ZyXEL

Firmware Release Note

ZyWALL 1

Release 3.60(WD.1)

Date: May, 5, 2003
Author: Neil Cheng

ZyWALL 1
V3.60(WD.1)
For Standard Release Note

Date: May 5, 2003

Supported Platforms:

ZyXEL ZyWALL 1

Versions:

RAS F/W Version: V3.60(WD.1) | 05/05/2003 09:30:07
Bootbase Version: V2.11 | 02/12/2003 13:58:22

Note:

1. After upgrading to V3.60(WD.0)b4, you should better upload the new default ROM file or reset ZyWALL device to the factory defaults.
2. Bootbase has updated to version 2.11. This version had fixed the product name can't display in eWC page.
3. Pre-Shared Key support hexadecimal format now, but even numbers is required in hexadecimal format. If you just provide odd numbers, the first character will automatically add 0 so that PSK will be even numbers.

Known Issues:

1. 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.
2. 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.
3. Symptom: After system boot up, static route cannot set into routing table.
   Condition: If gateway in static route belongs to WAN interface and if WAN is PPPoE/PPTP encapsulation, static route node will not add in routing table and have no function after ZyWALL reboot. So, users need to reactive static route rule to enable this function.
4. If Peer ID content is blank, and 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.
5. Nat traversal may not be stable when your VPN tunnel connects through it and rekey in a short time. We will modify it in the future.

Feature:

Modification in V3.60(WD.1) | 05/05/2003

Modification in V3.60(WD.1)b1 | 04/29/2003

1. [BUG FIX] Symptom: A special IPSec policies rule will make the ZyWALL can not establish the IPSec tunnel.
   Condition:
   (1) The security gateway is 0.0.0.0
   (2) The peer IP type is IP and the peer ID content is empty or "0.0.0.0".
   (3) The ZyWALL can't establish the IPSec tunnel when the peer site dials in.
2. [BUG FIX] Symptom: ZyWall detects normal DNS answers of as UDP port scan attacks.
   Condition: When router enables syslog service, the DNS reply packets to syslog server are sometimes detected as UDP port scan.
3. [BUG FIX] Symptom: It's a compatibility problem with SonicWall.
   Condition: Can't create the IPSec tunnel with a SonicWall security gateway, if the type of ID Content is FQDN.
4. [BUG FIX] Symptom & Condition: Under heavy traffic, sometimes, ZyWALL's firewall will make system crash.

Modification in V3.60(WD.0) | 04/01/2003

Modification in V3.60(WD.0)b9 | 03/26/2003

1. [ENHANCEMENT] Add eWC wizard WAN IP check – WAN IP address can't set with in LAN subnet.
2. [ENHANCEMENT] Add eWC wizard telia service check – Check relogin value, WAN IP assignment and telia login server should be domain name.
3. [BUG FIX] Symptom: Java and ActiveX can't be blocked when we block cookie.
   Condition: When we enable block cookie, system can't block Java applet and ActiveX object.

Modification in V3.60(WD.0)b8 | 03/18/2003

1. [BUG FIX] Symptom & Condition: Hexadecimal format of pre-shared key on eWC now can't save more than 30 characters.

Modification in V3.60(WD.0)b7 | 03/14/2003

1. [ENHANCEMENT] Hexadecimal format of pre-shared key on eWC now can edit total 64 characters on eWC.
2. [BUG FIX] Symptom: CI command of "ipsec load" error message is not friendly to our users.
   Condition: When loading ipsec rule number greater then system maximum rule number, the error message display error code and not friendly to our users.

Modification in V3.60(WD.0)b6 | 03/10/2003

1. [ENHANCEMENT] Support hexadecimal format of pre-shared key. Now pre-shared key starting with "0x" or "0X" will be treated as hexadecimal format.
   NOTE: If old configuration with leading "0x" or "0X" will also be treated as hexadecimal input when save it again.
2. [ENHANCEMENT] Add a range checker under Ether / PPPoE / PPTP when store WAN – IP setting. This avoids WAN IP set the value within LAN subnet.
3. [ENHANCEMENT] Protected "rom-0" file, when user did not login our router.
4. [FEATURE CHANGE] When the router assigns an IP address to clients or receives an IP address from DHCP server, the IP address of errlog information is changed to hexadecimal format.

5. [FEATURE CHANGE] Remove CI command “sys server” on ZyWALL1.
6. [BUG FIX] Symptom: Enable sending E-mail alert of IKE and using CI command “ipsec dial rule#” will cause ZyWALL crashes.
   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. Select IPSec and IKE alert on the Logs Settings page.
   4. Enter the CI command mode, and issue the CI command “ipsec dial rule#” to create the VPN tunnel.
   5. After seeing the message “Press any key to return....” press the Enter key.
   6. The ZyWALL crashes.
7. [BUG FIX] Symptom: When phase 1 ID check failed, IKE log didn't show the ID content correctly.
   Condition:
   1. Set Peer ID type = IP and leave Peer ID content as blank.
   2. Set different ID content in the peer site.
   3. Establish the tunnel. Due to phase 1 ID content is different, the procedure will fail. But in the log, "configured peer ID content" doesn't show correctly.
8. [BUG FIX] Symptom: Two IPSec hosts can establish IPSec connection when one uses main mode and the other chooses aggressive mode.
   Condition: When local and peer hosts use different IKE phase1 negotiation mode, they still can establish IPSec connection.
9. [BUG FIX] Symptom: Local and peer content can’t change when ID type is IP with CI command.
   Condition: “ipsec config lcIdContent” and “ipsec config peerIdcontent” can’t change the value when ID type is IP.
10. [BUG FIX] Symptom & Condition: Using "MG-SOFT MIB Browser" to get SNMP information (iso.org.dod.internet.mgmt.mib-2.ip.ipAddrTable.ipAddrEntry.ipAdEntIfIndex) twice will cause router crash.
11. [BUG FIX] Symptom & Condition: The errlog type does not match the centralized log type.
12. [BUG FIX] Symptom: Firewall CI command to ignore DoS has a useless DMZ option for those products without DMZ.
    Condition: Use “sys firewall ignore” can set LAN & WAN & DMZ even this product has no DMZ port.

Modification in V3.60(WD.0)b5 | 02/25/2003

1. [FEATURE CHANGE] Change NetBIOS hint message on WAN – IP page. User may need to add a SUA server when setting NetBIOS packet WAN to LAN forwarded.
2. [FEATURE CHANGE] Remove SUA server default setting in ROM file for Road Runner.
3. [BUG FIX] Symptom: Using CI command can create 2 IPSec Rules.
   Condition: Using CI command can configure the second IPSec rule that reserved for remote management tunnel.
4. [BUG FIX] Symptom: ZyWALL1 only have single address type in local, But using CI command can change local address type.
   Condition: Local address type can’t be changed to range and subnet by CI command.
5. [BUG FIX] Symptom: IPSec CI command display the wrong messages.
   Condition: Using “ipsec disp rule#”, the messages are not correct when local/remote address type is range/subnet.
6. [BUG FIX] Symptom: SNMP eWC setting can’t be saved
   Condition: Setting in eWC SNMP page can’t be saved.

Modification in V3.60(WD.0)b4 | 02/14/2003

1. [ENHANCEMENT] Modify the firmware upload successful page.
2. [ENHANCEMENT] Add service type - Telia login.

3. [ENHANCEMENT] Add a protection mechanism for password check. When users enter wrong password three times, the system will block users trying to log in for the minutes that user defined. The blocking time will be set by CI command.
   NOTE: Use CI command "sys pwderrtm [minutes]" to set this timeout value. System will not perform this check when timeout value is empty.
4. [ENHANCEMENT] Add IPSec NAT traversal support. It only supports ESP tunnel and ESP transport when key management is IKE. No manual key support for IPSec NAT traversal.
5. [ENHANCEMENT] In CI command "sys logs display", add a category filter to display only the specified category.
6. [ENHANCEMENT] Add Administrator Inactivity Timer. Let users can specify ZyWALL management session (either via the web configuration or SMT) idle timeout value.
7. [ENHANCEMENT] Add CI commands to configure IPSec rules. Please refer CI command list.
8. [ENHANCEMENT] Add UPnP CI commands. Users can use commands: “sys upnp [active | config | display | firewall | load | save]” to change the UPnP setting.
9. [ENHANCEMENT] The subject of email for the logs can be configuring by CI command "sys logs mail subject".
10. [ENHANCEMENT] Add full path + file name check for keyword blocking.
11. [ENHANCEMENT] ZyWALL can send an alert mail of "access control", "block java etc", "ipsec", and "ike" categories, and the log mail of "ike" category.
12. [ENHANCEMENT] Show the reason of forward/block by content filter in the centralized log message.
13. [ENHANCEMENT] Add centralized logs for phase 1 ID (FQDN).
14. [ENHANCEMENT] Check Point UDP port 2746 timeout value enlarge support.
    NOTE: Use CI command "ip nat timeout udp [port] <seconds>" to change the timeout value.
15. [ENHANCEMENT] Under anti-probe mode the router will drop the IDENT packet without sending the TCP reject packet back to sender. If enabling the reject IDENT function under anti-probe mode, the router will response a reject message to the sender.
    NOTE: Use CI command "ip ident <on|off>” to enable or disable this feature.
16. [FEATURE CHANGE] Make hard-coded NetBIOS CI commands visible by users.
17. [FEATURE CHANGE] Disable windows networking (NetBIOS over TCP/IP) from LAN to WAN and WAN to LAN in default setting.
18. [FEATURE CHANGE] Centralize Log GUI color defines. Block color is normal log messages and red color is alert log messages.
19. [FEATURE CHANGE] LAN DHCP server pool size can be 1.
    NOTE: When the pool size is 1, LAN IP cannot be the same as Client IP Pool Starting Address.
20. [FEATURE CHANGE] When phase 1 ID type is IP and content is blank or 0.0.0.0, ZyWALL will use WAN IP or Secure gateway address as content. In the previous design, only blank content will do. Please refer to appendix for more details.
21. [FEATURE CHANGE] Wording change for firewall log messages. For example: "set:1" will be "L to W" means packet from LAN to WAN.
22. [FEATURE CHANGE] Email log and alert can be sending by setting only “send log” or “send alert” Email address.
23. [BUG FIX] Symptom: WAN side PC can ping router's LAN IP
    Condition: When "firewall off", outside PC can ping router's LAN IP.
24. [BUG FIX] Symptom: The ZyWALL crashes when establishing IPSec connection.
    Condition: When local and peer use different phase 1 authentication algorithms in IKE, both ZyWALL crash.
25. [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.
26. [BUG FIX] Symptom: The blocking cookie feature does not work
    Condition: When connecting to web site that has cookie, the system still let the cookie information passed even if an user has enabled the blocking cookie function.
27. [BUG FIX] Symptom: The content of web forward log message is not correct.
    Condition: If user blocks the keyword "kimo" and access the web site that does not contain the keyword "kimo", the system should generate web forward log message.

28. [BUG FIX] Symptom: eWC-->VPN, manual key cannot save.
    Condition: When saving a manual key rule by eWC, an error message "Manual My ID only can be IP" shows. However manual key rule does not have ID field.
29. [BUG FIX] Fix a security issue related with port scan.
30. [BUG FIX] Symptom: Firewall logs duplicate ICMP type 3 code 3 which reply by itself.
    Condition: When router receives a unknown UDP service packet, it reply ICMP port unreachable and firewall logs this packet twice.
31. [BUG FIX] Symptom: Send an email log with more than 34 logs will cause system crash.
    Condition: In logs->view log in the WEB menu, when the number of logs is more than 34, press "Email Log Now" will cause system crash.
32. [BUG FIX] Symptom: The router can not block java & activex components.
    Condition: When connecting to web site that has java & activex components, ZyWALL can not block them.
33. [BUG FIX] Symptom: When a PC traceroute from LAN to WAN, only 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".
34. [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.
35. [BUG FIX] Symptom: The keyword blocking does not work.
    Condition:
    1. Use CI command "ip urlfilter customize actionFlag fullPath 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.
36. [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.
37. [BUG FIX] Symptom: XBox Live can't work through router.
    Condition: Xbox Live can not work through ZyWALL.
38. [BUG FIX] Symptom: Filter does not log information when blocking cookie.
    Condition: centralized log have no block cookie message.
39. [BUG FIX] Symptom: Content filtering will block keyword that contains *.html.
    Condition:
    1. Use "ip urlfilter customize actionFlag fullPath enable" to enable the full path setting.
    2. Add ".html" to keyword blocking.
40. [BUG FIX] Symptom: UPnP can't save Internet Gateway Services.
    Condition: When we add service in the Internet Gateway, the service can't be saved into the router.

Modification in V3.60(WD.0)b3 | 09/27/2002

1. [ENHANCEMENT] Support UPnP. For more information, please refer Appendix 5.
2. [FEATURE CHANGE] Added Custom Port setup on the Firewall Services page.
3. [FEATURE CHANGE] Added Firewall log selection on the Firewall Setup page.
4. [FEATURE CHANGE] Add more ID supported in IKE phase 1 authentication, includes ID-IP, ID-FQDN, ID-USER-FQDN

Modification in V3.60(WD.0)b2 | 08/21/2002

1. [BUG FIXED] Remote CNM management station can’t configure the ZyWALL device IPSec setting.

Modification in V3.60(WD.0)b2 | 07/31/2002

1. [FEATURE CHANGE] Allow NetBIOS was moved from Firewall setup page to WAN IP setup page. "addNetBios" and "RemoveNetBios" ci commands also be removed. Please see Appendix 3.
2. [ENHANCEMENT] Centralized Logs. New pages for Logs view and settings are added. All firewall logs and IPSec logs are also display on this new Logs page. The old IPSec log and firewall log pages are removed.
3. [ENHANCEMENT] Added new settings into the TimeZone page. They are Time Server setup, current time/current date setup.
4. [ENHANCEMENT] Added New CNM(Central Network Management) feature. CI command "cnm active 1" could be used to active this feature. The default is inactive. CI command "cnm managerIp xxx.xxx.xxx.xxx" is used to specify the IP address of the ZyXEL's CNM management station. For details for CNM, pelase reference to the User Guide for CNM.
5. [FEATURE CHANGED] Triangle route network topology is allowed. We changed the CI command to switch on/off firewall checking for triangle route, and this setting is saved in flash rom. It's "sys firewall ignore triangle all [on|off]". The default value is [off] to ignore triangle route check. For details for Triangle route, please see the Appendix 4

Modification in V3.50(WD.4)b2 | 07/03/2002

1. [BUG FIXED] The IP address of the SNMP trap message is always the LAN side IP address of ZW device.
2. [ENHANCEMENT] Provided new on-line helps for "sys syslog facility…" and "sys syslog type…" CI commands.

Modification in V3.50(WD.4)b1 | 06/28/2002

1. [BUG FIXED] CI command, "sys syslog server …." and "sys syslog facility…" don't work.
2. [BUG FIXED] Can't made changes on the default route setting, by using Web Configurator.
3. [BUG FIXED] When the ZyWALL device receives the TCP datagram with SYN and ACK bits, the corresponding remote managements service would crash.
4. [ENHANCEMENT] SNMP Setup page.

Modification in V3.50(WD.3)b1 | 06/12/2002

5. [BUG FIXED] Fixed the bug of the aggressive mode of IPSec IKE.

Modification in V3.50(WD.2)b3 | 05/29/2002

1. [FEATURE CHANGE] When the DHCP server doesn't response(maybe in a busy state) to ZW1's WAN side, ZW1 will do more DHCP requests.

Modification in V3.50(WD.2)b2 | 05/28/2002

1. [BUG FIXED] The bug of remote management tunnel.
2. [BUG FIXED] NAT/SUA problem on PPPoE dynamic WAN IP situation.
3. [NOTICE] Should reset ZW1 to factory defaults, after upload device F/W to this new version.

Modification in V3.50(WD.2)b1 | 05/16/2002

1. [BUG FIXED] Fragment Packets(with DF flag) can not pass NAT.
2. [BUG FIXED] Turn on Remote Managements on WAN side will cause Firewall holes.

Modification in V3.50(WD.1)b7 | 03/26/2002

4. [ENHANCEMENT] Added more IPSec settings on the web configurator.
5. [ENHANCEMENT] New CI command “ipsec display <rule index>” to display the details of the IPSec rule specified by the rule index.

Modification in V3.50(WD.1)b5 | 03/26/2002

1. [BUG FIXED] Fixed the bug of LAN to LAN forwarding.

Modification in V3.50(WD.1)b5 | 03/07/2002

1. [BUG FIXED] Fixed the bug on Web Configrator’s F/W upload.

Modification in V3.50(WD.1)b4 | 03/06/2002

1. [BUG FIXED] Fixed the bug on PPTP Tunnel (GRE) pass through problem.

Modification in V3.50(WD.1)b3 | 02/25/2002

1. [ENHANCEMENT] Fixed the bug on applying the General Setup page.

Modification in V3.50(WD.1)b2 | 02/25/2002

1. [ENHANCEMENT] New on-line help on IPSec settings.

Modification in V3.50(WD.1)b1 | 02/08/2002

1. [ENHANCEMENT] Active X, Java, Cookie, Web Proxy filtering on Web Configurator
2. [ENHANCEMENT] Allow NetBIOS passing, on Web Configurator
3. [ENHANCEMENT] Added IPSec IKE phase 1 Settings, on Web Configurator.
4. [ENHANCEMENT] VPN LOG is totally revised. Now it will show all IKE packets information.
5. [ENHANCEMENT] IKE process in phase 2 will check ID information between system and the peer. If they don’t match, i.e. both sites have different local / remote Addr setting, system will reject the connection and log in the VPN LOG.
6. [ENHANCEMENT] Add two CI commands : "ppp lcp echo time" and "ppp lcp echo retry" to control echo timer and retry counts. Set one of them to 0 will disable echo request.
7. [FEATURE CHANGE] CI commands for ipsec such as “ipsec sa” and “ipsec sa_sdb_status” are removed. To show SA status, we provide CI command “ipsec show_runtime sa”.
8. [BUG FIX] When two peers initiate connections at the same time in some special cases, the two peers will reject each other and on tunnel can be established.
9. [BUG FIX] When building the tunnel, sometimes system will crash.

Modification in V3.50(WD.0) | 12/10/2001

1. [ENHANCED] Only one LAN side site is allowed to apply to the IPSec feature.
2. [BUG FIXED] URL Blocking can’t work , according the schedule.
3. [ENHANCED] Put default PPTP settings(my PPTP IP and PPTP server IP) on Wizard.
4. [BUG FIXED] Soft-PK deleting phas 1 will cause long delay to re-connection
5. [BUG FIXED] Continue pinging through VPN tunnel will cause the connection unstable.

6. [ENHANCED] Some modifications on Web Configurator online help.
7. [BUG FIXED] When a SA time-out happened and reconnect, sometimes system losts some memory resources. After a longer connection, the system resources will be exhausted.
8. [BUG FIXED] VPN timeout re-connection function is not robust.
   → When "SA Life time" is time out, sometimes the VPN tunnel cannot be re-established again. This is cause of IPSec IKE stress test fail.
9. [ENHANCEMENT] Added a Time Zone setting page on web configurator.
10. [ENHANCEMENT] Removed NAT=NONE selection on WAN setup page.
11. [BUG FIXED] Firewall doesn't work on PPPoE.
12. [BUG FIXED] The site on the WAN's side can ICMP ping the LAN's side station which is with a private IP address.

13. [ENHANCEMENT] Added on-line help for VPN/IPSec and Firewall setup on Web Configurator.
14. [BUG FIXED] Fixed bugs about VPN/IPSec on manually key mode.

15. [ENHANCEMENT] Combined firewall access control setting and SUA setting on the SUA/NAT web GUI page. ZyWall 1 will build proper firewall access control rules when the user do the SUA setting on web configurator

Appendix:

1. SUA Support Table

The required settings of Port forwarding for some applications are listed in the following table.

SUA Support Table

Traffic Type	Application Version	Required Settings in Menu 15 Port/IP	
		Outgoing Connection	Incoming Connection
HTTP	Netscape, IE	None	80/client IP
FTP	Windows FTP, Cuteftp	None	21/client IP
TELNET	Windows Telnet, Neterm	None	23/client IP (and remove Telnet filter in WAN port)
POP3	Eudora	None	110/clinet IP
SMTP	Eudora	None	25/client IP
IRC	mIRC,Microsoft Chat	None for Chat. DCC support: MIRC < 5.31	None
PPTP	Windows PPTP	None	1723/client IP
ICQ	ICQ 99a	None for Chat. For file transfer, we must enable ICQ-preference-connections-firewall and set the firewall time out to 80 seconds in firewall setting.	Default/client IP
Cu-SeeMe	Cornell 1.1	None	7648/client IP
	White Pine 3.1.2	7648/client IP & 24032/client IP	Default/client IP
	White Pine 4.0 (CuSeeMe Pro)	7648/client IP & 24032/client IP	Default/client IP
NetMeeting	Microsoft NetMeeting 2.1 & 2.11	None	1720/client IP

			1503/client IP
Cisco IP/TV	Cisco IP/TV 2.0.0	Default/client IP	
RealPlayer	RealPlayer G2	None	
VDOLive		None	
Quake	Quake1.06	None	Default/client IP
QuakeII	QuakeII2.30	None	Default/client IP
QuakeIII	QuakeIII1.05beta	None	
StartCraft		6112/client IP	
Quick Time	Quick Time 4.0	None	
IPSEC (ESP)		None (only one client)	Default
MSNP	Microsoft Messenger service V3.0	6901/client IP	6901/client IP

2. Procedure to set MTU for LAN and WAN.

The procedure to set MUT is load parameter first, set MTU, and then save them back.

1) For LAN:
   ether edit load 1
   ether edit mtu <value>
   ether edit save

2) For WAN:
   sys rn load 1
   sys rn mtu <value>
   sys rn save

3. Hard-coded packet filter for "NetBIOS over TCP/IP"

The new set C/I commands are under "sys filter netbios" sub-command.
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:       Block
  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 NB/IP packets

sys filter netbios config 1 off => forward WAN to LAN NB/IP packets
sys filter netbios config 6 on => block IPSec NB/IP packets
sys filter netbios config 7 off => disable trigger dial

NOTE: Since one of "WAN to LAN" or "LAN to WAN" switch will affect packets transmitted through ZyWALL, if you need to access PCs on LAN side, please turn these two switch to "forward". We will combine this two switches to a single one in the future.

4. Traffic Redirect/Static Route/Policy Route Application Note

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

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

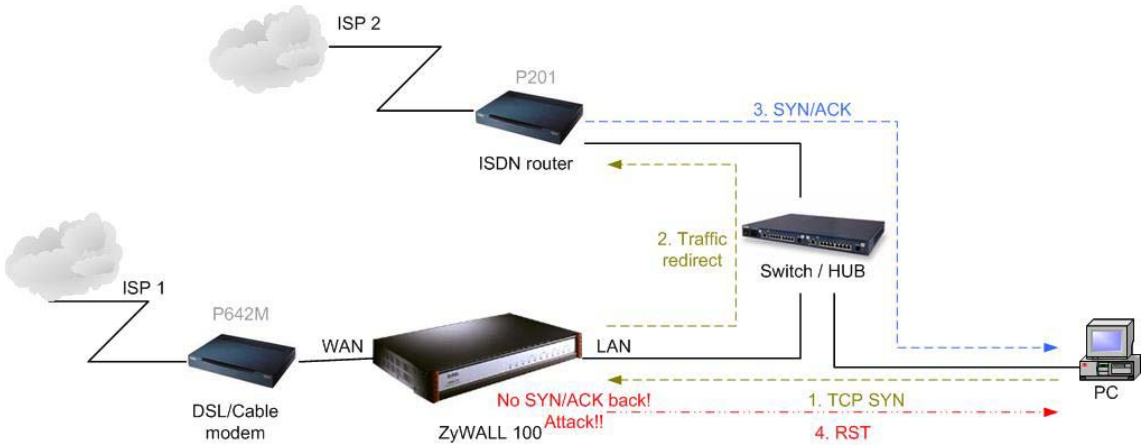

Figure 4-1 Triangle Route

Figure 4-1 indicates the triangle route topology. It works fine with turn off firewall. Let's take a look into the perspective toward this situation.

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

That causes all of outgoing TCP traffics being reset!

How traffic redirect/static/policy 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.

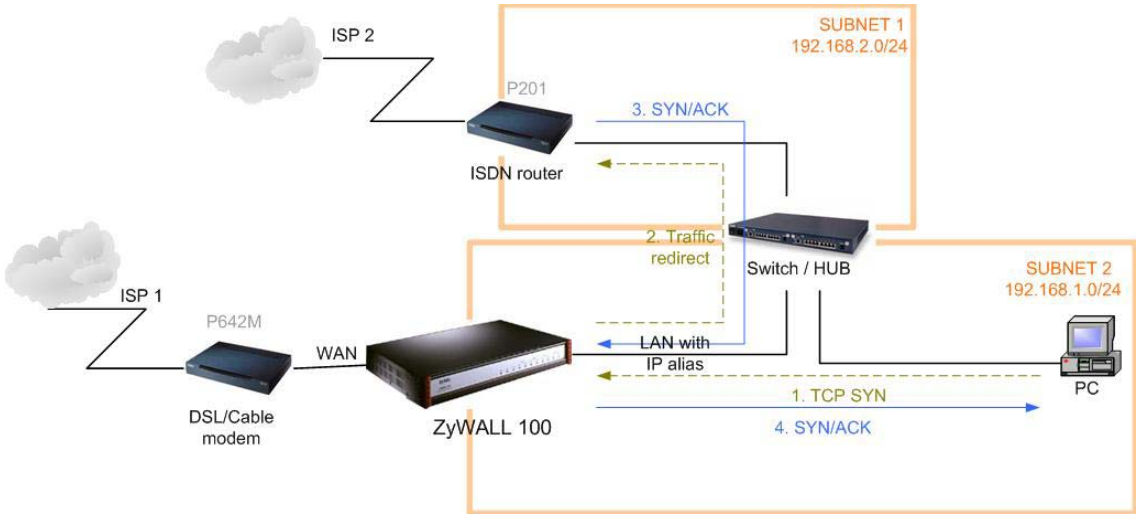

Figure 4-2 Gateway on alias IP network

(2) Gateway on WAN side

A working topology is suggested as below.

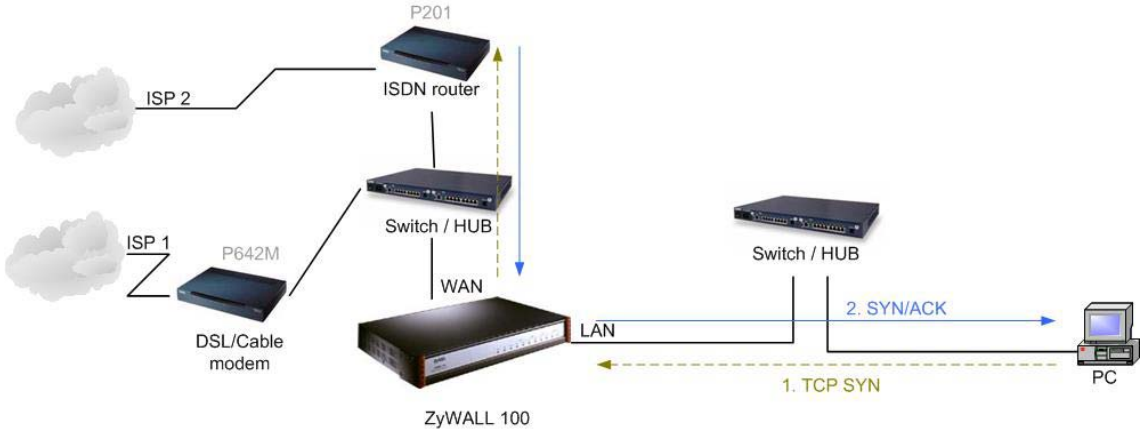

Figure 4-3 Gateway on WAN side

5. UPnP

What is UPnP: Universal Plug and Play(UPnP) is an architecture for pervasive peer-to-peer network connectively of PCs and intelligent devices or appliances, particularly within the home. UPnP builds on Internet standards and technologies, such as TCP/IP, HTTP, and XML, to enable these devices to automatically connect with one another and work together to make networking- particularly home networking- possible for more people.

Discovery: Once devices are attached to the network and addressed appropriately, discovery can take place. If you attach your router to the Windows XP or Me then you can find your device in Network Place.

NAT Traversal: Put simply: NAT can “break” many of the compelling new PC and home networking experiences, such as multiplayer games, real time communications, and other peer-to-peer services, that people increasingly want to use in their homes or small businesses. These applications will break if they use private address on the public Internet or simultaneous use of the same port number. Application must use a public address and for each session a unique port number. Large organizations have professional IT staff on hand to ensure their corporate applications can work with NAT, but smaller organizations and consumers do

not have this luxury. UPnP NAT Traversal can automatically solve many of the problems the NAT imposes on applications, making this an ideal solution for small businesses and consumers.

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.

7. Annex A CI Command List

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
			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 <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 [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
	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]	
	rn			
		load	<entry no.>	load remote node information
		disp	<entry no.>(0:working buffer)	display remote node information
		nat	<none|sua|full_feature>	config remote node nat
		nailup	<no|yes>	config remote node nailup
		mtu	<value>	set remote node mtu
		save	[entry no.]	save remote node information
	smt			not support in this product
	stdio		[second]	change terminal timeout value
	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
	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		

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-incomplete <0~255>		The threshold to start executing the block field
		set <set#>	name <desired name>		Edit the name for a set
			default-permit <forward|block>		Edit whether a packet is dropped or allowed when it does not match the default set
			icmp-timeout <seconds>		Edit the timeout for an idle ICMP session before it is terminated
			udp-idle-timeout <seconds>		Edit the timeout for an idle UDP session before it is terminated
			connection-timeout <seconds>		Edit the wait time for the SYN TCP sessions before it is terminated

			fin-wait-timeout <seconds>		Edit the wait time for FIN in concluding a TCP session before it is terminated
			tcp-idle-timeout <seconds>		Edit the timeout for an idle TCP session before it is terminated
			pnc <yes|no>		PNC is allowed when 'yes' is set even there is a rule to block PNC
			log <yes|no>		Switch on/off sending the log for matching the default permit
			rule <rule#>	permit <forward|block>	Edit whether a packet is dropped or allowed when it matches this rule
				active <yes|no>	Edit whether a rule is enabled or not
				protocol <0~255>	Edit the protocol number for a rule. 1=ICMP, 6=TCP, 17=UDP...
				log <none|match|not-match|both >	Sending a log for a rule when the packet none|matches|not match|both the rule
				alert <yes|no>	Activate or deactivate the notification when a DoS attack occurs or there is a violation of any alert settings. In case of such instances, the function will send an email to the SMTP destination address and log an alert.
				srcaddr-single <ip address>	Select and edit a source address of a packet which complies to this rule
				srcaddr-subnet <ip address> <subnet mask>	Select and edit a source address and subnet mask if a packet which complies to this rule.
				srcaddr-range <start ip address> <end ip address>	Select and edit a source address range of a packet which complies to this rule.
				destaddr-single <ip address>	Select and edit a destination address of a packet which complies to this rule
				destaddr-subnet <ip address> <subnet mask>	Select and edit a destination address and subnet mask if a packet which complies to this rule.
				destaddr-range <start ip address> <end ip address>	Select and edit a destination address range of a packet which complies to this rule.
				tcp destport-single <port#>	Select and edit the destination port of a packet which comply to this rule. For non-consecutive port numbers, the user may repeat this command line to enter the multiple port numbers.
				tcp destport-range <start port#> <end port#>	Select and edit a destination port range of a packet which comply to this rule.
				udp destport-single <port#>	Select and edit the destination port of a packet which comply to this rule. For non-consecutive port numbers, users may repeat this command line to enter the multiple port numbers.
				udp destport-range <start port#> <end port#>	Select and edit a destination port range of a packet which comply to this rule.
				desport-custom <desired custom port name>	Type in the desired custom port name
delete	firewall	e-mail			Remove all email alert settings
		attack			Reset all alert settings to defaults
		set <set#>			Remove a specified set from the firewall configuration
		set <set#>	rule <rule#>		Remove a specified rule in a set from the firewall configuration
insert	firewall	e-mail			Insert email alert settings
		attack			Insert attack alert settings

		set <set#>			Insert a specified rule set to the firewall configuration
		set <set#>	rule <rule#>		Insert a specified rule in a set to the firewall configuration
cli					Display the choices of command list.
debug	<1|0>				Turn on|off trace for firewall debug information.

IP Related Command Home

Command				Description
ip				
	address		[addr]	display host ip address
	alias		<iface>	alias iface
	aliasdis		<0|1>	disable alias
	arp			
		status	<iface>	display ip arp status
	dhcp		<iface>	
		client		
			release	release DHCP client IP
			renew	renew DHCP client IP
		status	[option]	show dhcp status
	dns			
		query		
		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
	udp			
		status		display udp status
	rip			
	sidepath			
		clear		clear side path
		disp		display side path
		set	<iface> <gateway>	set side path
	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
	forceproxy		<display|set> [on|off] [servicePort] [proxyIp] [proxyport]	enable TCP forceproxy
	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 [filterList/disableAllExceptTrusted/ unblockRWFToTrusted/keywordBl ock/fullPath/caseInsensitive/fileNa me][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
		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
		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
		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

ZyWALL 1 Standard Default Romfile Setting and Feature bits

```
ras> sys view autoexec.net
sys errctl 0
sys trcl level 5
sys trcl type 1180
sys trcp cr 96 128
sys trcl sw off
ip tcp mss 1460
ip tcp limit 2
ip tcp irtt 65000
ip tcp window 32
ip tcp ceiling 6000
ip rip activate
ip rip merge on
```

```
ip icmp disc enif0 off
ip antiprobe 1
ppp ipcp com off
sys wd sw off
sys mbuf debug off
ip nat loopback on
```

Feature Bits:

```
ZyWALL 1> atsh
ZyNOS Version           : V3.60(WD.0)b6 | 03/10/2003 16:54:53
Bootbase Version        : V2.11 | 02/12/2003 13:58:22
Vendor Name             : ZyXEL
Product Model           : ZyWALL 1
ZyNOS Code Model        : RAS zw1
HTP Code Model          : HTP_zw1 V 0.10
ZyNOS ROM address       : 06008000
System Type             : 5
MAC Address             : 00A0C54F3217
Default Country Code    : FF
Boot Module Debug Flag : 01
RomFile Version         : 01
RomFile Checksum        : 75e3
ZyNOS Checksum          : 28d5
Core Checksum           : ec5d
SNMP MIB level & OID    : 060102030405060708091011121314151617181920
Main Feature Bits       : C0
Other Feature Bits      :
          50 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00-00 41 33 00 00 04
( Default Country Code, Debug Flag, Romfile Version, MAC Address may
  be difference in Release )
```