



**Firmware Release Note**

**ZyWALL 2**

**Release 3.60(WK.1)c0**

**Date:**  
**Author:**

**Apr 19, 2003**  
**Vincent Chen**

# **ZyXEL ZyWALL 2 Standard Version**

## **Release 3.60(WK.1)c0**

### **Release Note**

**Date:** Apr 19, 2003

#### **Supported Platforms:**

---

ZyXEL ZyWALL 2

#### **Versions:**

---

ZyNOS F/W Version : V 3.60(WK.1) | 04/19/2003 13:03:34  
BootBase : V1.04 | 01/23/2003 15:24:37

#### **Notes:**

---

1. The setting of ignore triangle route is on in default ROMFILE. Triangle route network topology has potential security crisis. If you are not clear about it, please refer to Appendix for the triangle route issue.
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 ZyWALL by default; however, if users do not need it, a C/I command "ip nat loopback off" could turn it off.
6. 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.

#### **Known Issues:**

---

1. Dial-backup feature is not ready.
2. Sometimes on screen the "Local Area Connection" icon for UPnP disappears. The icon shows again when restarting PC.
3. When Peer ID content is blank when its ID type is IP and the secure gateway address is 0.0.0.0, the rule will be chosen when incoming packets' ID type is IP. This is because ZyWALL only check ID type when this rule's ID content is blank and ID type is IP. We will modify it in the future.

4. 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.
5. The DHCP client in ZW LAN side may get an IP which is reserved by static DHCP. The situation will disappear if the client releases the IP and requests again.
6. 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.

## **Features:**

---

### **Modifications in V 3.60(WK.1)c0 | 4/19/2003**

### **Modifications in V 3.60(WK.1)b4 | 4/14/2003**

1. [BUG FIX] Symptom & Condition: When users change the WAN MAC from factory default to spoofing a specific computer's MAC, traffic can not pass through ZyWALL from LAN to WAN.

### **Modifications in V 3.60(WK.1)b3 | 4/2/2003**

2. [BUG FIX] Symptom: Sometimes, IPSec re-key procedure failed.  
Condition: Under the heavy traffic situation, sometimes IPSec re-key failed.
3. [BUG FIX] Symptom: Even though the IPSec policy is correct, the IKE phase 1 negotiation may failed.  
Condition 1: When there are two IPSec policies with the same security gateway, ZyWALL sometimes can't create the second IPSec tunnel.  
Condition 2: If ZyWALL didn't send the DEL packet to info the security gateway to delete the IPSec tunnel (for example power off the device, or PPPoE drops...etc.), ZyWALL can't re-create the tunnel.
4. [BUG FIX] Symptom: It's a compatibility problem with SonicWall.  
Condition 1: Can't create the IPSec tunnel with a SonicWall security gateway, if the type of ID Content is FQDN.

### **Modifications in V 3.60(WK.1)b2 | 3/26/2003**

5. [BUG FIX] Add eWC wizard telia service check – Check relogin value, WAN IP assignment and Telia login server should be domain name.
6. [BUG FIX] Symptom: Save Telia login service under static IP address assignment will show roadrunner error message.  
Condition: Telia login only work when WAN IP is assigned with dynamic IP. If save this service with static IP, the error message is not correct.
7. [BUG FIX] Symptom: eWC can't save PSK with hexadecimal format that more than 32 characters.  
Condition: Save PSK in hexadecimal format that more 32 characters, the PSK will

be cut to 30 characters.

#### **Modifications in V 3.60(WK.1)b1 | 3/14/2003**

1. [BUG FIX] Symptom: A special case will make the ZyWALL device to reboot.
  - (1) Condition: (1) Configure an IPSec Rule.
  - (2) On the Logs Settings page, configure "Mail Server", "Mail Subject" and the mail address logs mails send to.
  - (3) Still on the Logs Settings page, select IPSec and IKE alert.
  - (4) Enter the CI command mode, and issue the CI command "ipsec dial #" to create the VPN tunnel.
  - (5) After seeing the message "Press any key to return....", press the Enter key.
  - (6) The ZyWALL crashes.
2. [BUG FIX] Symptom & Condition: On Firewall --- Rule Config, can't setup to log firewall logs.
3. [BUG FIX] The general user(not ZyWALL administrator), can directly retrieve ZyWALL rom file by using the rom-0 as the URL file, without password checking.
4. [ENHANCEMENT] Supports the hexadecimal format of IPSec Pre-Shared Key.
5. [ENHANCEMENT] Supports Telia login WAN access.
6. [ENHANCEMENT] Added a new CI commands to configure UDP port NAT timeout  
CI command: "ip nat timeout udp [port] <seconds>". For more details, please refer to CI command lists

#### **Modifications in V 3.60(WK.0)b9 | 2/21/2003**

#### **Modifications in V 3.60(WK.0)b9 | 2/21/2003**

1. [BUG FIX] Symptom: VPN setting causes system reboot.  
Condition: Step1. Build one VPN tunnel and set the secure gateway address by using IP address and establish the tunnel. Keep on pinging the client continuously  
Step2. Change the secure gateway address setting from IP to DNS and apply.
2. [BUG FIX] Symptom: Status display ERROR.  
Condition: When we change System/Time Zone to none by web, an internally ERROR 1 will be displayed in the Status-Line.
3. [BUG FIX] Symptom & Condition: In web, the page does not refresh when we change the time zone and apply.

#### **Modifications in V 3.60(WK.0)b8 | 2/14/2003**

1. [BUG FIX] Symptom & Condition: It's failed to restore default romfile by pressing reset button.

2. [BUG FIX] Symptom: System rebooted under heavy traffic.  
Condition: When watchdog turns on (sys wdog sw on) and under heavy traffic, ZW will reboot.
3. [BUG FIX] Symptom & Condition: The maximum number of source addresses or destination addresses in an ACL rule is 20. But users can set more than 20 addresses.

#### **Modifications in V 3.60(WK.0)b7 | 1/23/2003**

1. [FEATURE CHANGE] Enable eWC NAT Full-feature (add address mapping table).
2. [BUG FIX] Symptom & Condition: One special notebook PC(Dell Inspiron 8000) connect to ZyWALL's console port and none of terminal program open the console port. In this situation, the ZyWALL device boots fail.

#### **Modifications in V 3.60(WK.0)b6 | 1/10/2003**

1. [ENHANCEMENT] Add NAT traversal feature. This feature is supported only ESP tunnel and ESP transport when key management is IKE.
2. [ENHANCEMENT] Add the Full Feature NAT.
3. [FEATURE CHANGE] Message change from "Discard packet, the mac is not allowed. vlanTag=4" to "VPN1 discards packet, the mac is not allowed."
4. [FEATURE CHANGE] DHCP relay is not supported anymore.
5. [FEATURE CHANGE] The color of centralize Log GUI is defined. Black color is for normal log messages and red for alert log messages.
6. [BUG FIX] Symptom & Condition: While NAT is enabled, remote device can not access router's LAN IP through IPSec tunnel. In other words, remote management to the LAN IP over IPSec tunnel failed.
7. [BUG FIX] Symptom & Condition: When Traffic Redirect is active and change the WAN encapsulation to PPPoE or PPTP, and if idle time out the routing table will disorder.
8. [BUG FIX] Symptom & Condition: Removed wrong "DMZ" selection form all Remote Management pages.
9. [BUG FIX] Symptom & Condition: If the user didn't load IPSec rule first before executing IPSec configuration CI command, "ipsec config netbios active <yes|no>" or "ipsec config netbios group <...>", ZyWALL will crash.
10. [BUG FIX] Symptom: Can not change WAN MAC by web immediately:  
Condition: While we change WAN MAC by web, the MAC ca not change immediately till device reboot. But it is OK while we change by SMT menu.
11. [BUG FIX] Symptom: Console led does not light:  
Condition: Console led does not light while we login into SMT.
12. [BUG FIX] Symptom: Receiving hotmail mail will cause system crash.  
Condition: 1. Enable Block Cookies. 2. Receiving mail form hotmail causes system crash.
13. [BUG FIX] Symptom: System crashes when setting DHCP :  
Condition: If we disable DHCP server and set a static DHCP entry, the ZyWALL crashes.
14. [BUG FIX] Symptom: The value for sys stdio can not be saved. :

- Condition: Under CI command, we enter “sys stdio 0”. The value becomes the default value after we relogin SMT.
15. [BUG FIX] Symptom: Traffic redirect check path is not up :  
Condition: While WAN link is fine and the traffic redirect check point is failed, it spends long time to activate traffic redirect. Under the situation, the metric of the route for traffic redirect sometimes changes frequently.
  16. [BUG FIX] Symptom: Switching Web is not smooth:  
Condition: Sometimes we can not smoothly switch between VPN1/VPN2 in VPN page.
  17. [BUG FIX] Symptom: Traffic Redirect can't work on PPPoE connection.  
Condition: If the WAN side has a successful PPPoE connection, and the ZyWALL device would not check the checked site and update to correct the routing table.
  18. [BUG FIX] Symptom: LAN LED light on, when setup the WAN.  
Condition: Using the eWC to setup WAN or using SMT 2 to setup the WAN's MAC address. All Ethernet LEDs will light on.
  19. [BUG FIX] Symptom: Add, delete or refresh static route rule on SMT menu12 sometimes cause ZyWALL crash.  
Condition: Sometimes our action on menu12 with static route rule setup will cause ZyWALL crash.
  20. [BUG FIX] Symptom: When "ipsec switch" is off, "ipsec dial" still works.  
Condition: If user uses command "ipsec switch off" to turn off IPSec, "dial" still works.

#### **Modifications in V 3.60(WK.0)b5 | 12/12/2002**

1. [FEATURE ENHANCEMENT] show the reason of forward/block by content filter feature in the centralized log message.
2. [FEATURE CHANGE] Symptom & Condition: System reboot under heavy traffic if the watchdog mechanism is on.
3. [BUG FIXED] Symptom & Condition: The system crashes, if the user power off the PC which connect to the device's console port.
4. [BUG FIX] Symptom: Menu 24.6 Restore occur system reboot :  
Condition: Menu 24.6 Restore Configuration is Failed and Device will Hang then key any key Occur system reboot !
5. [BUG FIX] Symptom: System reboot :  
Condition: The ZW2 V3.60(WK.0)b2 /ZW2W V3.60(WJ.0)b2 system reboot occur The Step: Into Web; VPN Host ;VPN Hosts IP Address or MAC address, if you change IP or MAC and Apply the ZW will reboot!!
6. [BUG FIX] Symptom: The parsing string for keyword blocking is junk.  
Condition: 1. Use CI command "ip urlfilter customize actionFlag act5 enable" to enable the full path check. 2. Use browser to access the URL that set in the keyword blocking, the packets will be still allowed to pass.
7. [BUG FIX] Symptom & Condition: The system crashes, if the user changes the console's baud rate and presses any key by using a different data rate.
8. [BUG FIX] Symptom & Condition: eWC→WAN IP has bugs when WAN→ISP is PPPoE or PPTP. Leaving some values in remote IP or remote mask for WAN→IP and then switch to dynamic IP, ZyWALL cannot dial anymore
9. [BUG FIX] Symptom: System hangs when syslog is active.

Condition: System hangs when syslog is active and syslog daemon on the remote server turns off.

10. [BUG FIX] Symptom & Condition: After setting a VPN rule and then save it, sometimes warning message “[-6100] Fail to lock read” shows on screen. But the rule can be saved correctly and tunnel can be built successfully.

11. [BUG FIX] Symptom: The PPPOE or PPTP address can be set within the range of LAN subnet.

Condition: When using smt menu 4 or 11, choose the pppoe or pptp encapsulation, set the IP address within the range of LAN subnet and then save the configuration.

12. [BUG FIX] Symptom: Send email log will cause system to hang about 30 seconds.

Condition: 1. Email server address is written in domain name. 2. The WAN network link can not connect to Internet when applying email log setting.

13. [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. To avoid this situation, now user can set ID content when ID type is IP. In this case, A will check the ID content what B is configured. However, user can leave the ID content is blank when ID type is IP. Please refer to appendix for the detail setting and system behavior.

14. [BUG FIX] Symptom & Condition: During IKE phase 1 negotiation, if ZyWALL receives a Notify DEL payload, it may crash.

#### **Modifications in V 3.60(WK.0)b4 | 12/3/2002**

1. [BUG FIX] Symptom: HTP external test fail.

Condition: HTP test is failed in LAN and WAN external loopback test.

#### **Modifications in V 3.60(WK.0)b3 | 11/29/2002**

1. [BUG FIX] Symptom: Bootbase can not change baud rate.

Condition: Bootbase always use baud rate 9600 after the system starts or restarts. The baud rate which users set will take effect after RAS starts.

2. [BUG FIX] Symptom: Can not restore configuration by menu 24.6.

Condition: Menu 24.6 restore configuration is failed and device will hang then key any key occur system reboot.

3. [BUG FIX] Symptom: VPN page configuration causes system reboot.

Condition: Web -> VPN Host -> VPN host's IP address or Mac address. If you change IP and Apply, the ZW will reboot.

4. [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>.

5. [BUG FIX] Heavy traffic causes system reboot.  
Heavy traffic easily trigger watchdog to reset system.

#### **Modifications in V 3.60(WK.0)b2 | 11/21/2002**

1. First release.

#### **Modifications in V 3.60(WK.0)b1 | 11/11/2002**

2. [FEATURE CHANGE] HTP behavior is changed. Please refer to appendix 1
3. [BUG FIX] Ethernet external loop back test fail.

## 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.

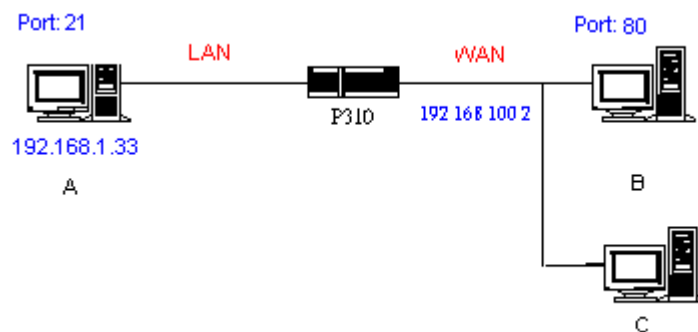
These triggered events can be timed so that they erase the port mapping as soon as they are done with the data transfer, so that the port mapping can be triggered by another Client computer. This gives the **illusion** that multiple computers can use the same port mapping at the same time, but the computers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

### How to use it

Following table is a configuration table.

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

### How it works



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

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

we did for port forwarding.)

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

#### **Notes**

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

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

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

There are two CI commands:

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

Example output:

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

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

Current filter types and their description are:

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

Example commands:

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

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

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

sys filter netbios config 7 off => disable trigger dial

## Appendix 4 Traffic Redirect/Static Route Application Note

### Why traffic redirect/static route be blocked by ZyWALL

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

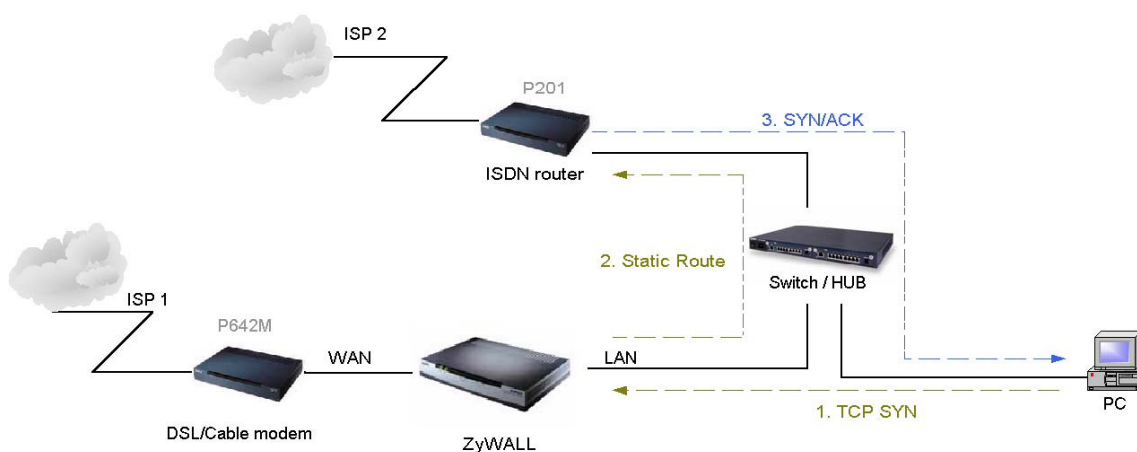


Figure 4-1 Triangle Route

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

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

That causes all of outgoing TCP traffics being reset!

### How traffic redirect/static route works under protection - Solutions

#### (1) Gateway on alias IP network

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

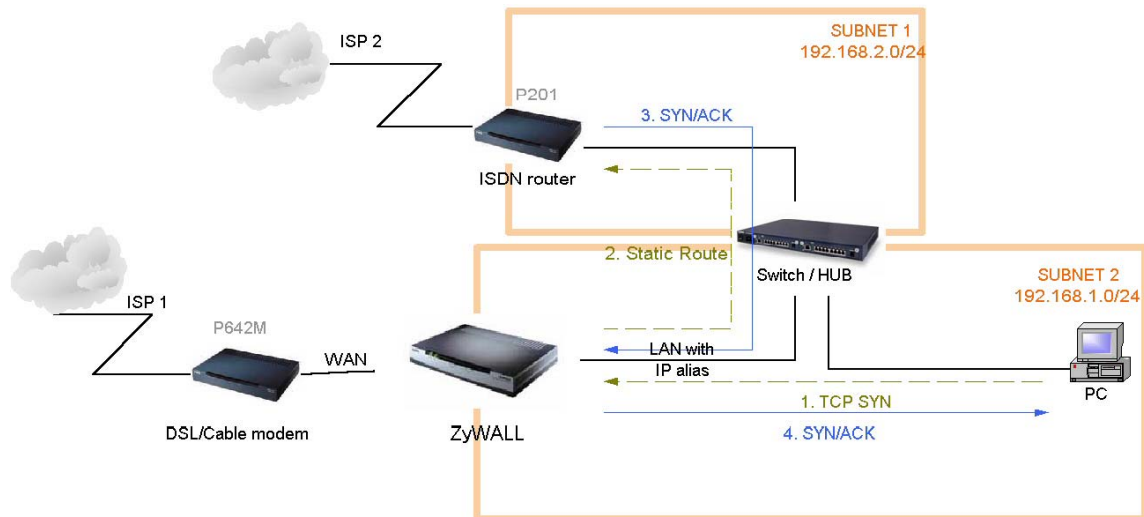


Figure 4-2 Gateway on alias IP network

## (2) Gateway on WAN side

A working topology is suggested as below.

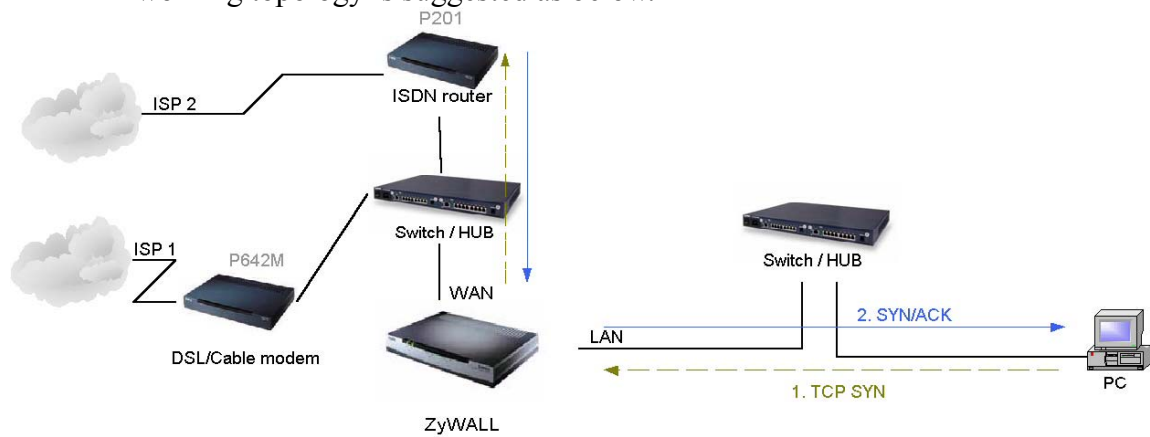


Figure 4-3 Gateway on WAN side

## Appendix 5 IPSec FQDN support

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

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

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

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

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

We can put all combinations in to these two tables:

(Local ID Type is IP):

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

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

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

(Peer ID Type is IP):

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

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

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

### Summary:

1. When Local ID Content is blank 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

| Command Class List Table               |                                       |  |
|--|---------------------------------------|--|
| <a href="#">System Related Command</a> | <a href="#">Exit Command</a>          | <a href="#">Ethernet Related Command</a> |
| <a href="#">IP Related Command</a>     | <a href="#">IPSec Related Command</a> | <a href="#">Firewall Related Command</a> |

| System Related Command |             |          |  | <a href="#">Home</a>                                |
|------------------------|-------------|----------|--|---|
| Command                |             |          |  | Description   |
| sys                    |             |          |  |   |
|                        | adjtime     |          |  | retrive date and time from Internet                 |
|                        |             | display  |  | display cbuf static                                 |
|                        | 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<br><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]                                      | 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]                                       | 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  |  | display all 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<br>[0:full/1:hourly/2:daily/3:weekly/4:non | mail schedule policy                                |

|  |            |          |  |   |
|--|------------|----------|--|---|
|  |            |          | e]   |   |
|  |            |          | schedule week<br>[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  |
|  | 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  |
|  | stdio      |          | [second]   | change terminal timeout value   |
|  | time       |          | [hour [min [sec]]]   | display/set system time   |
|  | trcdisp    |          |  | monitor packets   |
|  | trclog     |          |  |   |
|  | trcpacket  |          |  |   |
|  | 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   |
|  | socket     |          |  | display system socket information                                     |
|  | filter     |          |  |   |
|  |            | netbios  |  |   |
|  | roadrunner |          |  |   |
|  |            | debug    | <level>  | enable/disable roadrunner service<br>0: diable <default><br>1: enable |
|  |            | display  | <iface name>   | display roadrunner information<br>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.<br>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 |

#### 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              |
|         | edit    |        |             |                                       |
|         |         | load   | <ether no.> | load ether data from spt              |
|         |         | mtu    | <value>     | set ether data mtu                    |
|         |         | save   |             | save ether data to spt                |

#### 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                     |
|         |          | default    | <ip>   | Set default DNS server                     |
|         | httpd    |            |  |  |
|         |          | debug      | [on off]   | set http debug flag                        |
|         | 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>]<br><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.          |
|  | udp        |            |  |   |
|  |            | status     |  | display udp status                                |
|  | rip        |            |  |   |
|  | tcp        |            |  |   |
|  |            | status     | [tcb] [<interval>]                                       | display TCP statistic counters                    |
|  | telnet     |            | <host> [port]  | execute telnet clinet command                     |
|  | tftp       |            |  |   |
|  | 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              |
|  | urlfilter  |            |  |   |
|  |            | exemptZone |  |   |
|  |            |            | display  | display exemptzone information                    |
|  |            |            | actionFlags<br>[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                             |
|  | 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                                       |
|  |            | url        | [num]  | top url hit list                                  |
|  |            | ip         | [num]  | top ip addr list                                  |
|  |            | srv        | [num]  | top service port list                             |

|  |      |            |                             |   |
|--|------|------------|-----------------------------|---|
|  | 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  |
|         |                | 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 #  |
|  | 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   |
|  |              | keyAlive      | <Yes  No>                               | Set keep alive or not   |
|  |              | natTraversal  | <Yes  No>                               | Enable NAT traversal 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       |
|  |  | name       | <string>                            | Set rule name                                 |

#### 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 |