any IPsec

ZyXEL Confidential

				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
				Remark: Command available since 3.50(WA.3)
	updatePeerIp			Force system to update IPSec rules which use domain name as the secure gateway IP right away.
				Remark: Command available since 3.50(WA.3)
	dial	<rule #>		Initiate IPSec rule <#> from ZyWALL box
				Remark: Command available since 3.50(WA.3)
	display	<rule #>		Display IPSec rule #
	remote	key	<string>	I add a secured remote access tunnel with pre-shared key. It is a dynamic rule with local: the route's WAN IP. The algorithms with it are fixed to phase1: DES+MD5, DH1 and SA lifetime 28800 seconds; phase2: DES+MD5, PFS off, no anti-replay and SA lifetime 28800 seconds. The length of pre-shared key is between 8 to 31 ASCII characters.
		switch	<on off>	Activate or de-activate the secured remote access tunnel.
	keep_alive	<rule #>	<on off>	Set ipsec keep_alive flag
	load	<rule #>		Load ipsec rule
	save			Save ipsec rules
	config	netbios	active <on off>	Set netbios active flag
			group <group index1, group index2...>	Set netbios group
		name	<string>	Set rule name
		active	<Yes No>	Set active or not
		keepAlive	<Yes No>	Set keep alive or not
		natTraversal	<Yes No>	Enable NAT traversal or not.
		localIdType	<0:IP 1:DNS 2:Email>	Set local ID type
		localIdContent	<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
		protocol	<1:ICMP 6:TCP 17:UDP>	Set protocol
		localAddrType	<0:single 1:range 2:subnet>	Set local address type
		localAddrStart	<IP>	Set local start address

ZyXEL Confidential

		lcAddrEndMask	<IP>	Set local end address or mask
		lcPortStart	<port>	Set local start port
		lcPortEnd	<port>	Set local end port
		dnsServer	<IP>	Set DNS server for IPSec VPN
		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
		antiReplay	<Yes No>	Set antireplay or not
		keyManage	<0:IKE 1:Manual>	Set key manage
		ike	negotiationMode <0:Main 1:Aggressive>	Set negotiation mode in phase 1 in IKE
			authMethod <0:PreSharedKey 1:RSASignature>	Set authentication method in phase 1 in IKE
			preShareKey <string>	Set pre shared key in phase 1 in IKE
			certFile <FILE>	Set certificate file if using RSA signature as authentication method.
			p1EncryAlgo <0:DES 1:3DES>	Set encryption algorithm in phase 1 in IKE
			p1AuthAlgo <0:MD5 1:SHA1>	Set authentication algorithm in phase 1 in IKE
			p1SaLifeTime <seconds>	Set sa life time in phase 1 in IKE
			p1KeyGroup <0:DH1 1:DH2>	Set key group in phase 1 in IKE
			activeProtocol <0:AH 1:ESP>	Set active protocol in phase 2 in IKE
			p2EncryAlgo <0:Null 1:DES 2:3DES>	Set encryption algorithm in phase 2 in IKE
			p2AuthAlgo <0:MD5 1:SHA1>	Set authentication algorithm in phase 2 in IKE
			p2SaLifeTime <seconds>	Set sa life time in phase 2 in IKE
			encap <0:Tunnel 1:Transport>	set encapsulation in phase 2 in IKE
			pfs <0:None 1:DH1 2:DH2>	set pfs in phase 2 in IKE
		manual	activeProtocol <0:AH 1:ESP>	Set active protocol in manual
		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
		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
	swSkipOverlapp		<on/off>	<ul style="list-style-type: none"> - When a VPN rule with remote range overlaps with local range, the switch decides if a local to local packet should apply this rule. - Default value is “off” which means “no skip”.
	adjTcpMss		<off auto user defined value>	<ul style="list-style-type: none"> - After a tunnel is established, system will automatically adjust TCP MSS. - After all tunnels are drops, the MSS will adjust to the original value. - The default value is auto.

Command				Description
ppp				
	bod			
		remote	<i>iface</i>	show remote bod information
		reset		reset bod
		setremote	<i>iface</i>	set remote bod
		status	<wan i>face</i>	show wan port bod status
		clear	<wan i>face</i>	clear wan port bod data
		on		set bod flag on
		off		set bod flag off
		node	<node> <dir>	config the statistic method for remote node bod traffic data
		debug	[on off]	show bod debug flag
		cnt		
			disp	show bod state
			clear	clear bod state
	ccp		[on off]	set/display dial-in ccp switch
	lcp			
		acfc	[on off]	set address/control field compression flag
		pfc	[on off]	set protocol field compression flag
		mpin	[on off]	set incoming call MP flag
		callback	[on off]	set callback flag
		bacp	[on off]	set bandwidth allocation control flag
		echo		
			retry <retry count>	set/display retry count to send echo-request
			time <interval>	set/display time interval to send echo-request
	ipcp			
		close		close connection on ppp interface
		list	<i>iface</i>	show ipcp state
		open		open fsm link
		timeout	[value]	set timeout interval when waiting for response from remote peer
		try		
			configure [value]	set/display fsm try config
			failure [value]	set/display fsm try failure
			terminate [value]	set/display fsm try terminate
		compress	[on off]	set compress flag
		slots	[slot num]	set number of slots
		idcompress	[on off]	set/display slot id compress
		address	[on off]	set/display ip one address option
	mp			
		default		show link default flag
			rotate	set link default to rotate
			split	set link default to split
		split	[0 1]	set/display link split
		rotate	[0 1]	set/display link rotate
		sequence		set/display mp start sequence
	configure			
		ipcp		
			compress [on off]	enable/disable compress
			slots [slot num]	select number of slots
			idcompress [on off]	enable/disable slot id compress

		address [on/off]	set/display ip one address option
	atcp		apple talk feature not supported anymore
	ccp		
		ascend [on/off]	set/display ascend stac flag
		history <count>	set/display stac history count
		check [argv]	set/display stac check mode
		reset <mode>	set/display stac reset mode
		pfc [on/off]	set/display pfc flag
		debug [on/off]	set/display ccp debug flag
iface			
		<iface> ipcp	show the ipcp status of the given iface
		<iface> ipxcp	show the ipxcp status of the given iface
		<iface> atcp	
		<iface> ccp [reset skip flush]	show the ccp status of the given iface
		<iface> mp	show the mp status of the given iface
show		<channel>	show the ppp channel status
fsm			
	trace		
		break [num] [count] [flag]	set the fsm log break value
		clear	clear the fsm log data
		disp	display the fsm log data
		filter [mask] [protocol]	set the fsm log filter value
	tdata		
		filter [protocol1] [protocol2] ...	set the fsm filter data
		disp	display the fsm data
		clear	clear the fsm data
	struc		dump fsm data structure
delay		[interval]	set the delay timer for sending first PPP packet after call answered

Firewall Related Command

[Home](#)

Command				Description
sys	Firewall			
		acl		
			disp	Display specific ACL set # rule #, or all ACLs.
			delete	Delete specific ACL set # rule #.
		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.
		debug		Set firewall debug level.
		disp		Display firewall log
		init		### nothing. ###
		mailsubject		
			disp	Display mail setting which is used to mail alert.
			edit	Edit mail setting.
		online		Set firewall log online.
		pktdump		Dump the 64 bytes of dropped packet by firewall
		tos		
			delete	Delete specific TOS session.

ZyXEL Confidential

			display		Display TOS sessions.
			status		Display TOS sessions' status.
			dump		Dump TOS.
		tosctrl			
			destination		Display TOS destination hash
			incomplete		Display TOS incomplete List.
		dynamicrule			
			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			
			dos		Set if firewall ignore DoS in lan/wan/dmz/wlan
			triangle		Set if firewall ignore triangle route in lan/wan/dmz/wlan
		schedule			
			load [set # rule #]		Load firewall ACL schedule by rule.
			display		Display ACL schedule in buffer.
			save		Save buffer date and update runtime firewall ACL rule.
			week		
				monday [on/off]	Set schedule on or off by day – Monday.
				tuesday [on/off]	Set schedule on or off by day – Tuesday.
				wednesday [on/off]	Set schedule on or off by day – Wednesday.
				thursday [on/off]	Set schedule on or off by day – Thursday.
				friday [on/off]	Set schedule on or off by day – Friday.
				saturday [on/off]	Set schedule on or off by day – Saturday.
				sunday [on/off]	Set schedule on or off by day – Sunday.
				allweek [on/off]	Quick set schedule on or off by week.
			timeOfDay [always/hh: mm]		Set firewall ACL schedule block time of day.

Certificate Management (PKI) Command

[Home](#)

Command				Description
certificates				
	my_cert			
		create		
			selfsigned <name> <subject> [key size]	Create a self-signed local host certificate. <name> specifies a descriptive name for the generated certificate. <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn;{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024

				bits.
			request <name> <subject> [key size]	Create a certificate request and save it to the router for later manual enrollment. <name> specifies a descriptive name for the generated certification request. <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn; {ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.
			scep_enroll <name> <CA addr> <CA cert> <auth key> <subject> [key size]	Create a certificate request and enroll for a certificate immediately online using SCEP protocol. <name> specifies a descriptive name for the enrolled certificate. <CA addr> specifies the CA server address. <CA cert> specifies the name of the CA certificate. <auth key> specifies the key used for user authentication. If the key contains spaces, please put it in quotes. To leave it blank, type "". <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn; {ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.
			cmp_enroll <name> <CA addr> <CA cert> <auth key> <subject> [key size]	Create a certificate request and enroll for a certificate immediately online using CMP protocol. <name> specifies a descriptive name for the enrolled certificate. <CA addr> specifies the CA server address. <CA cert> specifies the name of the CA certificate. <auth key> specifies the id and key used for user authentication. The format is "id:key". To leave the id and key blank, type ":". <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn; {ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.
		import [name]		Import the PEM-encoded certificate from stdin. [name] specifies the descriptive name (optional) as which the imported certificate is to be saved. For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on ZyWALL. After the importation, the certification request will automatically be deleted. If a descriptive name is not specified for the imported certificate, the certificate will adopt the descriptive name of the certification request.
		export <name>		Export the PEM-encoded certificate to stdout for user to copy and paste. <name> specifies the name of the certificate to be exported.
		view <name>		View the information of the specified local host certificate. <name> specifies the name of the certificate to be viewed.
		verify <name> [timeout]		Verify the certification path of the specified local host certificate. <name> specifies the name of the certificate to be verified. [timeout] specifies the timeout value in seconds (optional). The default timeout value is 20 seconds.
		delete <name>		Delete the specified local host certificate. <name> specifies the name of the certificate to be deleted.
		list		List all my certificate names and basic information.
		rename <old name> <new name>		Rename the specified my certificate. <old name> specifies the name of the certificate to be renamed. <new name> specifies the new name as which the certificate is to be saved.
		def_selfsigned [name]		Set the specified self-signed certificate as the default self-signed certificate. [name] specifies the name of the certificate to be set as the default self-signed certificate. If [name] is not specified, the

				name of the current self-signed certificate is displayed.
	ca_trusted			
		import <name>		Import the PEM-encoded certificate from stdin. <name> specifies the name as which the imported CA certificate is to be saved.
		export <name>		Export the PEM-encoded certificate to stdout for user to copy and paste. <name> specifies the name of the certificate to be exported.
		view <name>		View the information of the specified trusted CA certificate. <name> specifies the name of the certificate to be viewed.
		verify <name> [timeout]		Verify the certification path of the specified trusted CA certificate. <name> specifies the name of the certificate to be verified. [timeout] specifies the timeout value in seconds (optional). The default timeout value is 20 seconds.
		delete <name>		Delete the specified trusted CA certificate. <name> specifies the name of the certificate to be deleted.
		list		List all trusted CA certificate names and basic information.
		rename <old name> <new name>		Rename the specified trusted CA certificate. <old name> specifies the name of the certificate to be renamed. <new name> specifies the new name as which the certificate is to be saved.
		crl_issuer <name> [on/off]		Specify whether or not the specified CA issues CRL. <name> specifies the name of the CA certificate. [on/off] specifies whether or not the CA issues CRL. If [on/off] is not specified, the current crl_issuer status of the CA.
	remote_trusted			
		import <name>		Import the PEM-encoded certificate from stdin. <name> specifies the name as which the imported remote host certificate is to be saved.
		export <name>		Export the PEM-encoded certificate to stdout for user to copy and paste. <name> specifies the name of the certificate to be exported.
		view <name>		View the information of the specified trusted remote host certificate. <name> specifies the name of the certificate to be viewed.
		verify <name> [timeout]		Verify the certification path of the specified trusted remote host certificate. <name> specifies the name of the certificate to be verified. [timeout] specifies the timeout value in seconds (optional). The default timeout value is 20 seconds.
		delete <name>		Delete the specified trusted remote host certificate. <name> specifies the name of the certificate to be deleted.
		list		List all trusted remote host certificate names and basic information.
		rename <old name> <new name>		Rename the specified trusted remote host certificate. <old name> specifies the name of the certificate to be renamed. <new name> specifies the new name as which the certificate is to be saved.
	dir_service			
		add <name> <addr[:port]> [login:pswd]		Add a new directory service. <name> specifies a descriptive name as which the added directory server is to be saved. <addr[:port]> specifies the server address (required) and port (optional). The format is "server-address[:port]". The default port is 389. [login:pswd] specifies the login name and password, if required. The format is "[login:password]".
		delete <name>		Delete the specified directory service. <name> specifies the name of the directory server to be deleted.
		view <name>		View the specified directory service. <name> specifies the name of the directory server to be viewed.
		edit <name> <addr[:port]> [login:pswd]		Edit the specified directory service. <name> specifies the name of the directory server to be edited. <addr[:port]> specifies the server address (required) and port (optional). The format is

				"server-address[:port]". The default port is 389. [login:pswd] specifies the login name and password, if required. The format is "[login:password]".
		list		List all directory service names and basic information.
		rename <old name> <new name>		Rename the specified directory service. <old name> specifies the name of the directory server to be renamed. <new name> specifies the new name as which the directory server is to be saved.
	cert manager			
		reinit		Reinitialize the certificate manager.

Bandwidth management Related Command

[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.
				<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

ZyXEL Confidential

						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.
		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

ZyXEL Confidential

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

ZyXEL Confidential

	config	save				Save the configuration.
		load				Load the configuration.
		clear				Clear the configuration.