ZyXEL

Firmware Release Note

ZyWALL 10W

Release 3.60(WH.2)

Date: **Mar, 31, 2003**
Author: **Jason Chiang**

s

ZyXEL ZyWALL 10W Standard Version
Release 3.60(WH.2)
Release Note

Date: Mar 31, 2003

Supported Platforms:

ZyXEL ZyWALL10W

Versions:

ZyNOS Version: V3.60(WH.2) | 03/31/2003 17:18:52
BootBase : V1.05 | 03/12/2002 16:55:33

Notes:

1. 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.
2. 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.
3. 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.
4. When firewall turns from “off” to “on”, the firewall initialization procedure will disconnect all connections running through the ZyWALL.
5. SUA/NAT address loopback feature was enabled on ZyWALL10W by default, however, if users do not need it, a C/I command “ip nat loopback off” could turn it off.
6. In WLAN configuration, a switch for enable / disable WLAN is added. The default value is “disable” since WLAN without any security setting is vulnerable. Please configure MAC filter, WEP and 802.1X when you enable WLAN feature.

Known Issues:

1. Dial-backup feature is not ready.
2. Click “iCard” or “Free” pages many times in few seconds, system will crash.

3. Sometimes eWC→time zone page can't be configured under IE 5.00.3315
4. Stations using Lucent WLAN cards sometimes cannot access ZyWALL10W if Intersil 2.5/3.0 cards are inserted.
5. When going inside an empty VPN rule, pre-shared key sometimes has been filled by some values which belong to other rules automatically.
6. eWC→WAN IP has bugs when WAN→ISP is PPPoE or PPTP. Leaving some values in remote IP or remote masks for WAN→IP and then switch to dynamic IP, ZyWALL cannot dial anymore.
7. Sometimes on screen the "Local Area Connection" icon for UPnP disappears. The icon shows again when restarting PC.
8. UPnP problems:
   (1) Sometimes XP can not find router in "My Network Place" after rebooting PC.
   (2) Service items in Internet Gateway→Service can not be saved and is always empty.
9. When user sends a large echo packet through the firewall, there are many weird ICMP packet logs to be generated.
10. Symptom: ZyWALL WLAN-802.1X can not connect with PC whose OS version is Windows XP SP1.
    Condition: Since ZyWALL doesn't support TLS and there is no MD5 supported in Windows XP SP1, ZyWALL can not connect with the PC which has upgraded to Windows XP SP1.
11. Symptom: VPN tunnels will be deleted when phase 1 parameters are the same.
    Condition:
    (1) Set up two rules (rule 1 and rule 2) with same phase 1 parameters.
    (2) Use CI command "ipsec dial 1" to set up tunnel 1.
    (3) Use CI command "ipsec dial 2" to set up tunnel 2.
    (4) Tunnel 1 will be deleted.
12. Symptom: Traffic redirect doesn't work correctly.
    Condition:
    (1) Traffic doesn't work in LAN
    (2) In WAN, when remote device disconnects, sometimes ZyWALL won't discover the line is dropped.

Features:

Modifications in V3.60(WH.2) | 3/31/2003

1. [BUG FIX] Symptom: eWC→WAN→Route: "Priorily" should be "Priority".

Modifications in V3.60(WH.2)b5 | 3/27/2003

1. [BUG FIX] Symptom: IPSec rekey procedure is not stable.
   Condition:
   (1) There exists an IPSec rule, it's Secure gateway address is domain name. And the

phase 2 PFS is on, either DH1 or DH2.
(2) Sometimes the IPSec rekey procedure will not work properly.
(3) From the log, user will see ZyWALL only receives IKE packets but never responses.

2. [BUG FIX] Symptom: Old SA won't be deleted.
   Condition: When SA is renegotiated, it won't be deleted after one minute.

Modifications in V3.60(WH.2)b4 | 3/21/2003

1. [BUG FIX] Symptom: When VPN tunnel is up, and SMT→27.1.1.1→PHS is on (DH 1 or DH 2), users can not PING. through tunnel to peer.

Modifications in V3.60(WH.2)b3 | 3/20/2003

1. [BUG FIX] Sympton: Even the parameter is correct, negotiation for IKE phase 1 may fail.
   Condition: There are two types of conditions. 1) When two rules have same secure gateway address, sometimes the second tunnel cannot be established after the first one is built. 2) This situation also happens in rekey. If the initiator did not send DEL phase 1 information packet first and then start another phase 1 negotiation directly, this negotiation may fail.
2. [BUG FIX]Symptom: Sometimes IPSec rekey procedure failed.
   Condition: Under heavy traffic, sometimes IPSec rekey failed.
3. [BUG FIX]Symptom: VPN tunnel can not be established in aggressive mode.
4. [BUG FIX]Symptom: TELIA login problem:
   (5) In SMT, hint is not correct.
   (6) The length of login name is inconsistent in SMT and GUI.
   (7) In eWC, login server can input IP address.
   (8) In SMT and eWC, users can set up WAN IP as static IP address which is not allowed.

Modifications in V3.60(WH.2)b2 | 3/18/2003

1. [BUG FIX] When user types the illegal value of the Telia server and relogin time, it will cause system reboot.

Modifications in V3.60(WH.2)b1 | 3/14/2003

1. [ENHANCEMENT] Support hexadecimal format of pre-shared key. Now pre-shared key starting with "0x" or "0X" will be treated as hexadecimal format.
2. [ENHANCEMENT] Support Telia login
3. [BUG FIX] Web URL can accept control characters <>.

4. [BUG FIX] User can download rom-0 through eWC without permission.

Modifications in V3.60(WH.1) | 3/14/2003

Modifications in V3.60(WH.1)b1 | 2/26/2003

1. [BUG FIX] Fix a security issue of web.
2. [BUG FIX] Symptom: VPN tunnel can not be established if ZyWALL sets phase 1 ID type as IP and wants to negotiate with another side by passing through a router with NAT.
   Condition: Take the figure below as the example:

   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 and will set secure gateway as C. In our implementation system will set peer ID content as secure gateway address if peer ID type is IP. So A's peer ID content is C's WAN IP if A's peer ID type is IP. In this case, A and B will never negotiate successfully. Now user can specify the ID content when ID type is IP. So user can set A's peer ID content as B's WAN IP and they can build tunnel successfully. For more detail, please refer to appendix 6.

Modifications in V3.60(WH.0) | 11/29/2002

1. [ENHANCEMENT] Add CI command for display categories. Now "sys logs disp CATEGORY" can show logs according to the CATEGORY field.
2. [ENHANCEMENT] Add new log category "ike" and four alerts: "access control", "block java etc", "ipsec", and "ike".
3. [ENHANCEMENT] The subject of email for the logs can be configure by CI command "sys logs mail subject.
4. [ENHANCEMENT] Add 802.1X access control on WLAN.
5. [ENHANCEMENT] Add more ID supported in IKE phase 1 authentication. Now ZyWALL10W supports ID-IP, ID-FQDN, ID-USER-FQDN.
6. [FEATURE CHANGE] In VPN configuration, local IP start field can accept 0.0.0.0.
7. [FEATURE CHANGE] The log of remote management is moved from error log to centralized log. Its category is "Access Control".
8. [FEATURE CHANGE] When WLAN is disable, the WLAN LED will be off.
9. [FEATURE CHANGE] Accept space character for ESSID in WLAN configuration.
10. [FEATURE CHANGE] The format of SYSLOG is changed. Source IP and destination IP are added.
11. [FEATURE CHANGE] After sending E-mail, the log will still remain.

12. [FEATURE CHANGE] Add a new CI command “clear” to clear a NAT entry. For example, ”ip nat server edit 2 clear” can clear rule NAT rule number 2.
13. [FEATURE CHANGE] Add range check for Many-One-to-One. The number of local IP should be the same with Global IP.
14. [FEATURE CHANGE] In WLAN Setup, add feature to enable/disable WLAN.
15. [FEATURE CHANGE] Sometimes user will get some default policy log without set, because other processes like NAT drop these packets or bypass firewall. We replace the default policy description with its actual reason in centralize log.
16. [FEATURE CHANGE] Syslog adds source / destination IP address field.
17. [FEATURE CHANGE] Change the behavior of FQDN when ID type is DNS. Now ID and Address fields are independent.
18. [BUG FIX] After 34 item of email log will be garbage.
19. [BUG FIX] Fix a security issue related with port scan.
20. [BUG FIX] Fix a security issue related with smurf attack.
21. [BUG FIX] Symptom: System is not stable when domain names of mail server or syslog server are un-resolvable.
    Condition: When users set up mail server or syslog server address with domain name and then save the setting, system halts if that address is an illegal or un-resolvable domain name at that time when sending mail or syslog.
    [Note] Please refer to Appendix 5 for detail.
22. [BUG FIX] Symptom: System halts when both firewall and syslog turn on.
    Condition: When syslog server daemon stops or syslog server host does not exist, the syslog packets explode and firewall generates masses of ICMP packet logs. As a result, system hangs.
23. [BUG FIX] Symptom: Checkbox in eWC→UPnP is not correct.
    Condition: In eWC→UPnP, if selecting “Allow UPnP to pass through Firewall” checkbox and apply, then go to other page and return to eWC→UPnP again, the “Allow UPnP to pass through Firewall” checkbox is still unselected.
24. [BUG FIX] Symptom: When a PC traces route from LAN to WAN, ZyWALL is not visible in the tracing path with firewall on.
    Condition: Firewall blocks the time exceed ICMP packet and log message is “Unsupported/out-of-order ICMP”.
25. [BUG FIX] Symptom: The content of web forward log message is junk.
    Condition: If user blocks the keyword “kimo” and access the web site that does not contain the keyword “kimo”, the system will generate web forward log message.
27. [BUG FIX] Symptom: eWC→VPN→VPN configuration error message.
    Condition: While access eWC→VPN→”VPN Configuration”, and then press “Go back” button, nothing happens and it shows “Please wait…” on “Status”.
28. [BUG FIX] Symptom: Traffic redirect can not be set
    Condition: Can not set traffic redirect in SMT and will get message “Status =-121303 Duplicate IP address to other node’s IP address” when saving rule in SMT 11.1.
29. [BUG FIX] Symptom: Can not change metrics in eWC→WAN→Route
    Condition: When press “Apply” in eWC→WAN→Route, nothing will be saved and message” Status =-121303 Duplicate IP address to other node’s IP address” shows on SMT.
29 [BUG FIX] Symptom: System hangs when turning on/off Internet Gateway several

times
Condition: When UPnP is on, system will hang while turning on/off Internet Gateway several times.

30 [BUG FIX] Symptom: WLAN LED flickers when WLAN is non-active.
Condition: WLAN LED flickers when WLAN card is inserted into router and not active.

31 [BUG FIX] Symptom: While access http://www.gamespy.com/articles/ and http://groups.yahoo.com system will crash.
Condition: System crashes when access http://www.gamespy.com/articles/ or when survey/read the forums via http://groups.yahoo.com.

32 [BUG FIX] Symptom: The system will allow the packet with DF=1 and packet length > MTU to pass through the router without any error message returned to the sender.
Condition: When the packet with its length larger than MTU but DF bit set, it is still allowed to pass through the router.

33 [BUG FIX] Symptom: Conflict check between multi-NAT configuration and VPN is not correct.
Condition: When VPN local IP address is SUBNET, the conflict check with multi-NAT will reply incorrect result.

34 [BUG FIX] Symptom: VPN web page configuration is not correct.
(1) If Edit VPN configuration choose “manual key”, then it cannot be save. The error message “Manual My ID only can be IP” will be displayed.
(2) If Edit VPN configuration choose “manual key”, and ESP encryption algorithm choose “NULL”, then press Apply. Edit the rule again, the authentication key cannot input anymore.

35. [BUG FIX] Symptom: SYSLOG entries truncated.
Condition: When the entry length is larger than 64 bytes, it will be truncated.

36. [BUG FIX] Symptom: Telnet session issue when firmware uploaded.
Condition: After firmware uploaded, system will reboot. However ZyWALL will not disconnect the telnet session connecting to it. As a result, users have to disconnect the telnet session manually.

37. [BUG FIX] Symptom: UPnP sometimes cannot work. After ZyWALL’s LAN IP is changed, sometimes PC with XP can not find ZyWALL
Condition: After restoring default rom file and then change ZyWALL’s LAN IP, PC with Windows XP can not find the router.

38. [BUG FIX] Symptom: eWC→SUA/NAT Address Mapping: rule can not be saved.
Condition: When a rule is configured as type Many-to-one, it cannot be saved. Status will show: “IGA and ILA range does not match”.

39. [BUG FIX] Symptom: High latency in PING across ZW 10 W.
Condition: Under SUA, the latency of PING packets enlarges 30~40ms when they pass through ZyWALL10W.

40. [BUG FIX] Symptom: eWC bugs of WAN / LAN / SYSTEM / WIZARD.
Conditions:
(1) WAN IP: When changing WAN IP from static to dynamic, Gateway IP Address will be “0.0.0.0
(2) Password: When entering wrong “Old Password “, the “Status” will show unreadable messages.

(3) LAN→IP: The ZyWALL 10W will put the "IP Pool Starting Address" to "Primary DNS Server" and "Secondary DNS Server" field, if keep these two fields empty.
(4) SYSTEM→TIME ZONE→"Maxico city" should be "Mexico city".
(5) WIZARD: The example, "my_domain.com", is not correct because "_" is not valid in domain name.
(6) eWC→WAN→Traffic redirect: The metric field cannot save correct value.

41. [BUG FIX] Symptom: eWC→Firewall bugs.
Conditions:
(1) WAN IP: When changing WAN IP from static to dynamic, Gateway IP Address will be "0.0.0.0
(2) When configuring rules, modify "active" option and then change the protocol fields, the screen will refresh and then the active option status does not keep.
(3) After configuring 10 rules, there will be a "go to rule" button. But the format is wrong.
(4) The tags of summary and attack alert are too large.
(5) When editing IP, the start IP can be larger than end IP, which is not correct.
(6) Set more than 8 firewall rules in any direction, and then delete rules from bottom to top, somehow all exist rules will be empty.
(7) Cannot insert rules more than 19.
(8) When inserting a new rule for firewall between existing rules, and then cancel editing this rule, the sorting of other rules is incorrect.
42. [BUG FIX] Symptom: eWC→LOGS bugs.
Conditions:
(1) eWC→LOGS: If the user doesn't input email address in "Send alerts to:" then the ZyWALL won't send log mail.
(2) Items in "Log" or "Send immediate alert" can be changed only once. After applying, furthermore modification will not take changes. Only selecting other pages and com back can configure it again.
(3) When sorting by time, the order is not correct when multiple entries recorded within one seconds.
43. [BUG FIX] Symptom: Blocking time status is not correct for "ip url category disp".
Condition: The blocking time format should be "hh:mm", but through the CI command it will show only integers.
44. [BUG FIX] Symptom: Xbox Live can't work through router.
Condition: Xbox Live can not work through ZyWALL 10 W.
45. [BUG FIX] Symptom: ZyWALL10W can not block JAVA & Active-X components.
Condition: When connecting to web site that has JAVA & Active-X components, the router can not block them by content filter.
46. [BUG FIX] Symptom: The content of the 128th email log is junk.
Condition: The content of email log will be incorrect if each log is large.
47. [BUG FIX] Symptom: The system crashes when establishing IPSec connection.
Condition: When local and peer machine use different phase 1 authentication algorithms in IKE, both systems crash.
48. [BUG FIX] Symptom: WAN side PC can ping ZyWALL's LAN IP

Condition: When “SUA only” and “firewall off”, outside PC can ping ZyWALL’s LAN IP.

49. [BUG FIX] Symptom: The isolated DNS proxy server behinds firewall can not work.
    Condition: When the second or proxy DNS server behinds firewall and try to connect with public DNS server, the TCP 3-ways handshake fails.
50. [BUG FIX] Symptom: eWC→VPN-IKE: Sometimes “Secure Gateway Addr” is empty after saving the VPN rule.
    Condition: After saving one VPN rule at eWC, the secure gateway address disappears and tunnel can never be built.
51. [BUG FIX] Symptom: UPnP doesn’t work
    Condition: Even the eWC showed UPnP in b4, it doesn’t work.
52. [BUG FIX] Symptom: System reboots when transferring data on wireless and change wireless setting at same time.
    Condition: With Intersil 2.5/3.0 cards inserted, while data is transferring on wireless, changing wireless setting will cause router to reboot.
53. [BUG FIX] Symptom: eWC→ Wireless: while we select Radius, then wireless can not be select again.
    Condition: When click Radius tab from Wireless web, Wireless hyperlink disappeared.
54. [BUG FIX] Symptom: Wireless RADIUS issues:
    Condition:
    (1) Without WEP key: while 2nd time the same user login router again, authentication will be ignored and he can login directly.
    (2) With WEP key is used, users can not login.
55. [BUG FIX] Symptom: System reboots when running “sys log disp”.
    Condition: With console port speed set to 9600, dump too much characters will reboot the system.
56. [BUG FIX] Symptom: FQDN doesn’t work correctly when setting rule by web
    Condition: When setting ID type as IP in web, corresponding content is always empty, and tunnel will never be built.
57. [BUG FIX] Symptom: Router learns illegal ARP packet.
    Condition: Router learns IP MAC addresses from wrong interface. For example, router may learn LAN IP Mac address from WAN. It causes some hosts can not connect to the router.
58. [BUG FIX] Symptom: When using Intersil 2.5/3.0 cards in ZyWALL10W, system may crash.
    Condition: During transmitting, save configuration in SMT will cause system to crash.
59. [BUG FIX] Symptom: Wireless Web error with RADIUS tag.
    Condition: In eWC→ WIRELESSLAN, while we select Radius, then wireless can not be selected again.

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

New function

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

Modification

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

```
          Menu 24.11 – Remote Management Control

TELNET Server:    Port = 23       Access = ALL
                  Secured Client IP = 0.0.0.0

FTP Server:       Port = 21       Access = ALL
                  Secured Client IP = 0.0.0.0

Web Server:       Port = 80       Access = ALL
                  Secured Client IP = 0.0.0.0

SNMP server:      Port = 161      Access = ALL
                  Secured Client IP = 0.0.0.0

DNS server:       Port = 53       Access = ALL
                  Secured Client IP = 0.0.0.0


              Press ENTER to Confirm or ESC to Cancel:
```

Appendix 2 Trigger Port

Introduction

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

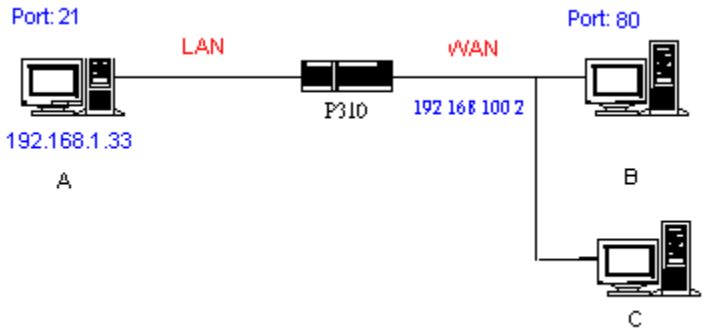
These triggered events can be timed so that they erase the port mapping as soon as they are done with the data transfer, so that the port mapping can be triggered by another Client computer. This gives the ***illusion*** that multiple computers can use the same port mapping at the same time, but the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

How to use it

Following table is a configuration table.

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

How it works



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

(1) As Prestige receives a packet from a local client A destined for the outside Internet machine B, it will check the destination port in the TCP/UDP header to see if it matches the setting in "Trigger Port" (80). If it matches, Prestige records the source IP of A (192.168.1.33) in its internal table.

(2) Now client C (or client B) tries to access the FTP server in machine A. When Prestige to forward any un-requested traffic generated from Internet, it will first check the rules in port forwarding set. When no matches are found, it will then check the

"Incoming Port". If it matches, Prestige will forward the packet to the recorded IP address in the internal table for this port. (This behavior is the same as we did for port forwarding.)

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

Notes

(1) Trigger events can't happen on data coming from ***outside*** the firewall because the NAT router's sharing function doesn't work in that direction.

(2) Only one computer can use a port or port range at a time on a given real (ISP assigned) IP address.

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

The new set C/I commands is under "sys filter netbios" sub-command. Default values of "LAN to WAN" and "WAN to LAN" are "Block", "IPSec Packets" is "Forward" and trigger dial is "Disabled".

There are two CI commands:
(1) "sys filter netbios disp": It will display the current filter mode.

Example ouput:

```
================ 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	Block
1	WAN to LAN	Block
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 dail

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.

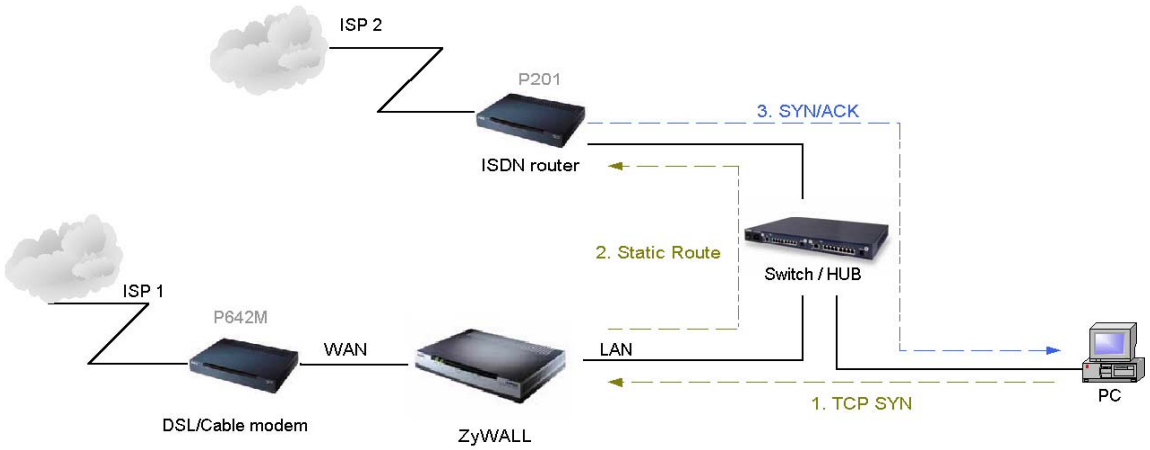


Figure 5-1 Triangle Route

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.

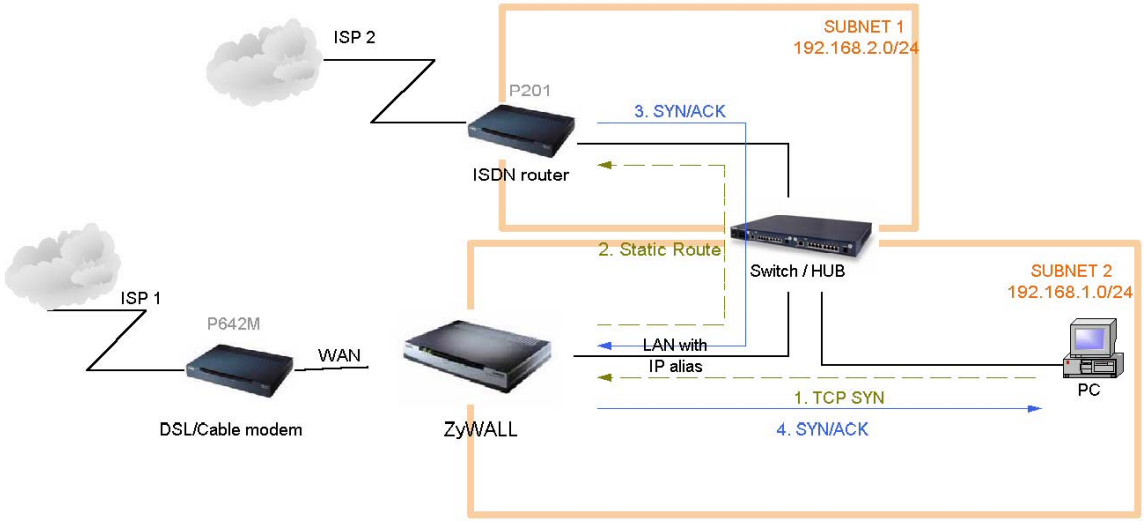


Figure 5-2 Gateway on alias IP network

(2) Gateway on WAN side

A working topology is suggested as below.

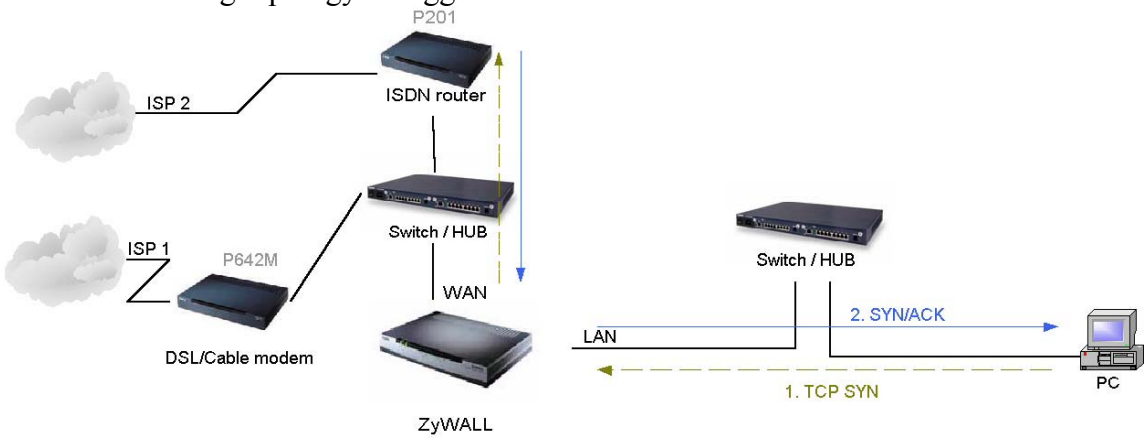


Figure 5-3 Gateway on WAN side

Appendix 5 Mail server setting causes system hang

Condition:

When users set up mail server or syslog server with domain name by CI command or set up in eWC→LOGS→Log Settings, system will resolve the server's domain name when users save the setting (or press "Apply" in eWC→LOGS→Log Settings). If the domain name for the mail server or syslog server can not be resolved (domain name is not correct, network is disconnected, etc.) at that time, system will halt if it sends logs or alert out.

Solution:

While saving the setting of mail server or syslog server address, if the server's address which is a domain name can not be resolved, system will not send alert or log out.

New CI command: *sys log resolve*

Purpose:

Force system to resolve syslog mail server address and mail server address.

Note:

This is a workaround version. During resolve, there will be no other DNS query packet can be processed.

Appendix 6 IPSec FQDN support

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

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

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

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

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

We can put all combinations in to these two tables:

(Local ID Type is IP):

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

*Blank: User can leave this field as empty, doesn't put anything here.
**Runtime status: During IKE negotiation, ZyWALL will use "My IP Addr" field as source IP of IKE packets, and put "Local ID Content" in the ID payload.

(Peer ID Type is IP):

Configuration	*Run-time check

Secure Gateway Addr	Peer ID Content	
0.0.0.0	Blank or 0.0.0.0	Just check ID types of incoming packet and machine's peer ID type. If the peer's ID is IP, then we accept it.
0.0.0.0	a.b.c.d (NOT 0.0.0.0)	System checks both type and content
a.b.c.d	Blank	1. System will check the ID type and the content. 2. The contents will match only if the ID content of coming packet is a.b.c.d because system will put Secure Gateway Address as Peer ID content.
a.b.c.d	e.f.g.h	1. System will check the ID type and the content. 2. The contents will match only if the ID content of coming packet is e.f.g.h.

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

Summary:

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

Annex A CI Command List

Last Updated: 2002/11/26

Command Class List Table		
System Related Command	Exit Command	Device Related Command
Ethernet Related Command	POE Related Command	PPTP Related Command
Configuration Related Command	IP Related Command	IPSec Related Command
Firewall Related Command		

System Related Command Home

Command				Description
sys				
	adjtime			retrive date and time from Internet
	callhist			
		display		display call history
		remove	<index>	remove entry from call history
	countrycode		[countrycode]	set country code
	date		[year month date]	set/display date
	domainname			display domain name
	edit		<filename>	edit a text file
	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
	hostname		[hostname]	display system hostname
	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
			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|urlblocked|urlforward]	display all logs or specify category logs
		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
			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
	log			
		clear		clear log error
		disp		display log error
		online	[on|off]	turn on/off error log online display
		resolve		Resolve mail server and syslog server address
	mbuf			
		link	link	list system mbuf link
		pool	<id> [type]	list system mbuf pool
		status		display system mbuf status
		disp	<address>	display mbuf status
		cnt		
			disp	display system mbuf count
			clear	clear system mbuf count
		debug	[on|off]	
	pwderrtm		[minute]	Set or display the password error blocking timeout value.
	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		[minute]	change terminal timeout value
	time		[hour [min [sec]]]	display/set system time
	trcdisp			monitor packets
	trclog			
	trcpacket			
	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
	romreset			restore default romfile
	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
	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
	cmgr			
		trace		
			disp <ch-name>	show the connection trace of this channel
			clear <ch-name>	clear the connection trace of this channel
		cnt	<ch-name>	show channel connection related counter
	socket			display system socket information
	filter			
		netbios		
	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
	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
	filter			
		netbios		
	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

		save		save upnp information

Exit Command [Home]

Command				Description
exit				exit smt menu

Device Related Command [Home]

Command				Description
dev				
	channel			
		drop	<channel_name>	drop channel
	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
		ioctl	<ch_name>	Useless in this stage.
		status	<ch_name>	see LAN status
	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
	debug			
		disp	<ch_name>	display ethernet debug infomation
		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
		accessblock	<0:disable 1:enable>	block internet access
		save		save ether data to spt

POE Related Command [Home]

Command				Description
poe				
	status		[ch_name]	see poe status
	dial		<node>	dial a remote node
	drop		<node>	drop a pppoe call
	ether		[rfc|3com]	set /display pppoe ether type

PPTP Related Command [Home]

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

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-low <0~255>		The threshold to stop deleting the half-opened session
			tcp-max-incompl		The threshold to start executing the block field

			ete <0~255>		
		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
			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	Select and edit a destination port range of a

				port#> <end port#>	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
	dhcp		<iface>	
		client		
			release	release DHCP client IP
			renew	renew DHCP client IP
		status	[option]	show dhcp status
	dns			
		query		
		server	<primary> [secondary] [third]	set dns server
		stats		
			clear	clear dns statistics
			disp	display dns statistics
	httpd			
	icmp			
		status		display icmp statistic counter
		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
	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
	smtp			

	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.
	traceroute		<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
	ave			anti-virus enforce
	urlfilter			
		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
			clearAll	clear exemptzone information
		customize		
			display	display customize action flags
			actionFlags [act(1-6)][enable/disable]	set action flags
			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
			clearAll	clear all information
		logDisplay		display cyber log
		ftplist		update cyber list data
		listServerIP	<ipaddr>	set list server ip
		listServerName	<name>	set list server name
	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
	nat			
		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
		resetport		reset all nat server table entries
		incikeport	[on|off]	turn on/off increase ike port flag
	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> grouptm <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			

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	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 connection has no traffic for certain period. If yes, system will disconnect it.
				- Interval is in minutes
				- Default is 2 minuets
				- 0 means never timeout
		update_peer	<0~255>	- Adjust auto-timer to update IPSec rules which use domain name as the secure gateway IP.
				- Interval is in minutes
				- Default is 30 minutes
				- 0 means never update
				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
		name	<string>	Set rule name
		keeyAlive	<Yes| No>	Set keep alive or not
		lcIdType	<0:IP | 1:DNS | 2:Email>	Set local ID type
		lcIdContent	<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
		lcAddrType	<0:single | 1:range | 2:subnet>	Set local address type
		lcAddrStart	<IP>	Set local start address
		lcAddrEndMask	<IP>	Set local end address or mask
		lcPortStart	<port>	Set local start port
		lcPortEnd	<port>	Set local end port
		rmAddrType	<0:single | 1:range | 2:subnet>	Set remote address type
		rmAddrStart	<IP>	Set remote start address
		rmAddrEndMask	<IP>	Set remote end address or mask
		rmPortStart	<port>	Set remote start port
		rmPortEnd	<port>	Set remote end port
		antiReplay	<Yes | No>	Set anitreplay or not
		keyManage	<0:IKE | 1:Manual>	Set key manage
		ike	negotiationMode <0:Main | 1:Aggressive>	Set negotiation mode in phase 1 in IKE
			preShareKey <string>	Set pre shared key in phase 1 in IKE
			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

Firewall Related Command Home

Command				Description
sys	Firewall			
		acl		
			disp	Display specific ACL set # rule #, or all ACLs.
		active	<yes|no>	Active firewall or deactivate firewall
		clear		Clear firewall log
		cnt		
			disp	Display firewall log type and count.
			clear	Clear firewall log count.
		disp		Display firewall log
		online		Set firewall log online.
		pktdump		Dump the 64 bytes of dropped packet by firewall
		update		Update firewall
		dynamicrule		
		tcprst		
			rst	Set TCP reset sending on/off.
			rst113	Set TCP reset sending for port 113 on/off.
			display	Display TCP reset sending setting.
		icmp		
		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