



**Firmware Release Note**

**ZyWALL 70**

**Release 3.62(WM.7)**

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

**Sep, 16, 2004**  
**Neil Cheng**  
**Lorin Yeh**

# **ZyXEL ZyWALL 70 Standard Version**

## **Release 3.62(WM.7)**

### **Release Note**

---

**Date:** Sep 16, 2004

#### **Supported Platforms:**

---

ZyXEL ZyWALL 70

#### **Versions:**

---

ZyNOS Version: V3.62(WM.7) | 09/16/2004

BootBase : V1.06 | 04/29/2004 16:11:40

#### **Notes:**

---

1. **Restore to Factory Defaults Setting Requirement: No.**
2. The secondary WAN interface, or WAN 2, is "Backup Line". It is the backup of the Primary WAN 1. If you want to make the WAN 2, go to SMT 11 to setup the second Remote Node and active it. WAN 2 will bring-up automatically when WAN 1 connection fails.
3. The setting of ignore triangle route is on in default ROM FILE. Triangle route network topology has potential security crisis. If you are not clear about it, please refer to Appendix for the triangle route issue.
4. IKE process in phase 2 will check ID information between system and the peer. If you found that the IPSec connection is failed, please check your settings.
5. Using Web to configure VPN, the phase 1 algorithms have been fixed to DES + MD5. If other algorithms are preferred, please use ADVANCE page to configure them.
6. When firewall turns from "off" to "on", the firewall initialization procedure will disconnect all connections running through the ZyWALL.
7. SUA/NAT address loopback feature was enabled on ZyWALL by default, however, if users do not need it, a C/I command "ip nat loopback off" could turn it off.
8. In WLAN configuration, a switch for enable / disable WLAN is added. The default value is "**disable**" since WLAN without any security setting is vulnerable. Please configure MAC filter, WEP and 802.1X when you enable WLAN feature.
9. When UPnP is on, and then reboot the router, Windows XP will not detect UPnP and refresh "My Network Places→Local Network". Plug in network wire again can solve this problem.
10. The default max NAT session number per host is changed to 1500.

## Known Issues:

---

1. If the metric of dial-backup is smaller (has higher priority) than the metric of Traffic-Redirect, Traffic-Redirect can't be triggered any more.
2. Sometimes on screen the "Local Area Connection" icon for UPnP disappears. The icon shows again when restarting PC.
3. When you use MSN messenger, sometimes you fail to open special applications, such as whiteboard, file transfer and video etc. You have to wait more than 3 minutes and retry these applications..
4. On the SUA/ Address Mapping page, users can enter two or above same rules.
5. On the SUA/ Address Mapping Edit page, the user can give the same local IP and global IP.
6. SMT 15.1, if we try to edit the 11<sup>th</sup> rule, the system returns some weird characters.
7. You must notice those metric values of WAN 1, WAN 2, Traffic-Redirect and Dial-backup. You should better give those values, Dial-backup > Traffic-Redirect > WAN 2 > WAN 1. For example, WAN 1(1), WAN 2(2), Traffic-Redirect(14), Dial-backup(15).
8. Bandwidth Management doesn't work on wireless LAN.
9. Sometime, modify an active IPsec rule (the VPN tunnel was created) will crash the system, if this tunnel is going the re-key process.
10. Can't block ActiveX in some case.
11. System may need to reboot when change the SNMP port number.
12. P2P device may not work with SIP ALG on ZyWALL 70.
13. H.323 may not work with following scenario:  
PC1 ↔ ZyWALL ↔ internet ↔ ZyWALL ↔ PC2.
14. When perform SPT partial reset via Vantage, device wouldn't reset all system parameters.
15. Device can't delete address mapping via Vantage.
  - 1).Let device registers to Vantage.
  - 2).Add 2 address-mapping rules via Vantage.
  - 3).Delete 1 address-mapping rule via Vantage. The rule can't be deleted.
16. Delete 1 address-mapping rule via Vantage. The rule can't be deleted.
17. CNM agent can register to Vantage success with different encryption key.
  - 1).Set encryption mode with "DES" and encryption key with "12345678" on Vantage.
  - 2).Set encryption mode with "DES" and encryption key with "12345679" on CNM agent.
  - 3).CNM agent can register to Vantage successfully.

## Features:

---

### Modifications in V 3.62(WM.7) | 09/16/2004

Modify for formal release.

### **Modifications in V 3.62(WM.7)b3 | 09/10/2004**

1. [FEATURE CHANGE] The three content filter customize flags - "Block full path", "Case insensitive" and "Block file name" are enabled by default.
2. [FEATURE CHANGE] Set maximum concurrent NAT sessions per host to 1024.
3. [ENHANCEMENT] Enhance "cnm keepalive" ci command. Add "cnm keepalive 0" command to stop sending of keepalive packet to Vantage.
4. [BUG FIX] Symptom: Symptom: FTP from WAN to LAN does not work.  
Condition:
  - 1). Set a FTP server on a host in the LAN side and configure a default server to this host.
  - 2). Using FTP from WAN to the default server with port mode.
  - 3). After typing username and password, "ls" command does not work.
5. [BUG FIX] Symptom: LAN host will get wrong DNS server.  
Condition:
  - 1). Set SMT 3.2 DNS first DNS server as user defined 1.1.1.1. Others are none.
  - 2). Unplug WAN port and reboot.
  - 3). LAN host get IP address and DNS server and the DNS server is LAN IP.
6. [BUG FIX] Symptom: System Crash when change encryption key in Vantage.  
Condition:
  - 1). Device register to Vantage in router mode under DES and PPPoE.
  - 2). configuration>>general>>system change the original encryption key and apply
  - 3). Device receives data but soon the system crash.
7. [BUG FIX] Symptom: WAN Gateway will be reset to 0.0.0.0.  
Condition:
  - 1). In Vantage CNM add a device (the device have a static IP),when it register to Vantage. Vantage set default value to device.
  - 2). After the device reset, WAN Gateway will be reset to 0.0.0.0.
8. [BUG FIX] Symptom: CNM agent accepts wrong CI command "cnm keepalive -3231231222222222222222".  
Condition:
  - 1). In SMT 24.8, type "cnm keep -3231231222222222222222".
  - 2). The system accepts it and saves with the value.
9. [BUG FIX] Symptom: CNM agent accepts wrong CI command "cnm encrymode 1231223".  
Condition:
  - 1). In SMT 24.8, type "cnm encrymode 1231223".
  - 2). The system accepts it and read it as "65535".
10. [BUG FIX] Symptom: [Vantage] Configuration>>VPN: When delete a active VPN tunnel successfully. Device sends VPN tunnel status "Destroy" to vantage.  
Condition:
  - 1). Create and dial up a VPN tunnel via Vantage.
  - 2). Delete this active rule in Vantage.
  - 3). Vantage server will have exception.
11. [BUG FIX] Symptom: Switch NAT mode of device from Vantage. Vantage can't get response packet from device.  
Condition:
  - 1). Edit a correct address mapping rule via Vantage.
  - 2). Switch NAT mode: none/full feature/SUA. Then you will find sometimes device

return -6000 (no difference). But there is difference. In the meanwhile, the NAT mode didn't change in device side. If device return 0, Vantage cannot get the response.

12. [BUG FIX] Symptom: [Vantage] Configuration >> WAN >> General >> WAN: Route not work.

Condition: Configure WAN >> General: WAN route on Vantage. Modify "traffic redirect priority" value and click apply button. The change can't be saved to router.

13. [BUG FIX] Symptom: System reboots as a result of memory leaks caused by ZyReport.

Condition:

- 1). Enable ZyReport.
- 2). Access huge amount of URLs which will be counted by ZyReport.
- 3). The system will run out of available memory sections and eventually reboot.

### **Modifications in V 3.62(WM.7)b2 | 08/13/2004**

1. [ENHANCEMENT] Support user config for SIP session timeout value
2. [ENHANCEMENT] ALG enable/disable setting can be saved in rom file. Note: SIP and H.323 is disabled with default setting.
3. [ENHANCEMENT] In LOGS > Log Settings page, add "Asymmetrical Routes", "Multicasts/ Broadcasts" log setting items under Access Control.
4. [BUG FIX] Symptom: Sometimes the ZyWALL reboots by software watchdog.  
Condition:
  - 1). Put the ZyWALL on the network for a long time.
  - 2). Sometimes the ZyWALL will reboot by software watchdog.
5. [BUG FIX] Symptom: H.323 can not pass through firewall from WAN to LAN.  
Condition:
  - 1). Set one firewall rule that forward H.323(TCP:1720) from WAN to LAN.
  - 2). H.323 phone call setup from WAN to LAN failed.
6. [BUG FIX] Symptom: Content filter timeout problem.  
Condition:
  - 1). A router is register the content filter (CF) server.
  - 2). Enable the CF feature.
  - 3). Enable the external database content filtering.
  - 4). The router log often record "Waiting content filter server (server name) timeout!".
  - 5). A PC in LAN fetch web from internet often hangs for a while.
7. [BUG FIX] Symptom: IKE negotiations will success when PFS parameter is different between Initiator and Responder.  
Condition:
  - 1). Initiator has only one rule without PFS.
  - 2). Responder has only one rule with PFS parameter is DH1.
  - 3). Initiator dial to Responder.
  - 4). Tunnel establishment will success, but should fail in this case.

### **Modifications in V 3.62(WM.7)b1 | 07/15/2004**

1. [ENHANCEMENT] Add Unified ALG for SIP and H.323.
2. [ENHANCEMENT] Each unified ALG can be enabled/disabled. Default is enabled.
3. [ENHANCEMENT] Firewall can bypass AX.25 (protocol #93) & IPv6 (protocol #41)

- protocols.
4. [ENHANCEMENT] Added a web page in the eWC > Remote MGMT for Vantage CNM.
  5. [BUG FIX] Symptom: Router block trusted web content.  
Condition:
    - 1). In "eWC->CONTENT FILTER->General", enable content filter.
    - 2). In "eWC->CONTENT FILTER->Customization", select check boxes of "Enable Web site customization" and "Disable all Web traffic except for trusted Web sites".
    - 3). In "eWC->CONTENT FILTER->Customization", set "www.hellowork.go.jp" as trusted web site.
    - 4). Open browser and access  
<http://www.hellowork.go.jp/kensaku/servlet/kensaku?pageid=001>
    - 5). In the new page, select third and fourth radio button and click "search" button.
    - 6). In the new page, click "next page" button.
    - 7). The new page will be blocked.
  6. [BUG FIX] Symptom: External Content Filtering cannot block the URL belonging to restricted category.  
Condition:
    - 1). In "eWC->CONTENT FILTER->Customization", unselect "Enable Web site customization".
    - 2). Add a URL to "trusted web sites".
    - 3). In "eWC->CONTENT FILTER->Customization", select "Block Web sites which contain these keywords".
    - 4). In "eWC->CONTENT FILTER->Categories", select the category which the URL belongs to.
    - 5). Access the trusted URL.
    - 6). The URL will not be blocked.
  7. [BUG FIX] Symptom: System crash by memory leak.  
Condition:
    - 1). Enable bandwidth management.
    - 2). Into eWC->Bandwidth Management->Monitor and wait for a period time.
    - 3). System crash by memory leak.
  8. [BUG FIX] Symptom: Remote node CI command crashes.  
Condition:
    - 1). Goto SMT 24.8
    - 2). Load dial backup remote node to working buffer.
    - 3). Type CI command "sys rn accessblock 0".
    - 4). Save this remote.
    - 5). System crashes.
  9. [BUG FIX] Symptom: For UPnP, MSN Messenger 6.1 voice function cannot work.  
Condition:
    - 1). Network topology: PC\_A <--> Router\_A <--> internet <--> Router\_B <--> PC\_B.
    - 2). PC\_A and PC\_B add Windows UPnP components.
    - 3). Router\_A and Router\_B enable UPnP function.
    - 4). The MSN Messenger 6.1 voice function cannot work between PC\_A and PC\_B.
  10. [BUG FIX] Symptom: Router will crash.  
Condition:
    - 1). Force router to execute many DNS queries.
    - 2). Router sometimes will crash.

11. [BUG FIX] Symptom: System crashes.  
Condition: Configure device by eWC sometimes cause crash.
12. [BUG FIX] Symptom: MSN Messenger's "Ask for Remote Assistance" function causes system crash.  
Condition:
  - 1). Enable UPnP.
  - 2). Set PC(A) and router(B) in intranet and PC(C) connects to LAN port of router(B).
  - 3). Test MSN Messenger's "Ask for Remote Assistance" function from PC(A) to PC(C).
  - 4). After PC(C) accepts the PC(A) request by "Ask for Remote Assistance" then the device will crash.
13. [BUG FIX] Symptom: System out of memory.  
Condition:
  - 1). Let the ZyWALL be a DNS proxy for LAN hosts.
  - 2). Do a lot of DNS inverse queries by running IPScan tool continuously from LAN host.
  - 3). After a long time, the ZyWALL will out of memory.
14. [BUG FIX] Symptom: Packets cannot pass through NAT router to LAN hosts.  
Condition:
  - 1). NAT default server is on
  - 2). Protocol of the packet is not TCP, UDP, ICMP, ESP, GRE.
  - 3). Packets from WAN to router.
  - 4). Packets cannot pass through NAT router to LAN hosts (NAT default server)
15. [BUG FIX] Symptom: External content filtering cannot register.  
Condition:
  - 1). In "eWC->content filter->categories", click "register" to connect to ZSSW.
  - 2). Do the registration on ZSSW.
  - 3). The registration will fail in the final step.
16. [ENHANCEMENT] External content filtering support full URL checking.  
Was: External content filtering only take domain name or IP address of URL into category checking.  
Is: External content filtering put entire URL into category checking.
17. [BUG FIX] Symptom: Router will crash.  
Condition:
  - 1). A host connects to router.
  - 2). User accesses website then disconnect.
  - 3). After 2 hours, user accesses website again.
18. [ENHANCEMENT] Centralized log add
  - 1). Triangle route log switch.
  - 2). Broadcast/Multicast log switch.Note: Add CI commands:
  - a. "sys logs switch".
  - b. "sys logs switch dispaly".
  - c. "sys logs switch bmlog <0:no|1:yes>".
  - d. "sys logs switch trilog <0:no|1:yes>".
19. [BUG FIX] Symptom: In SMT.4, the config menu won't change when changing the encapsulation from Ethernet to PPTP or PPPOE.  
Condition:
  - 1). Make sure WAN2 is on.
  - 2). Go to SMT.4.

- 3). Switch encapsulation to Ethernet.
- 4). Try to switch to PPTP or PPPOE. The config menu should change, but it won't.
- 20. [BUG FIX] Symptom: System out of memory and reboot when firewall enable.  
Condition:
  - 1). Enable firewall, then generate traffic.
  - 2). The memory will slowly leak until it uses up all the memory, then reboot.
- 21. [BUG FIX] Symptom: Generate a lot of TCP port 80 sessions to ZyWALL will cause device to hang and reboot by hardware watchdog.  
Condition:
  - 1). Use session.exe to generate a lot of TCP port 80 sessions to ZyWALL's LAN or WAN interface
  - 2). After several hundreds of sessions are established, the ZyWALL will hang and finally reboot.
- 22. [BUG FIX] Symptom: eWC spelling error.  
Condition: eWC->Firewall->Default Rule: Allow Asymmetrical should be Asymmetric.
- 23. [BUG FIX] Symptom:[Vantage] Configuration >> WAN >> General >> WAN: Route not work.  
Condition: Configure WAN >> General: WAN route on Vantage. Modify "traffic redirect priority" value and click apply button. The change can't be saved to router.
- 24. [BUG FIX] Symptom: IKE negotiation fails when NAT traversal is enabled.  
Condition: When enabling NAT traversal and setting local ID type as DNS or Email, IKE negotiation fails.

#### **Modifications in V 3.62(WM.6) | 06/18/2004**

Modify for formal release.

#### **Modifications in V 3.62(WM.6)b1 | 06/09/2004**

- 1. [BUG FIX] Symptom: Device can't register to Linux version Vantage.  
Condition:
  - (1) Device active cnm and start register process.
  - (2) Device sends register request packet to Vantage.
  - (3) Vantage responds register response packet to device and device get new SGID from the packet.
  - (4) Device save new SGID and try to re-register to Vantage again.
  - (5) Device can't register to Vantage successfully anymore.
- 2. [FEATURE CHANGE] If the SGID of device is changed then device will reset SGMP state machine (cnm reset).  
This is modified as follows:
  - (1) If SGID is changed when SGMP is in the state of SGMP\_STATE\_ACTIVE, then device will reset SGMP state machine.
  - (2) If SGID is changed when SGMP is in other states, such as registering to Vantage, then device will not reset SGMP state machine.
- 3. [BUG FIX] Symptom: Some trusted web sites' pictures cannot be seen.  
Condition:



- (1) In "eWC->CONTENT FILTER->Customization", select "Disable all Web traffic except for trusted Web sites" and "Don't block Java/ActiveX/Cookies/Web proxy to trusted Web sites".
- (2) At the same page, add "kobeoffshore.com" to "Trusted Web Sites".
- (3) Open web browser to access "kobeoffshore.com"
- (4) All the pictures cannot be seen.
4. [BUG FIX] Symptom: When more than two ZyWALL70s reboot at the same time, some ZyWALL70s will get the same IP address on WAN interface.  
Condition: On Vantage, perform firmware upgrade to two or more ZyWALL70s at the same time. After firmware upgrade complete and reboot, ZyWALL70s will re-register to Vantage. But some ZyWALL70s fail to register to Vantage and they have the same IP address on WAN interface.
5. [BUG FIX] Symptom: In SMT 1, change DNS server with User-Defined IP address, it does not save to ROM.  
Condition:
  - (1) In SMT 1, change DNS server with User-Defined.
  - (2) Set a User-defined IP address.
  - (3) Save it to ROM file.
  - (4) Change User-defined IP Address with new one.
  - (5) New DNS IP address do not change after rebooting the system.
6. [BUG FIX] Symptom: Fixed a wording error "DNS Server" in eWC>WAN>DDNS.  
Condition:
  - (1) Go to eWC>WAN>DDNS>IP Address Update Policy> DNS server auto detect IP Address(a radio button).Or go to SMT1.1>DNS Server Auto Detect IP Address.
  - (2) The words "DNS server" in "DNS server auto detect IP Address" should be "DDNS server".
7. [FEATURE CHANGE] Remove CI command "smtp" in ip category.
8. [BUG FIX] Symptom: CI "config" command does not work.  
Condition: In SMT 24.8, type "config", it won't work.
9. [BUG FIX] Symptom: There are error wordings in SMT's DDNS page .  
Condition:
  - (1) Goto SMT DDNS page.
  - (2) Some wordings are not identical with eWC->WAN->DDNS.
10. [BUG FIX] Symptom: DDNS Password value error.  
Condition:
  - (1) WAN>>DDNS fillup "Host Name 1"(aaa) "Username"(user) and "Password"(1234567890123456789012345678901) "Password" fill up 31 characters(Max length) ,Apply
  - (2) On SMT Menu 24.8
  - (3) CI command "sys ddns debug 1" CI command "sys ddns display"
  - (4) We can find filed "Password" show "1234567890123456789012345678901aaa"
11. [BUG FIX] Symptom:Set remote access (SSH service) to a certain interface such as LAN, this setting cannot be saved.  
Condition:Configure ZW70 via https, after set remote access (SSH service) to certain interface such as LAN, this setting cannot be saved
12. [BUG FIX] Symptom: Router crashes and reboots.

Condition: Computers are behind ZyWALL's LAN and run eMule to download large files. After ten hours ago, the system crash.

13. [BUG FIX] Symptom: The system might crash when enabling IPSec.

Condition: During IKE negotiation the system might crash.

14. [BUG FIX] Symptom: The "Enable off line option" check box in eWC->WAN->DDNS will dis-editable.

Condition:

(1) eWC->WAN->DDNS->DDNS Type is Custom and click "Enable off line option", click Apply.

(2) Reload this page, "Enable off line option" will become dis-editable.

15. [BUG FIX] Symptom: Trigger port will disappear after system reboot.

Condition:

(1) Configure Trigger port rule.

(2) System reboot.

(3) The configured Trigger port rule disappear.

#### **Modifications in V 3.62(WM.5) | 05/26/2004**

Modify for formal release.

#### **Modifications in V 3.62(WM.4) | 05/07/2004**

Modify for formal release.

#### **Modifications in V 3.62(WM.4)b2 | 05/05/2004**

1. [BUG FIX] Symptom: System may crash after transmmitting packets under 100 VPN tunnels after a while of time.

Condition:

(1) Setup 100 VPN rules.

(2) Trigger all VPN tunnels.

(3) Keep transmitting packets between all VPN tunnels.

(4) Router will crash after a while time.

2. [BUG FIX] Symptom: CI command "ip url web cache timeout" shows the wrong prompt.

Condition:

(1) Enter CI command mode in SMT.

(2) Type "ip url web cache timeout 0".

(3) It's will show prompt "Invalid timeout number(1~30)".

#### **Modifications in V 3.62(WM.4)b1 | 04/29/2004**

1. [BUG FIX] Symptom: When setting my IP address in IKE as the global IP address in the address mapping rules (SMT 15.1) and setting the NAT as full feature, IKE will

fail.

Condition:

- (1) Set the NAT as full feature (SMT 4).
  - (2) Set one rule in the address mapping rules in NAT setting (SMT 15.1).
  - (3) Set IKE responder's my IP address as the global IP address in the address mapping rules.
  - (4) When the responder receives the IKE packet, it will reply the IKE payload with WAN IP address, instead of my IP address, thus the IKE will fail.
2. [BUG FIX] Symptom: Traceroute or PingPlotter are not able to discover ZyWALL's LAN interface.

Condition:

- (1) Running Traceroute or PingPlotter on desktop.
  - (2) Both applications can not discover ZyWALL's LAN interface.
  - (3) Firewall log shows "Unsupported/out-of-order ICMP: ICMP(type:11, code:0)".
3. [BUG FIX] Symptom: System memory leak and eventually causing the reboot.

Condition:

- (1) Establish a IPSec IKE tunnel, and the tunnel's key life time is short.
  - (2) Continue transmitting heavy traffic through this tunnel.
  - (3) Rekey many times.
  - (4) System will run out of memory and become very unstable.
4. [BUG FIX] Symptom: Router will crash.  
Condition: Use CI command "ip urlfilter webControl cache timeout"
5. [BUG FIX] Symptom: Can't set wireless channel ID when country code is 219 (France).

Condition:

- (1) Set country code with 219.
  - (2) Set channel ID with 6 - 13 via SMT or eWC.
  - (3) After applying changes, the channel ID will resotre to 1.
6. [FEATURE CHANGE] Modify wireless channel ID mapping table with Country code setting.
7. [ENHANCEMENT] Put Cerberian company's logo on External Content Filtering blocked page.
8. [ENHANCEMENT] Implement the timeout mechanism on content filter's local cache. Once the cache entry is timeout, it will be delete.
9. [BUG FIX] Symptom: NAT loopback fail.

Condition:

- (1) Host A runs FTP server in ZyWALL's LAN side.
  - (2) Turn on SUA and NAT loopback on ZyWALL.
  - (3) Configure default server to host A.
  - (4) Turn on Firewall.
  - (5) Host A runs FTP client and connect to ZyWALL's WAN IP.
  - (6) Connection fails.
10. [BUG FIX] Symptom: Router will crash.  
Condition: When user continuously accesses eWC and press "Apply" button, sometimes router will crash.
11. [BUG FIX] Symptom: Fixed a wording error "CERTIRICATES - MY CERTIFICATE

- DETAILS" in eWC>CERTIFICATES>MY CERTIFICATE>DETAILS.

Condition:

(1) Go to eWC>CERTIFICATES>MY CERTIFICATE and check detail (a check box).

(2) The word "CERTIRICATES" on page title is misspelled.

12. [BUG FIX] Symptom: Router will crash when entering SMT menu 3.5

Condition:

(1) Insert WLAN card.

(2) In CI command, enter "wlan active 11" instead of "wlan active 1" to activate WLAN on router.

(3) Enter SMT 3.5, router will crash.

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

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

Responder:

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

Rule 2: Correct static rule.

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

When trigger tunnel from initiator, negotiation will fail.

14. [BUG FIX] Symptom: IPSec rule swap will be failed with X-Auth.

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

Initiator: X-AUTH is off.

Responder: Rule 1 ==>phase 2 peer ID is wrong. X-AUTH is on.

Rule 2 ==>dynamic rule. X-AUTH is off and all other parameters are correct.

Responder will use rule 1 to start negotiate, and then since rule 1's phase 2 peer ID is wrong, responder will jump to rule 2. During the rule swap, system will compare rule 1's parameter with rule 2's. Since rule 2 is X-AUTH on and rule 1 is X-AUTH off, their authentication method flags are different. So system will skip rule 2 and got no rule to keep negotiate.

15. [BUG FIX] Symptom: Responder will jump to wrong VPN rule when current rule's phase 2 parameter is wrong.

Condition: Initiator -----NAT router ----- Responder

(1) Initiator has one VPN rule in which NAT traversal is on.

(2) In responder, there are two VPN rules.

- Rule 1: NAT traversal is on, and phase 2 parameters are wrong.

- Rule 2: NAT traversal is off, and all other parameters are correct.

(3) Trigger tunnel from initiator, and responder will use rule 1 to negotiate.

(4) When phase 2 negotiation starts, responder found rule 1's parameters are wrong, and will jump to rule 2.

(5) Negotiation will keep going and tunnel will be up.

16. [BUG FIX] Symptom: When initiator receives wrong phase 1 ID from responder, it will jump to another rule.

Condition: During IKE negotiation in Main mode, if responder's "Local ID Content"

mismatches initiator's "Peer ID Content", initiator will do rule swap and choose another rule to negotiate.

17. [BUG FIX] Symptom: IPSec rule swap is fail with NAT traversal.  
Condition: Initiator -----NAT Router -----Responder
  - (1) Initiator has one rule with NAT Traversal on.
  - (2) Responder has two rules:
    - Rule 1: NAT Traversal is on, and phase 2 ID is wrong.
    - Rule 2: NAT Traversal is off, and phase 2 ID is correct.
    - All other parameters in rule 1 and rule 2 are correct.
  - (3) Dial tunnel from initiator. Responder will use rule 1 to start negotiate.
  - (4) In phase 2, since phase 2 ID is wrong, responder will swap to rule 2 and eventually tunnel will be up because system won't check NAT Traversal flag when swapping the rule.
18. [BUG FIX] Symptom: Sometimes when connect to router by TCP, FTP or HTTP will fail.  
Condition:
  - (1) One user connects to router by FTP, TELNET or HTTP.
  - (2) In TCP handshake, client doesn't receive SYN ACK. i.e., router is in SYN RECEIVE state.
  - (3) Client timeout and send RESET to router.
  - (4) Related socket in router is still alive and other users can't login router until this socket timeout.
19. [ENHANCEMENT] The ZyWALL now also records the time server address (domain name or IP address) in the time synchronization result (successful or failed) logs.
20. [BUG FIX] Symptom: Router cannot access Internet.  
Condition:
  - (1) Restore default ROM file.
  - (2) In SMT4 menu, change Network Address Translation from SUA to Full Feature.
  - (3) Router cannot access Internet anymore and user does not know what happened.
21. [BUG FIX] Symptom: In Backup Line, ZyWALL might not show the actual route assessment.  
Condition:
  - (1) In Backup Line mode.
  - (2) Set WAN 1 route assessment on check point mode.
  - (3) If disconnect the connection to check point, the icmp check cannot report the correct status of the connection.
22. [BUG FIX] Symptom: System out of memory and reboot when firewall enable.  
Condition:
  - (1) Enable firewall, then generate traffic.
  - (2) The memory will slowly leak until it uses up all the memory, then reboot.
23. [FEATURE CHANGE] Add more information about content filter's error events in centralized log and block message. When the packet was blocked because of error happens.
24. [FEATURE CHANGE] Give different returned error message between timeout and invalid license in "eWC->CONTENT FILTER->Categories->"Test Again Internet Server"

25. [BUG FIX] Symptom: Router will crash.  
Condition:  
(1) In "eWC->CONTENT FILTER->General", select "Enable Content Filter" and click "Apply"  
(2) In "eWC->CONTENT FILTER->Categories", select "Enable External Database Content Filtering" and at least one category in "Select Categories". Click "Apply" after selection.  
(3) Open web browser and access a web site which belongs the category you select in step 2.  
(4) In "eWC->CONTENT FILTER->Categories", un-select the category selected in step 2 and keep at least one category is selected. Click "Apply" after selection.  
(5) Repeat step 3 immediately after step 4.  
(6) Router will crash or hang.
26. [FEATURE CHANGE] Change external content filtering message on centralized log and blocked page for some error events.
27. [BUG FIX] Symptom: Vantage can't sync VPN tunnel status.  
Condition: On Vantage, when create a VPN tunnel and dial the tunnel success. Vantage hasn't display the VPN tunnel status.
28. [ENHANCEMENT] Supports Intel TE28F640 J3C120 and TE28F128 J3C150 Flash ROM when ZyWALL is programming flash and displaying flash type information by using "sys atsh".
29. [BUG FIX] Symptom: Fixed a wording error "Assymertical" in eWC>FIREWALL>Default Rule.
30. [BUG FIX] Symptom: Router will not enter "Debug Mode".  
Condition:  
(1) Go to SMT 24.7.1  
(2) Select "Y" for "upload system firmware".  
(3) After rebooting, it will not enter "Debug Mode".
31. [BUG FIX] Symptom: SA monitor shows messy code.  
Condition:  
(1) Create a workable VPN rule.  
(2) Set the encryption algorithm in Phase 2 with "NULL"  
(3) SA Monitor will show "ESP ???-MD5".
32. [ENHANCEMENT]  
Enhance concurrent VPN tunnels to 100 and 120 configurable VPN rules.

#### **Modifications in V 3.62(WM.3)b1 | 04/23/2004**

1. [BUG FIX] Symptom: ZyWALL cannot establish IPSec connection to SSH Sentinel.  
Condition: When ZyWALL and Sentinel both enable XAUTH, the IKE negotiattion will fail.
2. [ENHANCEMENT] Auto configures MSS size according to MTU size. If users set the MSS value to 0, system would auto configure the MSS size according MTU size. Otherwise, the mss value would be the user specified value. The default MSS size is 1400.
3. [BUG FIX] Symptom: PPPoE connection sometimes fails in France.

Condition: Since France Telecom changes their core network setup to BRAS, ZyWALL PPPoE connection on authentication phase most of the time fails.

#### **Modifications in V 3.62(WM.2) | 04/16/2004**

1. Modify for formal release.

#### **Modifications in V 3.62(WM.2)b2 | 04/14/2004**

1. [BUG FIX] Symptom: When delete LAN->Static DHCP MAC and IP via Vantage. The IP become "0.0.0.0" on Web. It should be empty.  
Condition:  
(1) On Vantage, Configuration->LAN->Static DHCP.  
(2) Add MAX and IP Address from index 1 to 5 and press Apply.  
(3) Clear MAC Address and fill up IP Address to "0.0.0.0" from index 4 to 5 on Vantage and press Apply.  
(4) Check MAC and IP on Web. MAC always exist, and IP Address become "0.0.0.0".
2. [BUG FIX] Symptom: When device changes the encapsulation will lose connect with Vantage server.  
Condition:  
(1) Original device go Ethernet.  
(2) Change WAN ISP to PPPoE on Web.  
(3) Vantage's device status display connected. But device IP is still Ethernet IP.  
(4) We can't control device via Vantage now.
3. [BUG FIX] Symptom: The device console display "size of spAclBuffer\_t=2048" message after restore.  
Condition:  
(1) On Vantage, DEVICE->Configuration File->Restore.  
(2) Select a rom file and perform rom file restore to device.  
(3) After the restore, device console will display "size of spAclBuffer\_t=2048".
4. [BUG FIX] Symptom: WAN->Dial Backup->"Port Speed" can't select to "230400".  
Condition:  
(1) On Vantage, CONFIGURATION->WAN->Dial.  
(2) On 'Dial Backup Port Speed', select 230400 and it cannot be configured to device.
5. [BUG FIX] Symptom: Vantage can't find this version F/W just uploaded.  
Condition:  
(1) On Vantage, DEVICE->Firmware Mgmt, upload the F/W.  
(2) DEVICE->Firmware Upgrade, we can't find the F/W just uploaded.

#### **Modifications in V 3.62(WM.2)b1 | 03/31/2004**

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

## **Modifications in V 3.62(WM.1) | 03/01/2004**

1. Formal release.

## **Modifications in V 3.62(WM.1)b1 | 02/23/2004**

1. [ENHANCEMENT] Add new CI command "ip arp period" to change the ARP lifetime interval.
2. [ENHANCEMENT] Add a new CI command "ip arp force <on|off>". When the user uses "ip arp force on", the age function of APR function will be disabled. That means even the ARP entry has been referred, the timer of it will not reset to 300 seconds, it will be still time out.
3. [BUG FIX] Symptom: System memory leak and eventually causing the reboot.  
Condition:
  - (1) Start collecting data in eWC->LOGS->Reports or using CI command "ip rpt start".
  - (2) Run for some time.
  - (3) System will run out of memory and become very unstable.
4. [BUG FIX] Symptom: Edit/Delete bandwidth management rule, sometimes system will crash.  
Condition:
  - (1) Set up a Bandwidth management rule.
  - (2) By using this rule, do FTP.
  - (3) During FTP, change related eWC->BW MGNT->Class Setup->Edit Class->Priority.
  - (4) System crashes.
5. [BUG FIX] Symptom: Packets will not go through ZyWALL.  
Condition:
  - (1) There is heavy traffic through router.
  - (2) Sometimes PC A send a DNS query to outside DNS server, but the reply packet will be forwarded to another PC.
6. [BUG FIX] Symptom: Packet can't be transmitted under Half Duplex mode.  
Condition:
  - (1) Connect ZyWALL LAN (or WAN) port to a 10M Hub so that the port will operate in 10M/Half-Duplex mode.
  - (2) Generate a lot of traffic over the 10M Hub.
  - (3) Have the ZyWALL LAN (or WAN) port continuously transmit a lot of packets.
  - (4) After some time, ZyWALL's LAN (or WAN) port may not transmit packets forever.
7. [BUG FIX] Symptom: IPSec XAUTH cannot work with SoftRemote.  
Condition:
  - (1) Configure corresponding IPSec rule with XAUTH on SoftRemote and ZyWALL.
  - (2) Trigger SoftRemote IPSec rule.
  - (3) SoftRemote log shows "no proposal chosen" and connection fails.
8. [BUG FIX] Symptom: IPsec NAT-Traversal can not work.  
Condition:



- (1) Setup NAT-Traversal rule at Initiator and Responder, both sides are Tunnel encapsulation mode.
  - (2) Connect from Initiator side.
  - (3) Tunnel can not be established.
9. [BUG FIX] Symptom: ICMP packet of NAT loopback will be blocked by Firewall.  
Condition:
- (1) Enable Firewall.
  - (2) NAT default server is set to host A.
  - (3) Turn on NAT loopback.
  - (4) Host A pings router's WAN IP address.
  - (5) Host A does not receive echo reply packet and Firewall log shows "Land Attack".

#### **Modifications in V 3.62(WM.0)b11 | 12/18/2003**

1. [FEATURE CHANGE] eWC/Bandwidth Managemet/Class Setup, remote the Services field from the Filter Configuration.

#### **Modifications in V 3.62(WM.0)b10 | 12/13/2003**

1. [BUG FIX] When the DNS query is in progress and the system's WAN interface is changed between different interfaces(WAN 1, WAN 2, traffic redirect and dial backup), the system will crash.
2. [ENHANCEMENT] A new warning message "Warning! No NAT rule configured in system", would appear if the system be setup to NAT full feature but the used doesn't configure any NAT rule.
3. [FEATURE CHANGE] The default time server has been changed to "a.ntp.alphazed.net".
4. [BUG FIX] eWC/Home/Internet Access, if the user select PPTP encapsulation, this page can't display the correct "My IP Subnet Mask".

#### **Modifications in V 3.62(WM.0)b9 | 12/10/2003**

1. [BUG FIX] Symptom: FTP transformation crash the system.  
Condition: (1) Enable the bandwidth management on LAN.  
(2) Setup the FTP service on the Class configuration & filter.  
(3) Use "passive mode" to do FTP transformation.  
(4) System crash.
2. [BUG FIX] ACT LED doesn't light on when the dial backup is active.
3. [BUG FIX] Symptom: XAUTH fail but tunnel can be established.  
Condition: (1) Both two routers are set to XAUTH Server mode, and tunnel is established successfully.  
XAUTH fail but continue phase 2 negotiate and create tunnel finally.  
(2) One router is set to Client mode and the other is Server mode, but the passwords are mismatch.

XAUTH fail but continue phase 2 negotiate and create tunnel finally.

4. [ENHANCEMENT] The one-line certification request PEM data is broken into 64-byte-wide lines so that OpenSSL certificate enrollment can accept it without problems.
5. [BUG FIX] On eWC/Internet Access Wizard, can't save the static IP address, if the encapsulation type of the WAN is PPPoE or PPTP.
6. [BUG FIX] The dial backup password will be destroyed if the user save this page without re-keying the correct password again.

#### **Modifications in V 3.62(WM.0)b8 | 12/04/2003**

1. [BUG FIX] The DHCP client lease renewal process always fail, causes the DHCP client IP address to expire.
2. [BUG FIX] Symptom: IPsec rule swapping can not work if we setup X-Auth.  
Condition: The ZyWALL device, an IPsec responder, we have setup two IPsec rules by using same phase 1 parameters, but we only enable X-Auth on the second rule. The ZW can't use the second rule to respond to the initiator if the initiator enables the X-Auth.
3. [BUG FIX] Symptom: The router will add an unnecessary route entry in PPPoE type.  
Condition:
  1. Configure the WAN Encapsulation type as Ethernet, Static P in SMT4, or SMT11\_1.
  2. Change the WAN Encapsulation type as PPPoE, dynamic IP.
  3. Reboot the router
  4. Use the CI command "ip route status" to display all routing entries.

There is an unnecessary routing entry.

4. [BUG FIX] IPsec re-key process fails if the IPsec rule is dynamic rule.
5. [BUG FIX] Can't create 70 IPsec tunnels if we have PSK and PKI rules at the same time.
6. [BUG FIX] ZW70 doesn't display DHCP table.
7. [BUG FIX] ZW70 doesn't display SA status from eWC/Home
8. [BUG FIX] Has been setup the WAN check point, ZW70 would not drop PPPoE connection, even the check period is large than WAN idle time out.
9. [BUG FIX] eWC/Home page, doesn't give the correct status information when the WAN encapsulation is PPPoE/PPTP.
10. [ENHANCEMENT] eWC pages, changed the 4-fields IP address to one field IP address.
11. [BUG FIX] In bandwidth management, the function "maximize bandwidth usage" doesn't work.
12. [BUG FIX] The service (only FTP, at this time) in the bandwidth management only works on the firewall feature enabled condition.
13. [BUG FIX] Some internal 802.1X debug messages show on console screen.

**Modifications in V 3.62(WM.0)b7 | 11/05/2003**

1. [BUG FIX] Symptom: Can't transmit packets to the remote network by way of the IPSec tunnel. Condition: ZW can create the IPSec tunnel to the remote secure gateway, but data packets can be transmitted to the remote network.
2. [ENHANCEMENT] On SMT 6.1, supports check points for WAN 1 and WAN2, when the Encapsulation is PPPoE/PPTP.
3. [ENHANCEMENT] Change the background color of eWC.
4. [BUG FIX] Menu 11.3 is not correct, a weird character appears.
5. [BUG FIX] WAN 2 can't do PPPoE/PPTP dial, if WAN 2 is setup by eWC/WAN/WAN 2 page.

**Modifications in V 3.62(WM.0)b6 | 11/31/2003**

6. [FEATURE CHANGE] The new session management feature has been removed on this version.

**Modifications in V 3.62(WM.0)b5 | 10/29/2003**

7. [BUG FIX] Modified NAT part for test NAT table full problem.
8. [ENHANCEMENT] eWC/VPN/VPN Rules page, dynamically display VPN rules. That is, only show those VPN rules which have been configured. Those displayed entries are sorted by rule name.
9. [ENHANCEMENT] eWC, Use edit and delete icons to edit/delete IPSec Rules, Firewall ACL Rules and Certificates.
10. [ENHANCEMENT] eWC/CONTENT FILTER/Categories, two new category setup, "Unrated Web Sites" and "When Content Filter Server Is Unavailable". Users can setup to block/unblock and log/no-log those kind of web access.
11. [BUG FIX] In a short time, totally 70 IPSec tunnels has been created, the system crashed.
12. [FEATURE CHANGE] Support a new session management feature. Please see Note 10.

**Modifications in V 3.62(WM.0)b4 | 10/17/2003**

1. [FEATURE CHANGE] Supports Embedded HTTPS proxy server. Please see **Appendix 6**.
2. [ENHANCEMENT] Provides PKI for SSH Server Host Key.
3. [BUG FIX] Symptom: "MG-SOFT MIB Browser" cannot contact router's snmp server via LAN side after changing the router's LAN IP address.  
Condition: 1. Using "MG-SOFT MIB Browser" to contact the router's snmp server via LAN side. 2. Enter eWC/REMOTE MGNT/SNMP 3. In "Service Access", select "Disable" and tick "Apply" button. 4. In "Service Access", select "LAN&WAN&DMZ" and tick "Apply" button. 5. Change the router's LAN IP address. 6. Change PC's IP address to fit

the router's new address setting. 7. Using "MG-SOFT MIB Browser" to contact the router's snmp server again. 8. The contacting will fail in step 7.

#### **Modifications in V 3.62(WM.0)b3 |**

4. [BUG FIX] Symptom: System crashes when enabling bandwidth management and syslog.  
Condition: When enabling syslog and setting one bandwidth management rule for this syslog traffic, the system crashes while user wants to login this system.
5. [BUG FIX] The system generates some incorrect logs for Cerberian content filtering.
  1. Enter eWC/CONTENT FILTER/Categories
  2. Select the checkbox of "Log Matched Web Sites " and unselect the checkbox of "Block Matched Web Sites ".
  3. Select some restricted categories.
  4. Access some web sites that belong to those restricted categories.
  5. The system would not block web contents, but have "Web Block" centralized logs.
6. [BUG FIX] Symptom: Content filter block the trusted domain's web content.
  1. Enter eWC/content filter/Customize.
  2. Select the checkbox of "Enable Filter List Customization " and "Disable all web traffic except for Trusted Domains ".
  3. Unselect the checkbox of "Don't block Java/ActiveX/Cookies/Web Proxy to Trusted Domain sites".
  4. Set a trusted domain set and access this web site.
  5. The web content will be blocked.
7. [FEATURE CHANGE] Support a mechanism to re-register the Content filter. It is useful that you had registered the Content filter and reset your system to the factory defaults, the system would lost the register key. Now you can register the Content filter again.
8. [FEATURE CHANGE] Support the second WAN interface. The second WAN, or WAN 2 is "Backup Line". Please see Note 2 and Known Issues 10, 11.
9. [FEATURE CHANGE] eWC, on-line help pages.
10. [BUG FIX] Symptom:SMT, NAT Traversal is always enabled.
  1. Enable NAT Traversal and phase 2 Use ESP protocol, then save to rom.
  2. Change this rule from ESP to AH and disable NAT Traversal, then save to rom, but actually the NAT Traversal always enable.
11. [BUG FIX] "Home->VPN Wizard" can not create the correct VPN rule.
12. [BUG FIX] eWC/Home, The button [VPN Station] be changed to [VPN status].
13. [BUG FIX] eWC/VPN Wizard, can't save the Remote (Peer) Gateway's IP address to the IPSec policy.
14. [BUG FIX] When the system brings up, it show a wired message "iface enif0 is NAT off" on the console.

15. [BUG FIX] Using SMT menu 24.6 restore rom file can cause device to crash.
16. [BUG FIX] Menu 24.5, can not enter Ctrl-x to terminate operation, the system hang.
17. [ENHANCEMENT] eWC/"Internet Access" Wizard, added password confirm field on the first page if the encapsulation is PPPoE/PPTP.
18. [BUG FIX] Can't show the correct NAT session information on eWC/Home page.
19. [BUG FIX] Even the system doesn't trust the Cert., it still can build the IPSec tunnel.
20. [ENHANCEMENT] eWC/LOGS/Log Settings page, we changed some words.

### **Modifications in V 3.62(WM.0)b2 |**

1. [BUG FIX] Symptom & Condition: Sometimes there will be a log "Un-consistent SA happens!!" showed on log page.
2. [BUG FIX] Some incorrect IPSec IKE logs
  - When enable XAUTH in IKE, we have two "Start Phase 2: Quick Mode" logs in the initiator and two "Phase 1 IKE SA process done" logs in the responder.
  - When the initiator and the responder choose different negotiation mode, the system displays "Rule [%d] phase1 negotiation mode mismatch." The system should give the correct rule number.
  - Sometimes we will get error message "Cannot resolve secure gateway for rule 1", even the address of the secure gateway is a real IP address.
  - Change the color of the log "'Start Phase 2:Quick Mode'" from red to block.
  - On the SMT, the system shows the incorrect message "Min Value of Life time is 180 seconds" if the pre-shared key field is empty.
3. [BUG FIX] Symptom : The SMT shows incorrect information when displaying an IKE rule.  
 Condition : When choosing AH as phase 2 active protocol, the phase 1 authentication algorithm will be changed to "N/A". It should change phase 2 Encryption as "N/A"
4. [BUG FIX] Symptom: Firewall can't detect port scan attack.  
 Condition: When port scan tools scan router's WAN port, the firewall have no attack logs about the portscan. The port scan attack has been blocked by WAN to WAN/ZyWALL default policy.
5. [FEATURE CHANGE] Before: All ICMP packets information will log in "ICMP" catalog even the packet is blocked/forwarded by firewall.  
 Now: When ICMP packet is blocked/forwarded by firewall, the log messages will be "ACCESS CONTROL" catalog.
6. [FEATURE CHANGE] Change the alignment order to be WAN1, WAN2, LAN, WLAN, DMZ in the smt24.1 of the ZW70
7. [BUG FIX] eWC/Access Policy page, if there is no any firirwall rule, eWC displays an empty row on the summary table.
8. [BUG FIX] eWC/Cert. pages, if import a file which with the file size large than 20K bytes, we got an error message(sfswriteFile #) on the console.
9. [BUG FIX] eWC/Content Filter, General page: no error message when the user give invalid address range.
10. [BUG FIX] eWC/Content Filter/General Page, we only add address range, hasn't yet

clicked “apply”, but eWC saved it.

11. [BUG FIX] eWC/Content Filter/General Page, eWC returns the error message “Write to Flash error”, if the user gives the incorrect IP range.
12. [BUG FIX] IPsec VPN, can’t work with ZW10W, 3.61 version.
13. [BUG FIX] Although the device can get IP address by using PPPoE / PPTP, eWC/ Home page’s WAN IP information is still empty / wrong.
14. [BUG FIX] eWC/Home/VPN Wizard page, the warning page shows Error :”Min. value of Life Time is 1 minute”
15. [BUG FIX] On the WAN page, while setting an unreachable ip address as spoof wan mac address ( not submit )then change encapsulation between Ethernet, PPPoE, and PPTP, the status shows “Can not get the WAN MAC Address”.
16. [BUG FIX] eWC, after editing “VPN->Advance”, the pre-shared key disappear.
17. [BUG FIX] eWC/LAN page, the user can save three DNS Relay.
18. [BUG FIX] eWC/AUTH SERVER/RADIUS page, if keep the key blank and apply, the status shows : ERROR: Fail to update due to internal error (-6611 or -6613).
19. [BUG FIX] Bandwidth management->Class->”Borrow bandwidth from parent class” function can not work appropriately while the schedule is “Fairness-Based”

#### **Modifications in V 3.62(WM.0)b1 | 08/27/2003**

1. First release.

## 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	
SSH Server:	Port = 22	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.

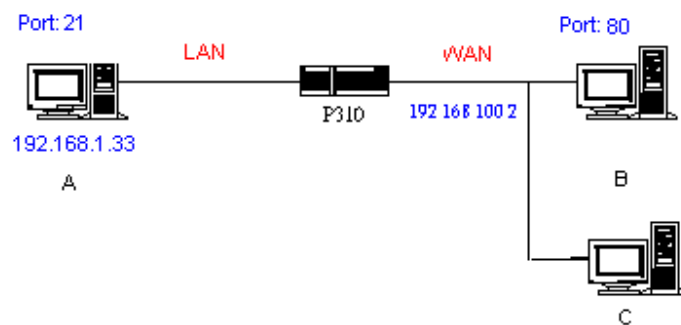
These triggered events can be timed so that they erase the port mapping as soon as they are done with the data transfer, so that the port mapping can be triggered by another Client computer. This gives the *illusion* that multiple computers can use the same port mapping at the same time, but the computers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

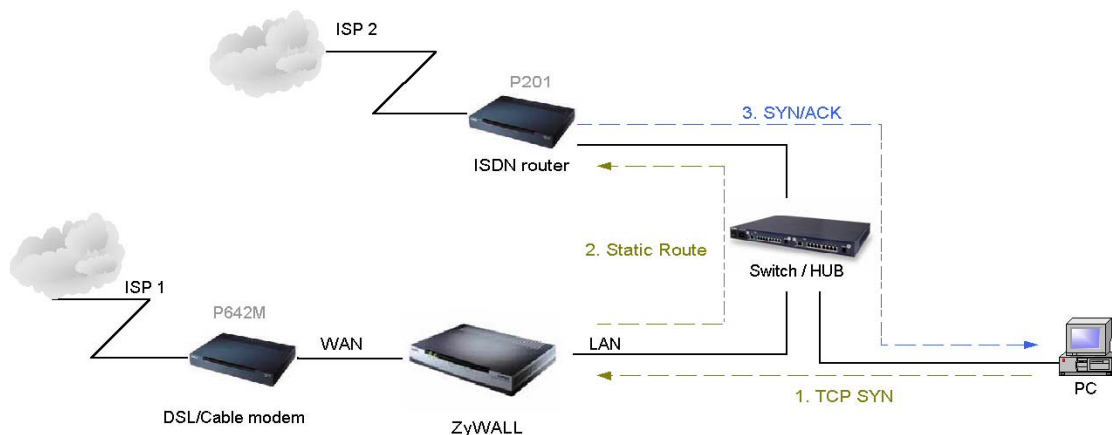


Figure 5-1 Triangle Route

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

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

That causes all of outgoing TCP traffics being reset!

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

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

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

normal function.

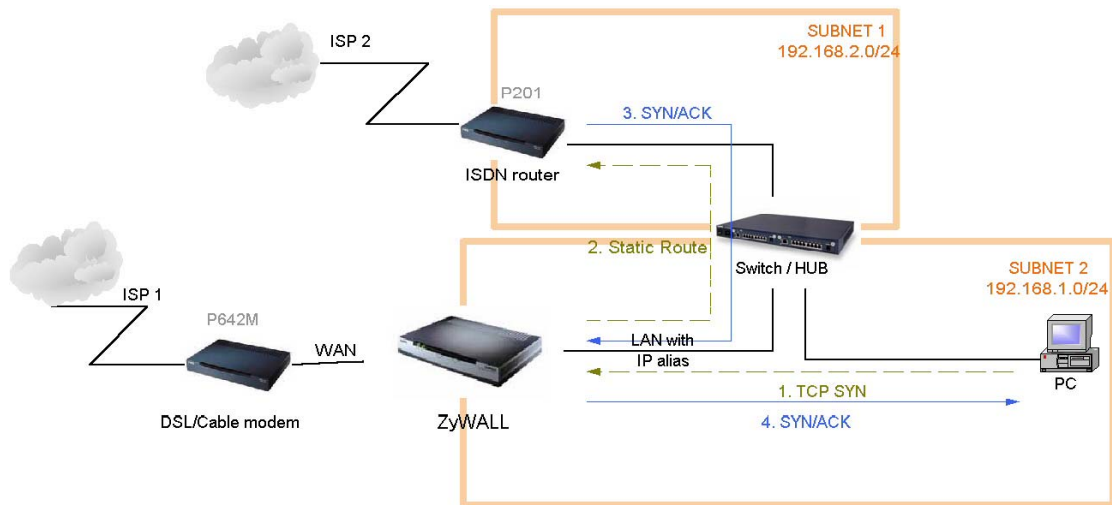


Figure 5-2 Gateway on alias IP network

## (2) Gateway on WAN side

A working topology is suggested as below.

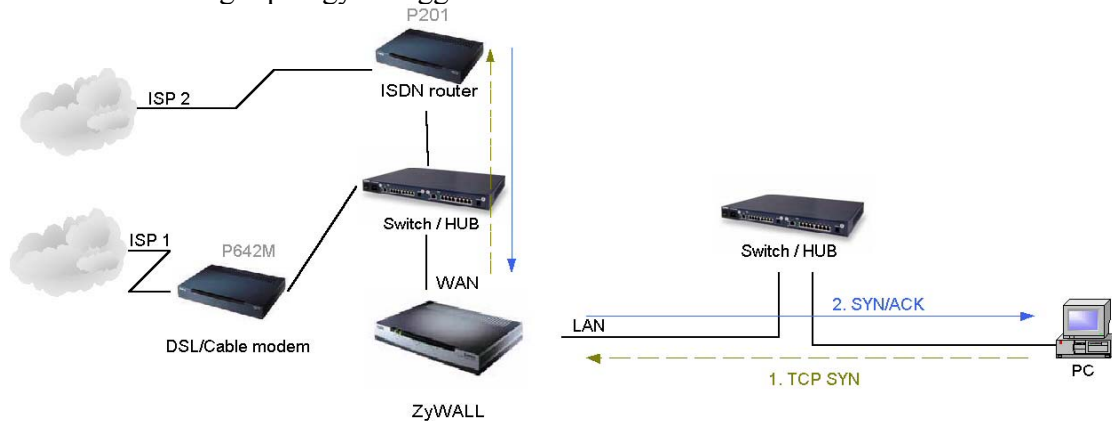


Figure 5-3 Gateway on WAN side

## Appendix 5 IPSec FQDN support

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

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

In FQDN design, all three types, IP, DNS, E-Mail, can set ID content. For ID type is

DNS or E-mail, the behavior is simple. ZyWALL A and ZyWALL B only checks the ID contents are consistent and they can connect.

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

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

We can put all combinations in to these two tables:

(Local ID Type is IP):

Configuration		**Run-time status	
My IP Addr	Local ID Content	My IP Addr	Local ID Content
0.0.0.0	*blank	My WAN IP	My WAN IP
0.0.0.0	a.b.c.d (it can be 0.0.0.0)	My WAN IP	a.b.c.d ( 0.0.0.0, if user specified it)
a.b.c.d (not 0.0.0.0)	*blank	a.b.c.d	a.b.c.d
a.b.c.d (not 0.0.0.0)	e.f.g.h (or 0.0.0.0)	a.b.c.d	e.f.g.h (or 0.0.0.0)

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

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

(Peer ID Type is IP):

Configuration		*Run-time check
Secure Gateway Addr	Peer ID Content	
0.0.0.0	blank	Just check ID types of incoming packet and machine's peer ID type. If the peer's ID is IP, then we accept it.
0.0.0.0	a.b.c.d	System checks both type and content
a.b.c.d	blank	1. System will check the ID type and the content. 2. The contents will match only if the ID content of coming packet is a.b.c.d because system will put Secure Gateway Address as Peer ID content.
a.b.c.d	e.f.g.h	1. System will check the ID type and the content. 2. The contents will match only if the ID content of coming packet is e.f.g.h.

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

**Summary:**

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

**Appendix 6 Embedded HTTPS proxy server**

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

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

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

## Annex A CI Command List

Last Updated: 2002/11/26

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

### System Related Command

[Home](#)

Command				Description
sys				
	adjtime			retrive date and time from Internet
	callhist			
		display		display call history
		remove	<index>	remove entry from call history
	countrycode		[countrycode]	set country code
	date		[year month date]	set/display date
	domainname			display domain name
	edit		<filename>	edit a text file
	extraphnum			maintain extra phone numbers for outcalls
		add	<set 1-3> <1 <sup>st</sup> phone num> [2 <sup>nd</sup> phone num]	add extra phone numbers
		display		display extra phone numbers
		node	<num>	set all extend phone number to remote node <num>
		remove	<set 1-3>	remove extra phone numbers
		reset		reset flag and mask
	feature			display feature bit
	hostname		[hostname]	display system hostname
	logs			
		category		
			access [0:none/1:log/2:alert/3:both]	record the access control logs
			attack [0:none/1:log/2:alert/3:both]	record and alert the firewall attack logs
			display	display the category setting
			error [0:none/1:log/2:alert/3:both]	record and alert the system error logs
			ipsec [0:none/1:log/2:alert/3:both]	record the access control logs
			ike [0:none/1:log/2:alert/3:both]	record the access control logs
			javablocked [0:none/1:log]	record the java etc. blocked logs
			mten [0:none/1:log]	record the system maintenance logs
			upnp [0:none/1:log]	record upnp logs
			urlblocked [0:none/1:log/2:alert/3:both]	record and alert the web blocked logs
			urlforward [0:none/1:log]	record web forward logs
		clear		clear log
		display	[access attack error ipsec ike javablocked mten urlblocked urlforward]	display all logs or specify category logs
		errlog		
			clear	display log error
			disp	clear log error
			online	turn on/off error log online display

		load		load the log setting buffer
		mail		
			alertAddr [mail address]	send alerts to this mail address
			display	display mail setting
			logAddr [mail address]	send logs to this mail address
			schedule display	display mail schedule
			schedule hour [0-23]	hour time to send the logs
			schedule minute [0-59]	minute time to send the logs
			schedule policy [0:full/1:hourly/2:daily/3:weekly/4:none]	mail schedule policy
			schedule week [0:sun/1:mon/2:tue/3:wed/4:thu/5:fri/6:sat]	weekly time to send the logs
			server [domainName/IP]	mail server to send the logs
			subject [mail subject]	mail subject
		save		save the log setting buffer
		syslog		
			active [0:no/1:yes]	active to enable unix syslog
			display	display syslog setting
			facility [Local ID(1-7)]	log the messages to different files
			server [domainName/IP]	syslog server to send the logs
	log			
		clear		clear log error
		disp		display log error
		online	[on/off]	turn on/off error log online display
		resolve		Resolve mail server and syslog server address
	mbuf			
		link	link	list system mbuf link
		pool	<id> [type]	list system mbuf pool
		status		display system mbuf status
		disp	<address>	display mbuf status
		cnt		
			disp	display system mbuf count
			clear	clear system mbuf count
		debug	[on/off]	
	pwderrtm		[minute]	Set or display the password error blocking timeout value.
	rn			
		load	<entry no.>	load remote node information
		disp	<entry no.>(0:working buffer)	display remote node information
		nat	<none sua full_feature>	config remote node nat
		nailup	<no yes>	config remote node nailup
		mtu	<value>	set remote node mtu
		save	[entry no.]	save remote node information
	smt			not support in this product
	stdio		[minute]	change terminal timeout value
	time		[hour [min [sec]]]	display/set system time
	trcdisp			monitor packets
	trclog			
	trcpacket			
	syslog			
		server	[destIP]	set syslog server IP address
		facility	<FacilityNo>	set syslog facility



		type	[type]	set/display syslog type flag
		mode	[on/off]	set syslog mode
	version			display RAS code and driver version
	view		<filename>	view a text file
	wdog			
		switch	[on/off]	set on/off wdog
		cnt	[value]	display watchdog counts value: 0-34463
	romreset			restore default romfile
	server			
		access	<telnet ftp web icmp snmp dns> <value>	set server access type
		load		load server information
		disp		display server information
		port	<telnet ftp web snmp> <port>	set server port
		save		save server information
		secureip	<telnet ftp web icmp snmp dns> <ip>	set server secure ip addr
	fwnotify			
		load		load fwnotify entry from spt
		save		save fwnotify entry to spt
		url	<url>	set fwnotify url
		days	<days>	set fwnotify days
		active	<flag>	turn on/off fwnotify flag
		disp		display firmware notify information
		check		check firmware notify event
		debug	<flag>	turn on/off firmware notify debug flag
	cmgr			
		trace		
			disp <ch-name>	show the connection trace of this channel
			clear <ch-name>	clear the connection trace of this channel
		cnt	<ch-name>	show channel connection related counter
	socket			display system socket information
	filter			
		netbios		
	roadrunner			
		debug	<level>	enable/disable roadrunner service 0: diable <default> 1: enable
		display	<iface name>	display roadrunner information iface-name: enif0, wanif0
		restart	<iface name>	restart roadrunner
	ddns			
		debug	<level>	enable/disable ddns service
		display	<iface name>	display ddns information
		restart	<iface name>	restart ddns
		logout	<iface name>	logout ddns
	cpu			
		display		display CPU utilization
	filter			
		netbios		
	upnp			
		active	[0:no/1:yes]	Activate or deactivate the saved upnp settings
		config	[0:deny/1:permit]	Allow users to make configuration changes. through UPnP
		display		display upnp information
		firewall	[0:deny/1:pass]	Allow UPnP to pass through Firewall.

		load		save upnp information
		save		save upnp information

#### Exit Command

[Home](#)

Command				Description
exit				exit smt menu

#### Device Related Command

[Home](#)

Command				Description
dev				
	channel			
		drop	<channel name>	drop channel
	dial		<node#>	dial to remote node

#### Ethernet Related Command

[Home](#)

Command				Description
ether				
	config			display LAN configuration information
	driver			
		cnt		
			disp <name>	display ether driver counters
		ioctl	<ch_name>	Useless in this stage.
		status	<ch_name>	see LAN status
	version			see ethernet device type
	pkttest			
		disp		
			packet <level>	set ether test packet display level
			event <ch> [on/off]	turn on/off ether test event display
		sap	[ch_name]	send sap packet
		arp	<ch_name> <ip-addr>	send arp packet to ip-addr
	debug			
		disp	<ch_name>	display ethernet debug infomation
		level	<ch_name> <level>	set the ethernet debug level level 0: disable debug log level 1:enable debug log (default)
	edit			
		load	<ether no.>	load ether data from spt
		mtu	<value>	set ether data mtu
		accessblock	<0:disable 1:enable>	block internet access
		save		save ether data to spt

#### POE Related Command

[Home](#)

Command				Description
poe				
	status		[ch_name]	see poe status
	dial		<node>	dial a remote node
	drop		<node>	drop a pppoe call
	ether		[rfc3com]	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		
		server	<primary> [secondary] [third]	set dns server
		stats		
			clear	clear dns statistics
			disp	display dns statistics
	httpd			
	icmp			
		status		display icmp statistic counter
		discovery	<iface> [on off]	set icmp router discovery flag
	ifconfig		[iface] [ipaddr] [broadcast <addr>  mtu <value> dynamic]	configure network interface
	ping		<hostid>	ping remote host
	route			
		status	[if]	display routing table
		add	<dest_addr default>[/<bits>] <gateway> [<metric>]	add route
		addiface	<dest_addr default>[/<bits>] <gateway> [<metric>]	add an entry to the routing table to iface
		addprivate	<dest_addr default>[/<bits>] <gateway> [<metric>]	add private route
		drop	<host addr> [/<bits>]	drop a route

	smtp			
	status			display ip statistic counters
	stroute			
		display	[rule #   buf]	display rule index or detail message in rule.
		load	<rule #>	load static route rule in buffer
		save		save rule from buffer to spt.
		config		
			name <site name>	set name for static route.
			destination <dest addr>[/<bits>] <gateway> [<metric>]	set static route destination address and gateway.
			mask <IP subnet mask>	set static route subnet mask.
			gateway <IP address>	set static route gateway address.
			metric <metric #>	set static route metric number.
			private <yes/no>	set private mode.
			active <yes/no>	set static route rule enable or disable.
	traceroute		<host> [ttl] [wait] [queries]	send probes to trace route of a remote host
	xparent			
		join	<iface1> [<iface2>]	join iface2 to iface1 group
		break	<iface>	break iface to leave ipxparent group
	ave			anti-virus enforce
	urlfilter			
		reginfo		
			display	display urlfilter registration information
			name	set urlfilter registration name
			eMail <size>	set urlfilter registration email addr
			country <size>	set urlfilter registration country
			clearAll	clear urlfilter register information
		category		
			display	display urlfilter category
			webFeature [block/nonblock] [activex/java/cookei/webproxy]	block or unblock webfeature
			logAndBlock [log/logAndBlock]	set log only or log and block
			blockCategory [block/nonblock] [all/type(1-14)]	block or unblock type
			timeOfDay [always/hh:mm] [hh:mm]	set block time
			clearAll	clear all category information
		listUpdate		
			display	display listupdate status
			actionFlags [yes/no]	set listupdate or not
			scheduleFlag [pending]	set schedule flag
			dayFlag [pending]	set day flag
			time [pending]	set time
			clearAll	clear all listupdate information
		exemptZone		
			display	display exemptzone information
			actionFlags [type(1-3)][enable/disable]	set action flags
			add [ip1] [ip2]	add exempt range
			delete [ip1] [ip2]	delete exempt range
			clearAll	clear exemptzone information
		customize		
			display	display customize action flags
			actionFlags [act(1-6)][enable/disable]	set action flags

			logFlags [type(1-3)][enable/disable]	set log flags
			add [string] [trust/untrust/keyword]	add url string
			delete [string] [trust/untrust/keyword]	delete url string
			clearAll	clear all information
		logDisplay		display cyber log
		ftplist		update cyber list data
		listServerIP	<ipaddr>	set list server ip
		listServerName	<name>	set list server name
	tredir			
		failcount	<count>	set tredir failcount
		partner	<ipaddr>	set tredir partner
		target	<ipaddr>	set tredir target
		timeout	<timeout>	set tredir timeout
		checktime	<period>	set tredir checktime
		active	<on/off>	set tredir active
		save		save tredir information
		disp		display tredir information
		debug	<value>	set tredir debug value
	nat			
		server		
			disp	display nat server table
			load <set id>	load nat server information from ROM
			save	save nat server information to ROM
			clear <set id>	clear nat server information
			edit active <yes/no>	set nat server edit active flag
			edit svrport <start port> [end port]	set nat server server port
			edit intport <start port> [end port]	set nat server forward port
			edit remotehost <start ip> [end ip]	set nat server remote host ip
			edit leasetime [time]	set nat server lease time
			edit rulename [name]	set nat server rule name
			edit forwardip [ip]	set nat server server ip
			edit protocol [protocol id]	set nat server protocol
			edit clear	clear one rule in the set
		service		
			irc [on/off]	turn on/off irc flag
		resetport		reset all nat server table entries
		incikeport	[on/off]	turn on/off increase ike port flag
	igmp			
		debug	[level]	set igmp debug level
		forwardall	[on/off]	turn on/off igmp forward to all interfaces flag
		querier	[on/off]	turn on/off igmp stop query flag
		iface		
			<iface> grouptm <timeout>	set igmp group timeout
			<iface> interval <interval>	set igmp query interval
			<iface> join <group>	join a group on iface
			<iface> leave <group>	leave a group on iface
			<iface> query	send query on iface
			<iface> rsptime [time]	set igmp response time
			<iface> start	turn on of igmp on iface
			<iface> stop	turn off of igmp on iface
			<iface> ttl <threshold>	set ttl threshold
			<iface> v1compat [on/off]	turn on/off v1compat on iface
		robustness	<num>	set igmp robustness variable
		status		dump igmp status

	pr			
--	----	--	--	--

# IPSec Related Command

[Home](#)

Command				Description
ipsec				
	debug	<1 0>		turn on off trace for IPsec debug information
	ipsec log disp			show IPSec log, same as menu 27.3
	route	lan	<on off>	After a packet is IPSec processed and will be sent to LAN side, this switch is to control if this packet can be applied IPSec again. Remark: Command available since 3.50(WA.3)
		wan	<on off>	After a packet is IPSec processed and will be sent to WAN side, this switch is to control if this packet can be applied IPSec again. Remark: Command available since 3.50(WA.3)
	show_runtime	sa		display runtime phase 1 and phase 2 SA information
		spd		When a dynamic rule accepts a request and a tunnel is established, a runtime SPD is created according to peer local IP address. This command is to show these runtime SPD.
	switch	<on off>		As long as there exists one active IPSec rule, all packets will run into IPSec process to check SPD. This switch is to control if a packet should do this. If it is turned on, even there exists active IPSec rules, packets will not run IPSec process.
	timer	chk_my_ip	<1~3600>	- Adjust timer to check if WAN IP in menu is changed - Interval is in seconds - Default is 10 seconds - 0 is not a valid value
		chk_conn.	<0~255>	- Adjust auto-timer to check if any IPSec connection has no traffic for certain period. If yes, system will disconnect it. - Interval is in minutes - Default is 2 minuets - 0 means never timeout
		update_peer	<0~255>	- Adjust auto-timer to update IPSec rules which use domain name as the secure gateway IP. - Interval is in minutes - Default is 30 minutes - 0 means never update Remark: Command available since 3.50(WA.3)
	updatePeerIp			Force system to update IPSec rules which use domain name as the secure gateway IP right away. Remark: Command available since 3.50(WA.3)
	dial	<rule #>		Initiate IPSec rule <#> from ZyWALL box Remark: Command available since 3.50(WA.3)
	display	<rule #>		Display IPSec rule #
	remote	key	<string>	I add a secured remote access tunnel with pre-shared key. It is a dynamic rule with local: the route's WAN IP. The algorithms with it are fixed to phase1: DES+MD5, DH1 and SA



				lifetime 28800 seconds; phase2: DES+MD5, PFS off, no anti-replay and SA lifetime 28800 seconds. The length of pre-shared key is between 8 to 31 ASCII characters.
		switch	<on off>	Activate or de-activate the secured remote access tunnel.
	keep_alive	<rule #>	<on off>	Set ipsec keep_alive flag
	load	<rule #>		Load ipsec rule
	save			Save ipsec rules
	config	netbios	active <on off>	Set netbios active flag
			group <group index1, group index2...>	Set netbios group
		name	<string>	Set rule name
		name	<string>	Set rule name
		keyAlive	<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		
		teprst		
			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

#### Certificate Management (PKI) Command

[Home](#)

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

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

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

		view <name>		View the specified directory service. <name> specifies the name of the directory server to be viewed.
		edit <name> <addr[:port]> [login:pswd]		Edit the specified directory service. <name> specifies the name of the directory server to be edited. <addr[:port]> specifies the server address (required) and port (optional). The format is "server-address[:port]". The default port is 389. [login:pswd] specifies the login name and password, if required. The format is "[login:password]".
		list		List all directory service names and basic information.
		rename <old name> <new name>		Rename the specified directory service. <old name> specifies the name of the directory server to be renamed. <new name> specifies the new name as which the directory server is to be saved.
	cert_ma nager			
		reinit		Reinitialize the certificate manager.

#### Bandwidth management Related Command

[Home](#)

Command						Description
bm						
	interfac e	lan	enable	<bandwidth xxx>		Enable bandwidth management in LAN with bandwidth xxx bps. If the user doesn't set the bandwidth, the default value is 100Mbps.
				<wrr pr>		Select fairness-based(WRR) or priority-based(PRR) mechanism. the default value is fairness-based.
				<efficient>		Enable work-conserving feature.
			disable			Disable bandwidth management in LAN
		wan	enable	<bandwidth xxx>		Enable bandwidth management in WAN with bandwidth xxx bps. If the user doesn't set the bandwidth, the default value is 100Mbps.
				<wrr pr>		Select fairness-based(WRR) or priority-based(PRR) mechanism. the default value is fairness-based.
				<efficient>		Enable work-conserving feature.
			disable			Disable bandwidth management in WAN
		dmz	enable	<bandwidth xxx>		Enable bandwidth management in DMZ with bandwidth xxx bps. If the user doesn't set the bandwidth, the default value is 100Mbps.
				<wrr pr>		Select fairness-based(WRR) or priority-based(PRR) mechanism. the default value is fairness-based.
				<efficient>		Enable work-conserving feature.
			disable			Disable bandwidth management in DMZ
		wlan	enable	<bandwidth xxx>		Enable bandwidth management in WLAN with bandwidth xxx bps. If the user doesn't set the bandwidth, the default value is 100Mbps.
				<wrr pr>		Select fairness-based(WRR) or priority-based(PRR) mechanism. the default value is fairness-based.
				<efficient>		Enable work-conserving feature.
			disable			Disable bandwidth management in WLAN

	class	lan	add #	bandwidth xxx	<name xxx>	Add a class with bandwidth xxx bps in LAN. The name is for users' information.
					<priority x>	Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The default value is 3.
					<borrow on/off>	The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The default value is off.
			mod #	<bandwidth xxx>		Modify the parameters of the class in LAN. The bandwidth is unchanged if the user doesn't set a new value.
				<name xxx>		Set the class' name.
				<priority x>		Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The priority is unchanged if the user doesn't set a new value.
				<borrow on/off>		The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The borrow is unchanged if the user doesn't set a new value.
			del #			Delete the class # and its filter and all its children class and their filters in LAN.
		wan	add #	bandwidth xxx	<name xxx>	Add a class with bandwidth xxx bps in WAN. The name is for users' information.
					<priority x>	Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The default value is 3.
					<borrow on/off>	The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The default value is off.
			mod #	<bandwidth xxx>		Modify the parameters of the class in WAN. The bandwidth is unchanged if the user doesn't set a new value.
				<name xxx>		Set the class' name.
				<priority x>		Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The priority is unchanged if the user doesn't set a new value.
				<borrow on/off>		The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The borrow is unchanged if the user doesn't set a new value.
			del #			Delete the class # and its filter and all its children class and their filters in WAN.
		dmz	add #	bandwidth xxx	<name xxx>	Add a class with bandwidth xxx bps in DMZ. The name is for users' information.
					<priority x>	Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The default value is 3.
					<borrow on/off>	The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The default value is off.
			mod #	<bandwidth xxx>		Modify the parameters of the class in DMZ. The bandwidth is unchanged if the user doesn't set a new value.
				<name xxx>		Set the class' name.
				<priority x>		Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The priority is unchanged if the user doesn't set a new value.
				<borrow on/off>		The class can borrow bandwidth from its parent

						class when the borrow is set on, and vice versa. The borrow is unchanged if the user doesn't set a new value.
			del #			Delete the class # and its filter and all its children class and their filters in DMZ.
		wlan	add #	bandwidth xxx	<name xxx>	Add a class with bandwidth xxx bps in WLAN. The name is for users' information.
					<priority x>	Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The default value is 3.
					<borrow on off>	The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The default value is off.
			mod #	<bandwidth xxx>		Modify the parameters of the class in WLAN. The bandwidth is unchanged if the user doesn't set a new value.
				<name xxx>		Set the class' name.
				<priority x>		Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The priority is unchanged if the user doesn't set a new value.
				<borrow on off>		The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The borrow is unchanged if the user doesn't set a new value.
			del #			Delete the class # and its filter and all its children class and their filters in WLAN.
	filter	lan	add #	Daddr <mask Dmask> Dport Saddr <mask Smask> Sport protocol		Add a filter for class # in LAN. The filter contains destination address (netmask), destination port, source address (netmask), source port and protocol. You may set the value as 0 if you do not care the item.
			del #			Delete a filter which belongs to class # in LAN.
		wan	add #	Daddr <mask Dmask> Dport Saddr <mask Smask> Sport protocol		Add a filter for class # in WAN. The filter contains destination address (netmask), destination port, source address (netmask), source port and protocol. You may set the value as 0 if you do not care the item.
			del #			Delete a filter which belongs to class # in WAN.
		dmz	add #	Daddr <mask Dmask> Dport Saddr <mask Smask> Sport protocol		Add a filter for class # in DMZ. The filter contains destination address (netmask), destination port, source address (netmask), source port and protocol. You may set the value as 0 if you do not care the item.
			del #			Delete a filter which belongs to class # in DMZ.
		wlan	add #	Daddr <mask Dmask> Dport Saddr <mask Smask> Sport protocol		Add a filter for class # in WLAN. The filter contains destination address (netmask), destination port, source address (netmask), source port and protocol. You may set the value as 0 if you do not care the item.
			del #			Delete a filter which belongs to class # in WLAN.
	show	interface	lan			Show the interface settings of LAN
			wan			Show the interface settings of WAN
			dmz			Show the interface settings of DMZ
			wlan			Show the interface settings of WLAN
		class	lan			Show the classes settings of LAN

			wan			Show the classes settings of WAN
			dmz			Show the classes settings of DMZ
			wlan			Show the classes settings of WLAN
		filter	lan			Show the filters settings of LAN
			wan			Show the filters settings of WAN
			dmz			Show the filters settings of DMZ
			wlan			Show the filters settings of WLAN
		statistics	lan			Show the statistics of the classes in LAN
			wan			Show the statistics of the classes in WAN
			dmz			Show the statistics of the classes in DMZ
			wlan			Show the statistics of the classes in WLAN
	monitor	lan	<#>			Monitor the bandwidth of class # in LAN. If the class is not specific, all the classes in LAN will be monitored. The first time you key the command will set it on; the second time you will set it off, and so on.
		wan	<#>			Monitor the bandwidth of class # in WAN. If the class is not specific, all the classes in WAN will be monitored. The first time you key the command will set it on; the second time you will set it off, and so on.
		dmz	<#>			Monitor the bandwidth of class # in DMZ. If the class is not specific, all the classes in DMZ will be monitored. The first time you key the command will set it on; the second time you will set it off, and so on.
		wlan	<#>			Monitor the bandwidth of class # in WLAN. If the class is not specific, all the classes in WLAN will be monitored. The first time you key the command will set it on; the second time you will set it off, and so on.
	config	save				Save the configuration.
		load				Load the configuration.
		clear				Clear the configuration.