ZyXEL

Firmware Release Note

ZyWALL 70

Release 3.63(WM.2)

Date:	**January, 31, 2005**
Author:	**Stanley Liu**
Project Leader:	**Stanley Liu**

ZyXEL ZyWALL 70 Standard Version
Release 3.63(WM.2)
Release Note

Date: January 31, 2005

Supported Platforms:

ZyXEL ZyWALL 70

Versions:

ZyNOS Version: V3.63(WM.2) | 01/31/2005
BootBase : V1.07 | 01/17/2005
Vantage Agent Version : 2.0.2-b3

Notes:

1. **Restore to Factory Defaults Setting Requirement: No.**
2. 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.
3. 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.
4. 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.
5. When firewall turns from "off" to "on", the firewall initialization procedure will disconnect all connections running through the ZyWALL.
6. 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.
7. 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, 802.1X and WPA when you enable WLAN feature.
8. 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.
9. The default max NAT session number per host is changed to 1500.
10. In bridge mode, If LAN side DHCP clients want to get DHCP address from WAN side DHCP server, you may need to add and turn on the firewall rule for BOOT_CLIENT service type in WAN→LAN direction.
11. If you were using MSN Messenger Voice Communication through ZyWALL UPnP and found voice is blocked by firewall, we suggest you download MSN Messenger

7.0 and try again. This is because we found MSN Messenger 6.2 sometimes fails to detect UPnP status when it's starting voice invitation.

Known Issues:

1. Currently, ZyWALL Multiple WAN does not support WAN 1/WAN 2 on the same sub-net. If you configure WAN 1 and WAN 2 to “Ethernet” encapsulation, you should not connect then to the same IP subnet.
2. Sometimes on screen the “Local Area Connection” icon for UPnP disappears. The icon shows again when restarting PC.
3. When you use MSN messenger, sometimes you fail to open special applications, such as whiteboard, file transfer and video etc. You have to wait more than 3 minutes and retry these applications..
4. On the SUA/ Address Mapping page, users can enter two or above same rules.
5. On the SUA/ Address Mapping Edit page, the user can give the same local IP and global IP.
6. SMT 15.1, if we try to edit the 11th rule, 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. 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.
13. When device boots in Bridge Mode, some CI command error messages will be displayed on console. This is because some predefined CI commands in autoexec.net is forbidden to execute in Bridge Mode.
14. Under Bridge Mode, all DMZ ports will behave as a hub.
15. Don’t use CI command “bridge rstp bridge enable” to enable RSTP” to enable RSTP, it will change the initial Path Cost value to an incorrect value..
16. G-100 WLAN card, does not support the fragment size below 800.
17. If ZyWALL WAN is setup to PPPoE/PPTP, it would be trigger to dial to ISP when any one from the LAN side trying to access ZyWALL itself(for example, ping to ZyWALL LAN IP).
18. ZyWALL would not update to the DDNS server if it use Dial Backup to connect to ISP.
19. In eWC/NAT/NAT Overview page, after copy port forwarding rules, it would not take effect until the user click “Apply” on eWC/NAT/Port Forwarding page.

20. Bandwidth management H.323 service does not support Netmeeting H.323 application.
21. The setup of bandwidth services doesn't take effect when the WAN encapsulation is PPPoE or PPTP.
22. On the eWC/VPN/EDIT VPN RULE page, if the user gives a Remote ID Content with the length exceeds 32 characters, some fields(for example, My Address) would not show correct values.

Features:

Modifications in V 3.63(WM.2) | 01/31/2005
Modify for formal release.

Modifications in V 3.63(WM.2)b2 | 01/27/2005
1. [BUG FIX]
   Symptom: ZyWALL 70's throughput is very slow
   Condition:
   (1) Use smartbit to measure LAN->WAN pure routing throughput.
   (2) The throughput is much slower than previous version 3.63(WM.1)

Modifications in V 3.63(WM.2)b1 | 01/17/2005
1. [BUG FIX]
   Symptom: A firewall rule is created automatically after Click on Cancel button.
   Condition:
   (1) On GUI>FIREWALL>Summary, Click on "Insert" button to go to the firewall edit rule screen.
   (2) Click on "Add" to create Custom Port Service in Firewall.
   (3) Delete the above created Custom Port Service.
   (4) Click on Cancel button, back to summary page, a firewall rule is created automatically.
2. [BUG FIX]
   Symptom: The CI command "ip nat service irc" may display strange Enable state.
   Condition:
   (1) Execute "ip nat service irc test_is_good".
   (2) Execute "ip nat service irc 0".
   (3) Execute "ip nat service irc test_is_bad".
   (4) After Step 3, you will see that a strange Enable state, e.g., "IRC enable = 12".
3. [BUG FIX]
   Symptom: System reset after ping.
   Condition:
   (1) Let router's LAN is DHCP server mode. Suppose router's LAN IP is 192.168.1.1.
   (2) PC in LAN side and get IP from router. Suppose PC's LAN IP is 192.168.1.33.
   (3) Turn on UPnP and all related check box. (Make sure that you have turn on UPnP service in your PC).
   (4) PC keeps ping 192.168.1.1.
   (5) Change router's LAN to 192.168.2.1, IP pool start IP address = "192.168.2.33"

(router is Still in DHCP server mode).
(6) Now PC cannot PING to router anymore. After few seconds, router will crash because of system reset in iproute.c (Line 5831).

4. [BUG FIX]
   Symptom & Condition: Port trigger sometimes does not work on certain condition.
5. [BUG FIX]
   Symptom: DHCP client does not work on certian environment.
   Condition: DHCP client does not follow RFC 2131 on rebinding request. According to RFC, it should be broadcast where our device is send unicast.
6. [BUG FIX]
   Symptom: VPN X-Auth wrong setting and VPN tunnel will build up.
   Condition:
   (1) Initiator use X-Auth (client Mode), Phase 1 phase 2 parameter is default.
   (2) Responder rule 1 use X-Auth (Server Mode), and Phase 2 Encryption Algorithm change to 3DES, Security Gateway set Initiator's WAN IP (or Dynamic rule)
   (3) Responder rule 2 not enable X-Auth, and phase 1 and phase 2 parameter the same as Initiator. Security Gateway set Initiator's WAN IP (or Dynamic rule)
   (4) Check log, it will XAUTH Succeed and Swap to Rule 2 ,then Rule 2 built tunnel successfully
7. [BUG FIX]
   Symptom: Packets which size are (1419~1426) can't pass through VPN tunnel.
   Condition:
   (1) Create a VPN tunnel (Encryption Algorithm = AES or 3DES).
   (2) Generate a ping packet (size is from 1419 to 1426), we can't get any response from the remote host through tunnel.
8. [ENHANCEMENT] The CI command "ether edit speed" adds "The device doesn't support LAN ether speed change." alert message.
9. [ENHANCEMENT] Add CI command "ip nat service aol [on|off]" for turning on|off NAT AOL alg.
10. [ENHANCEMENT] Change "keep alive" behavior to "nailed-up" in IPSec

Modifications in V 3.63(WM.1) | 12/12/2004
Modify for formal release.

Modifications in V 3.63(WM.1)b2 | 12/15/2004
1. [ENHANCEMENT]
   User can force ZyWALL to 10/100 half/full mode.
   Note: If user's setting is wrong, the network status will be unstable.
   For example:
   (1) 100/Full<-->10/Half: LED blinking on 10/Half side and link is unstable.
   (2) 100/Half<-->10/Half: The link status is opposite on both side. User should be aware of this issue.
2. [ENHANCEMENT]
   Add "ip urlfilter webControl reginfo refresh" The CI command is to query whether device's external CF had been registered. If yes, write the original license key to flash.

3. [BUG FIX]Symptom: Possible NAT issue in combination with specific SUA entry.
   Condition:
   (1) Go to eWC>NAT Port Forwarding Page set a rule with port start from 10000 to 20000, inactive this rule.
   (2) After some outbound traffic, use CI command “ip nat hashTable enif1” to check, the outgoing port incorrectly start from 20000.
4. [BUG FIX]Symptom: If M-1 & 1-1 are using the same public IP address, it would cause some problem.
   Condition:
   (1) Go to eWC>NAT Address Mapping Page set M-1 NAT and 1-1 NAT with same global IP address.
   (2) The M-1 NAT entries will let the first 1-1 NAT connections fail.
5. [BUG FIX]Symptom: Router will crash under VPN stress test
   Condition:
   (1) Use two ZW35 and configure 40 VPN rules.
   (2) Use SmartBit build up 35 VPN tunnels and run stress test
   (3) Router will crash after a long time
6. [BUG FIX]Symptom: System exception and reboot occur when system name is up to 30 characters long and enable 802.1x.
   Condition:
   (1) Set SMT menu 1 System Name more then 16 characters.
   (2) enable 802.1x or WPA.
   (3) user association.
   (4) system exception.

Modifications in V 3.63(WM.1)b1 | 11/30/2004

1. [ENHANCEMENT] For IP Policy Route,
   (1) The IP routing policy parses first packet only to increase routing efficiency.
   (2) Policy route logs are created on a per-connection basis, instead of per-packet.
2. [ENHANCEMENT]
   Support for DNS queries from WAN to LAN internal DNS server.
3. [BUG FIX] Symptom: The length of Peer Subject Name ID Content in eWC>VPN - EDIT VPN RULE was wrong.
   Condition:
   (1) Go to eWC>VPN - EDIT VPN RULE.
   (2) Click "Certificate" as Authentication Method.
   (3) Choose "Subject Name" for Peer ID Type.
   (4) The max length of Peer Subject Name ID Content is 255 characters, but only up to 31 characters can be entered.
4. [BUG FIX] Symptom: The eWC timeout mechanism sometimes malfunctions.
   Condition:
   (1) Log onto the ZyWALL eWC.
   (2) Go to eWC>Maintenance>General and set the "Administrator Inactivity Timer" as 1 minute.
   (3) Go to eWC>Maintenance>Time&Date and manually set the system time back by an amount more than the system up time.

(4) Do not log out. Wait for more than 1 minute, and then attempt to access the eWC again.
(5) You will find that the eWC has not timed out and is still accessible.

5. [BUG FIX] Symptom: VPN traffic go out by WAN1 and WAN2 while LB enable
   Condition: Turn LB on，built VPN tunnel with WAN1，but actually traffic go out by WAN1 and WAN2
6. [BUG FIX] Symptom: In GUI, System DNS Server configuration is inconsistent .
   Condition:
   HOME>Internet Access, the system DNS server is inconsistent with DNS>Name Server Record.
7. [BUG FIX] Symptom: Bandwidth management ALG can not work on PPPoE and PPTP
   Condition:
   Bandwidth ALG(FTP,SIP,H.323) can not work while WAN is PPPoE / PPTP，FTP ALG can not work CutFTP
8. [BUG FIX] Symptom: On eWC>REMOTE MGMT>CNM help page is missing.
9. [BUG FIX] Symptom: Zywall will reboot.
   Condition: When using BT (Bitspirit) to download, the ZyWALL will reboot itself sometimes.
10. [BUG FIX] Symptom: The system mails logs with the incorrect "DATE" mail header in the daylight saving period.
    Condition:
    (1) Go to eWC->MAINTENANCE->Time and Date page.
    (2) Click the checkbox of "Enable Daylight Saving" option
    (3) Configure ZW70's system time in daylight saving period via the "Start Date" option and the "End Date" option
    (4) Go to eWC->LOGS->Log Settings page
    (5) Configure "E-mail Log Settings"
    (6) Go to eWC->LOGS->View Log page and click "EMail Log Now" button to mail logs
    (7) Receive the mail sent in (6) and check the "DATE" header in the mail is "Date: Fri, 1 Oct 2004 15:34:04 +0800" and not in the daylight saving period. The correct date should be "Date: Fri, 1 Oct 2004 16:34:04 +0900"
11. [BUG FIX] Symptom: Under the remote-access VPN scenario, the mobile user cannot access the internet via the VPN tunnel.
    Condition:
    (1) Configure a dynamic IPSec rule on ZyWALL_a with Local Network as 0.0.0.0 ~255.255.255.255.
    (2) Configure an IPSec rule on a mobile user to connect with ZyWALL_a.
    (3) After a tunnel is established between ZyWALL_a and the mobile user, all the internet-bound traffic from the mobile user will be tunnelled to ZyWALL_a. ZyWALL_a should be able to route these traffics to the internet and then route the responses back to the tunnel. However, ZyWALL_a fails to do so.
12. [BUG FIX] Symptom: The eWC>NAT>PortForwarding>PortTranslation field does not function properly on Mozilla.
    Condition:

(1) Go to eWC>NAT>PortForwarding.
(2) The Port Translation End Port is not disabled.
(3) The Port Translation End Port is not automatically calculated.

13. [BUG FIX] Symptom: WAN2 PPPoE idle timer still functions when Nailed-Up is enabled.
    Condition:
    (1) Restore to default ROM file.
    (2) Connect WAN2 to a DSL modem.
    (3) Set WAN2 encapsulation to ”PPPoE”.
    (4) Enable ”Nailed-Up”.
    (5) After idling for a few minutes, the ZyWALL drops the PPPoE connection. Immediately after the disconnection, the ZyWALL dials a PPPoE connection.
14. [BUG FIX] Symptom: After restarting device, time zone didn’t add one hour in daylight saving.
    Condition:
    (1) In SMT, setup time and date to fall within daylight saving period.
    (2) When restart device, in SMT 24>1, current time didn’t add one hour immediately.
15. [BUG FIX] Symptom: The DHCP server assigns the incorrect static IP to client sometimes.
    Condition:
    (1) Enable LAN DHCP server, PC A and PC B are on LAN side.
    (2) PC A uses the dynamic IP and get IP 192.168.1.33 from the device.
    (3) Set a static IP rule, IP is 192.168.1.33 and mac is PC B.
    (4) After PC A renewing IP, the DHCP server will response 192.168.1.33 to PC
16. [BUG FIX] Symptom: DDNS won’t update when interface is modem Condition:
    (1) Setup DDNS configuration in SMT or eWC. The tested hostnames should enable "HA".
    (2) Unplug WAN1 and WAN2 cable to make WAN disconnection situation.
    (3) DDNS won’t update the hostnames with "HA" when the modem is dialed up.
17. [BUG FIX] Symptom: Firewall judges that Linux traceroute behavior is port scan attack.
    Condition:
    (1) Turn on Firewall
    (2) Linux computer locates in LAN side and traceroute to the host which distance is over 5 hubs.
    (3) Firewall judges that Linux traceroute behavior is port scan attack
18. [BUG FIX] Symptom: DNS query causes cbuf leak.
    Condition:
    Router will sync with NTP server once a day, sometimes this action may be a failure and cause cbuf leak.
19. [BUG FIX] Symptom: For multiple WAN, the UPnP cannot pass through Firewall on WAN 2 interface.
    Condition:
    (1) Enter eWC->UPnP page.
    (2) Enable UPnP all items and select WAN 2 for the outgoing WAN interface.

(3) The device activates firewall.
(4) Test the Windows Messenger failed.

20. [BUG FIX] Symptom: Max Firewall ACL rule will cause device crash.
    Condition:
    (1) Enter eWC->Firewall.
    (2) Add firewall rules to cause acl memory full.
    (3) Add a service port in one firewall rule.
    (4) Save the acl will cause device crash.
21. [BUG FIX] Symptom: Datetime calibration failed to sync with user-defined NTP server.
    Condition:
    (1) Restore default ROM file.
    (2) Go to eWC->MAINTENANCE->Time and Date, set Time Server Address with "time.stdtime.gov.tw".
    (3) Reboot the router.
    (4) Go to eWC->LOG, the router will start time synchronization process, it does not sync user-defined server first (no log).
22. [BUG FIX] Symptom: ZYWALL doesn't perform DDNS update in PPPOE mode
    Condition:
    (1) ZYWALL dials to a remote ISP
    (2) The ISP disconnects PPOE session
    (3) ZYWALL re-dials to the remote ISP and get a different IP
    (4) ZYWALL doesn't perform DDNS update

Modifications in V 3.63(WM.0) | 10/01/2004
Modify for formal release.

Modifications in V 3.63(WM.0)b9 | 09/27/2004
1. [BUG FIX] Symptom & Condition: ZyWALL doesn't log those packets which were blocked or forward by firewall.
2. [ENHANCEMENT] Support CI command "ip alg…" on the bridge mode.
3. [ENHANCEMENT] Extended the size of Remote ID Content field(in eWC/VPN/EDIT VPN RULE page) from 31 to 255.

Modifications in V 3.63(WM.0)b8 | 09/17/2004
1. [BUG FIX] Symptom: If the operation mode of WAN is "Active/Active" mode, ZyWALL could not establish IPSec tunnel on WAN 2.
   Condition: (1) Set the operation mode of WAN to "Active/Active" mode.
   (2) The Route Priority of WAN 1 is higher than the The Route Priority of WAN 2
   (3) Create a IPSec rule with "0.0.0.0" or a domain name of My Address.
   (4) Initial a IPSec tunnel form the remote initiator, and ZyWALL WAN 2 is the response interface.
   (5) ZyWALL would use the WAN 1 interface to response, so it can establish the IPSec tunnel.
4. [BUG FIX] Symptom: In the bridge mode, DHCP client stations on the LAN side

can't get IP information from those DHCP servers on the WAN 2 side or DMZ side.
Condition: (1) Set ZyWALL to the Bridge mode.
(2) Go to eWC/BW MGNT/Summary page, and enable WAN 2 and DMZ to active.
(3) Connect a DHCP Client station on the LAN side, and try to get IP information form those DHCP servers on the WAN 2 side or DMZ side.
(4) The station can't get IP information.

5. [BUG FIX] Symptom & Condition: Sometime, ZyWALL would exhaust all its internal data structure, cbuf, and let itself to restart.
6. [BUG FIX] Symptom: ZyWALL Content Filtering can't filter forbidden web sites.
Condition: (1) Enable ZyWALL's Content Filtering feature.
(2) Give ZyWALL forbidden web sites URLs and save them. For example "sina.com".
(3) ZyWALL could forbid the user to access www.sina.com, if the user directly key in the URL to his browser.
(4) If the user uses a search engine (for example: www.google.com) to search those forbidden web sites and click them from the search engine, ZyWALL could not block the user's access.
7. [BUG FIX] Symptom: ZyWALL's Bandwidth Management doesn't work, if the user select a Service (FTP, H.323, or SIP) on the filter configuration.
Condition: (1) Go to eWC/BW MGNT/Summary page, enable one or some interface classes.
(2) Go to eWC/BW MGNT/Class setup page, click "Add Sub-Class" or "Edit" to setup a Class/Filter configuration.
(3) Setup Class and Filter configuration. The Service is setup to "FTP", "SIP" or "H.323", and the user should specify the Source IP Address.
(4) ZyWALL's would limit all traffic even the source of traffic is not equal to the source IP of the Filter configuration.
8. [ENHANCEMENT] eWC/BW MGNT/Class setup page, if the user select any service (FTP, H.323 or SIP), the Destination Port, Source Port, and Protocol ID would be grayed out.
9. [ENHANCEMENT] Supports SIP ALG for ZyXEL Wi-Fi phone under P-2-P condition.
10. [ENHANCEMENT] Supports SIP ALG for ZyXEL P2002 device.

Modifications in V 3.63(WM.0)b7 | 09/02/2004

1. [BUG FIX] Symptom & Condition. Some Static Routes created by ZyWALL 70, V3.62 F/W, would be erased, when upgrade ZyWALL 70 to V3.63(WM.0)b6 F/W.

Modifications in V 3.63(WM.0)b6 | 09/01/2004

2. [BUG FIX] Symptom: IGMP packet can not pass through ZyWALL 70 via WAN2 port.
Condition: (1) In ZyWALL 70, turn off Firewall.
(2) Connect an IPTV Server to WAN2 interface.

(3) Turn on Multicast for LAN interface, use IPTV Viewer at LAN side to watch IPTV.
(4) LAN side host get nothing

3. [BUG FIX] Symptom & Condition. Those Firewall ACL rules created by ZyWALL 70, V3.62 F/W, have no effects, when upgrade ZyWALL 70 to V3.63(WM.0)b5 F/W.
4. [BUG FIX] Symptom: ZyWALL would leak mbuf.
   Condition: (1) Let ZyWALL 70 be a DNS proxy server.
   (5) All stations on the ZyWALL LAN side would see ZyWALL as DNS server and send DNS query to ZyWALL.
   (6) ZyWALL would exhaust its memory buffer for receiving and sending packets. Finally ZyWALL couldn't forward any network traffic any more.
5. [BUG FIX] Symptom: ZyWALL would leak mbuf.
   Condition: (1) Set ZyWALL to Bridge Mode.
   (7) Enable the External Database Content Filtering
   (8) ZyWALL would exhaust its memory buffer for receiving and sending packets. Finally ZyWALL couldn't forward any network traffic any more.
6. [BUG FIX] Symptom: Could not save settings on eWC/DMZ page
   Condition: (1) Go to eWC/DMZ page.
   (9) Enable "Allow between DMZ and LAN" and "Allow between DMZ and WAN".
   (10) Click "Apply", but ZyWALL does not save the above settings.
7. [BUG FIX] Symptom: In bridge mode, SMT24.1 shows error status in WAN interface.
   Condition: (1) In router mode, set WAN1 to PPTP mode.
   (11) Change router as bridge mode and the WAN1 status in SMT24.1 shows "Idle".
   (12) In bridge mode, the status should the same with Ethernet mode("Down" or "100M/FULL"), but it the status is "Idle".
8. [BUG FIX] Symptom: Content filter timeout problem.
   Condition: (1) A router register the content filter (CF) server.
   (13) Enable the Content Filtering feature.
   (14) Enable the External Database Content Filtering.
   (15) The router log often record "Waiting content filter server (server name) timeout!".
   (16) The station on the LAN side fetches web sites from the internet often wait a longer time.
9. [BUG FIX] Symptom: Those settings of DNS server would be over-written when ZyWALL is in Bridge Mode.
   Condition: (1) In Bridge Mode, go to eWC/Bridge page to setup DNS servers.
   (17) Goto eWC/MAINTENANCE/General page, click "Apply".
   (18) Return back to eWC/Bridge page, those setting of DNS servers were gone.
10. [ENHANCEMENT] New CI command "ip alg enable/disable ALG_SIP" to enable or disable SIP ALG.

11. [ENHANCEMENT] New CI command “ip alg siptimeout“ to set the timeout value of SIP.

Modifications in V 3.63(WM.0)b5 | 08/13/2004

1. [BUG FIX] Symptom: In ZyWALL bridge mode, SMT 24.1 does not show the correct status of WAN.
   Condition: (1) Set the WAN interface to PPPoE or PPTP mode.
   (19) Change ZyWALL from “Route mode” to “Bridge Mode”
   (20) Go to SMT 24.1
   (21) SMT 24.1 shows the status of WAN is “Idle”, not “Down”.
2. [BUG FIX] Symptom: System crashes, when the Load Balancing Algorithm is “Spillover”.
   Condition: (1) Set the operation mode of WAN to “Active/Active” mode.
   (22) Select “Spillover” as the Load Balancing Algorithm.
   (23) Use a packet generator S/W to generate a lot of UDP packets, on the ZyWALL LAN side.
   (24) Restart the system.
   (25) The system will crash.
3. [BUG FIX] Symptom and Condition: If turn on Bandwidth Management or Load Balancing, the performance of the system becomes very poor.
4. [BUG FIX] Symptom and Condition: System crashes, if the user setup ZyWALL WLAN (using G-100 card) security mode to WPA/WPA-PSK.
5. [BUG FIX] Symptom & Condition: Dial Backup doesn’t work when the router priority of Traffic Redirect is lower than the router priority of Dial Backup.
6. [BUG FIX] Symptom and Condition: WAN to LAN IGMP packets would be blocked by ZyWALL Firewall, even exists a ACL rule to allow IGMP packets.

Modifications in V 3.63(WM.0)b4 | 08/06/2004

7. [BUG FIX] Symptom: When click Apply, status bar will show error message in eWC>Logs>Reports.
   Condition: (1) Check or uncheck "Send Raw Traffic Statistics to Syslog Server for Analysis"
   (2) Click "Apply".
   (3) Status bar shows 'Nothing changed; no need to perform save".
8. [ENHANCEMENT] Add DNS Server Info into eWC/Bridge/Bridge page.
9. [BUG FIX] Symptom: ZyWALL crashes when a lot of TCP connections connect to ZyWALL’s port 80.
   Condition: (1) Use a application S/W, session.exe, to generate a lot of TCP connections to connect to the port 80 of ZyWALL.
   (2) After several hundreds of sessions were established, the ZyWALL hung and finally rebooted.
10. [BUG FIX] Symptom: IPSec tunnel will fail to be built when use aggressive mode with PKI support.
    Condition: (1) Set a VPN rule with aggressive mode.
    (2) Use PKI to be authentication method.
    (3) Save and try to trigger this tunnel will fail.

11. [FEATURE CHANGE]
    WAS: ZyWALL always shows that the date and time of “ras" and “rom-0” are Jul 01 12:00".
    IS: ZyWALL shows that the date and time of “ras" is the built time of F/W and the date and time of “rom-0" is the last update time of “rom-0”.
12. [FEATURE CHANGE]
    WAS: MAC spoofing would be applied to WAN 1 and WAN 2, even if ZyWALL be configured to “Bridge Mode”.
    IS: If ZyWALL is in “Bridge Mode”, MAC spoofing would not be applied to WAN 1 and WAN 2.
13. [FEATURE CHANGE] Changed some words on SMT 1.1.1 -- DDNS Edit Host.
    (2) Changed "Use IP Address" to "Use WAN IP Address".
    (3) Changed "Use Specified IP Address" to "Use User-Defined".
    (4) Changed "DDNS Server Auto Detect IP Address" to "Let DDNS Server Auto Detect".
14. [BUG FIX] Symptom & Condition: The “Check WAN Connectivity” function does not work when the ZyWALL WAN operation mode is “Activie/Active” mode and the encapsulation mode is “PPTP”.
15. [BUG FIX] Sometimes the ZyWALL reboots by software watchdog.
16. [BUG FIX] Symptom: ZyWALL eWC/Home/Statistics still shows WAN 1 traffic while WAN1 is disconnected.
    Condition: (1) Setup WAN1 to PPTP.
    (2) Connect WAN 1 to ISP and make some traffic go through WAN 1.
    (3) Pull out the WAN 1.
    (4) Open the “Statistics” windows, it will show that there are some traffic on WAN 1.
17. [BUG FIX] Symptom & Condition: In eWC/CERTIFICATES/My Certificates/Create, ZyWALL can’t show the correct help page.
18. [BUG FIX] Symptom: ZyWALL doesn’t according to the Load Balancing algorithm to route traffic to WAN 1 and WAN 2.
    Condition: (1) Configure ZyWALL WAN operation mode to “Active/Active” mode.
    (2) Select “Spillover” as the Load Balancing Algorithm.
    (3) Change the primary WAN from WAN 1 to WAN 2.(The router priority of WAN 2 is higher than WAN 1)
    (4) Start to do transfer data from LAN to WAN, but ZyWALL only use WAN 2 to send data.
19. [BUG FIX] Symptom & Condition: ZyWALL crashes very often in bridge mode.
20. [BUG FIX] Symptom: SMT 2 doesn’t show the correct MAC spoofing status.
    Condition: (1) Use eWC/WAN/WAN 1 page setup MAC spoofing.
    (2) After ZyWALL save configurations successfully, go to SMT 2.
    (3) The field, “Assigned By” does not the correct setting, “IP address attached on LAN”.
21. [BUG FIX] Symptom & Condition: Traffic Redirect doesn’t work when the router priority of Traffic Redirect is lower than the router priority of Dial Backup.
22. [BUG FIX] ZyWALL doesn’t update new IP address DDNS server when WAN gets a new IP address, if the WAN operation mode is “Active/Passive”.

Condition: (1) Set WAN Operation Mode to “Active/Passive”.
(2) Set one DDNS rule for WAN 1. The IP Address Update Policy is “Use WAN IP Address”. HA is disabled.
(3) After changing the IP address of WAN 1, ZyWALL wouldn’t update the IP address on DDNS server.

Modifications in V 3.63(WM.0)b3 | 07/13/2004

23. [BUG FIX] Symptom: The ZyWALL crashes and reboots when deleting a FTP Bandwidth Management class.
    Condition: (1) Add a Bandwidth Management sub-class and the FTP service of the filter of this sub-class is enabled.
    (2) Create FTP traffic to apply to the sub-class created at step(1).
    (3) Delete the sub-class created at step(1).
    (4) Router crashes and reboots.
24. [BUG FIX] Symptom: In the eWC, Statistics of WAN 1/WAN 2 are incorrect if WAN 1/WAN 2 is PPPoE/PPTP.
    Condition: (1) Setup WAN 1/WAN 2 to PPPoE or PPTP encapsulation.
    (2) Make some traffic on WAN 1 or WAN 2.
    (3) Click “Show Statistics” on eWC/Home page to open the Statistics windows.
    (4) Tx and Rx of WAN 1 and WAN 2 are 0, even there are traffic on WAN 1 or WAN 2.

Modifications in V 3.63(WM.0)b2 | 07/06/2004

1. [ENHANCEMENT] ZyWALL would popup a windows to ask the user “Are you sure you want to logout ?”. The use can click the “Yes”, and ZyWALL shows the login dialog box again.
2. [ENHANCEMENT] Removed “Show LB Statistics” button from eWC/Home page. The user can click the button in the top-left of eWC/Home page to see the throughput of each interface.
3. [ENHANCEMENT] Enhanced the eWC/Home page, information for LAN/DMZ IP alias were added. Users can expand or collapse LAN and DMZ to show or hide the IP Alias information by clicking the [+]/[-] icon.
4. [ENHANCEMENT] In eWC/Home page, the Current Time and the Current Date are merged to one System Time.
5. [ENHANCEMENT] In eWC/Home page, the NAT concurrent session is changed to Sessions.
6. [ENHANCEMENT] Support new Load Balancing Algorithms: Weight Round-Robin and Spilover. The “Dynamic Load Balancing” Algorithms is changed to “Least Load First” algorithm.
7. [ENHANCEMENT] In eWC/LOGS/Log Setting page, added new log types for Triangle route and Broadcast/Multicast.
8. [ENHANCEMENT] In SMT 15.1.1, support to edit to 100 NAT mapping rules.
9. [ENHANCEMENT] In SMT 15.1.2, support to edit to 100 Port forwarding rules.
10. [ENHANCEMENT] In eWC/VPN/VPN Rule Setup page, added “dial” icon for each

VPN rule to manual dial VPN connection.

11. [ENHANCEMENT] In eWC/LOGS/Reports, (1) Used the "Collect statistics" check box instead of “Start Collection” button. (2) Added “Send raw traffic statistics to syslog server for analysis" check box. (3) Added “Flush” button, would be used to clear all reports.
12. [ENHANCEMENT] Support full URL checking content filtering. WAS: ZyWALL only takes domain name or IP address of URL into category checking. IS: ZyWALL takes entire URL into category checking.
13. [BUG FIX] Symptom & Condition: Can’t configure the spoof MAC address on WAN 2.
14. [BUG FIX] Symptom: TCP bandwidth usage is too low when the service is managed by Bandwidth management.
    Condition: If there is a TCP service going through ZyWALL and is managed by router’s bandwidth management mechanism, the bandwidth of this service is much slower than the limited bandwidth.
15. [BUG FIX] Symptom: In eWC/VPN/MANUAL KEY page, exists an incorrect DNS Server field.
    Condition: (1) Enter the eWC/VPN page.
    (2) Click “Add” button to add a new VPN rule.
    (3) Change the Key Management from “IKE” to “Manual Key”
    (4) The DNS Server has a wrong display "0.0.0.7".
16. [BUG FIX] Symptom & Condition: ZyWALL don’t drop the Dial Backup connection even the WAN 1 or WAN 2 rolls back.
17. [ENHANCEMENT] In SMT 24.4, ZyWALL supports DHCP Release/Renew for WAN 1 and WAN 2.
18. [BUG FIX] Symptom: ZyWALL would not add those routing table entries for static route.
    Condition: (1) Go to the SMT 12, add a static route. The address of the gateway of this static route is located at the sub-net WAN 1 connect to.
    (2) Unplug the WAN 1, and reboot ZyWALL.
    (3) After ZyWALL reboot, go to SMT 24.8, enter the command “ip route status”
    (4) ZyWALL does not create the corresponded routing table entry for the static route.
19. [BUG FIX] Symptom & Condition: When a WAN interface goes down, those ARP entries related to this interface still exist in the ARP table.
20. [ENHANCEMENT] Change the Daylight Saving mechanism. The user can use the week day to setup the duration of Daylight Saving.
21. [BUG FIX] Symptom: FTP traffic still can be managed by Bandwidth Management even when we disable FTP service for Bandwidth Management filter.
    Condition: (1) Setup a sub-class WAN1-1 on WAN1 interface.
    (2) Enable filter and select FTP service for sub-class WAN1-1, now FTP traffic is managed by sub-class WAN1-1.
    (3) Disable filter for sub-class WAN1-1, the FTP traffic is still managed by sub-class WAN1-1, but it should not.
22. [BUG FIX] Symptom: MSN Messenger's "Ask for Remote Assistance" function

causes system crash.
Condition: (1) Enable the UPnP on ZyWALL
(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.

23. [BUG FIX] Symptom: ZyWALL itself can not access Internet by using Dial Backup
Condition: (1) Enable Dial Backup, then disconnect all LAN/WAN interface to trigger Dial Backup.
(2) ZyWALL itself can not access Internet. ZyWALL ping to the internet fail.
24. [BUG FIX] Symptom & Condition: WAN 2 received a lot of packets, even the destination MAC address of the packet is not the MAC address of WAN 2.
25. [BUG FIX] Symptom: ZyWALL do connectivity check fail, if the WAN is in the PPTP.
Condition: In WAN PPTP mode, the device would get an IP address 17.1.2.3, but its default gateway of check point is 10.0.0.138, so ZyWALL can't get the ICMP Echo response from the check point.
26. [BUG FIX] Symptom & Condition: NAT lookback doesn't work on WAN 2.
27. [BUG FIX] Symptom: After system reboot, the UPnP outgoing interface is WAN 1 but the setting is WAN 2.
Condition: (1) Set UPnP outgoing interface is WAN 2.
(2) Reboot the device.
(3) The UPnP outgoing interface information on Ports page is WAN 1 and file transmit is via WAN 1.
28. [BUG FIX] Symptom & Condition: ZyWALL always do rom converting when starting.
29. [BUG FIX] Symptom & Condition: Can't login ZyWALL by using eWC, after the user changed the password.
30. [BUG FIX] Symptom: In eWC/NAT/Address Mapping page, the "Go-To-Page" dropdown list would be corrupted, if the user adds more than 90 address mapping rules.
Condition: (1) Go to eWC/NAT/Address Mapping page.
(2) Add more than 90 address mapping rules.
(3) Go to the 10th page by selecting from the "Go-To-Page" dropdown list.
(4) The "Go-To-Page" dropdown list becomes empty.
31. [BUG FIX] Symptom: IPSec Rule swapping behavior is not correct.
Condition: Case 1
(5) The IPSec initiator has one VPN rule with aggressive mode.
(6) The responder has three rules:
- Rule 1 is aggressive mode, dynamic rule.
- Rule 2 is main mode, static rule. Phase 2 peer ID is not correct.
- Rule 3 is aggressive mode, static rule. All parameters are correct.

(7) Can't create the VPN tunnel successfully.

Condition: Case 2

(1) The IPSec initiator has one VPN rule with aggressive mode.

(2) The responder has three rules:

- Rule 1 is aggressive mode, static rule.
- Rule 2 is aggressive mode, dynamic rule. All parameters are correct.
- Rule 3 is aggressive mode, static rule. All parameters are correct.

(3) Can't create the VPN tunnel successfully.

32. [BUG FIX] Symptom: Can not ignore those DOS attacks from WAN 2.
    Condition: (1) Connect ZyWALL WAN 2 port to an activated sun-net.
    (2) Use CI command to ignore DOS attack on WAN port.
    (3) Do port scan S/W to scan ZyWALL WAN 2.
    (4) Check sys log, the log says it got the attacks from WAN..
33. [BUG FIX] Symptom & Condition: In ZyWALL bridge mode, eWC\Home\Network Status\LAN\Status would show the correct status, if the user doesn't connect the LAN port.
34. [BUG FIX] Symptom & Condition: ZyWALL can't use USR Courier, V.Everything as the Dial Backup external modem.

Modifications in V 3.63(WM.0)b1 | 06/04/2004

1. [FEATURE CHANGE] New feature, Multiple WAN Access. Please see Appendix 7.
2. [FEATURE CHANGE] New feature, Load Balancing.
3. [FEATURE CHANGE] New feature, DNS Server.
4. [FEATURE CHANGE] New feature, Bridge Mode.
5. [FEATURE CHANGE] New feature, Wi-Fi Protected Access(WPA) on WLAN. Please Appendix 8.
6. [FEATURE CHANGE] New feature, Firewall/NAT/Bandwidth Management ALG for SIP/H.323
7. [ENHANCEMENT] Support up to 100 IPSec VPN connections simultaneously. User can configure 120 IPSec policies.
8. [ENHANCEMENT] Support 48 policy route rules.
9. [ENHANCEMENT] Support 12000 NAT sessions.
10. [ENHANCEMENT] Support up to 100 NAT rules and 100 port forwarding rules.
11. [ENHANCEMENT] Firewall ACL buffer size is up to 80K bytes, the user can configure up to 100 customer ports.
12. [ENHANCEMENT] The size of the cache of Cerberian content filter is up to 4096K bytes.
13. [ENHANCEMENT] Support to use ZyAIR B-120 and ZyAIR G-100 WLAN card.
14. [ENHANCEMENT] Added call schedule for dial backup. The SMT 11.1, for dial backup, has the "Schedules=" option to enable schedule rules.
15. [ENHANCEMENT] Add a new firewall service type – Road runner(TCP/UDP:1026)

in eWC/FIREWALL/EDIT RULE..

16. [ENHANCEMENT] In eWC/Home page, added a new entry for displaying Dial Backup status into the Network Status table.
17. In eWC/Home page, ZyWALL would display the current NAT session number for WAN 1 and WAN2.
18. [FEATURE CHANGE] In eWC/LAN/LAN page, those settings for DNS Server addressed has been moved to eWC/DNS/LAN page.
19. [FEATURE CHANGE] In eWC/WIRELESS LAN, the page 802.1X, has been merged into the security list box of the Wireless page. The user can setup those settings for 802.1X, WPA, and WEP by selecting the security.
20. [ENHANCEMENT] In eWC/WAN, the "Route" tag has been changed to "General" tag.
21. [ENHANCEMENT] In eWC/WAN/General page, a new Operation Mode group has been added in the top of this page. The user can setup ZyWALL to be Active/Passive mode or Active/Active mode. The user also can setup the Load balancing for WAN 1/WAN 2 in here. Please reference to Note XX to know more information about ZyWALL Multiple WAN.
22. [ENHANCEMENT] In eWC/WAN/General page, the wording, "Route Assessment" has been changed to "Connectivity Check".
23. [FEATURE CHANGE] In eWC/WAN/WAN 1 and WAN 2 page, NAT Full Feature selection has been moved to eWC/NAT/NAT overview page.
24. [FEATURE CHANGE] In eWC/WAN/WAN 1 and WAN 2 page, the Windows Networking group has been moved to eWC/WAN/General page.
25. [ENHANCEMENT] In eWC/VPN/VPN//VPN Edit VPN Rule page, the user can setup my IP address to the domain name which the user has been setup in the DNS server. Please see …XX
26. [ENHANCEMENT] eWC/SUA/NAT has been re-designed. The new Web GUI for NAT has four pages, they are NAT Overview, Address Mapping, Port Forwarding, and Port Triggering. WAN 1 and WAN 2 have separated NAT Address Mapping tables, Port Forwarding tables and Port Triggering tables.

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 transmitting 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) Re-key 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 restore 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 packet 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 belong 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 negotiation 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 Telcom 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 Management/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 date 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 process 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 default, 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 port scan. 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 firewall 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.

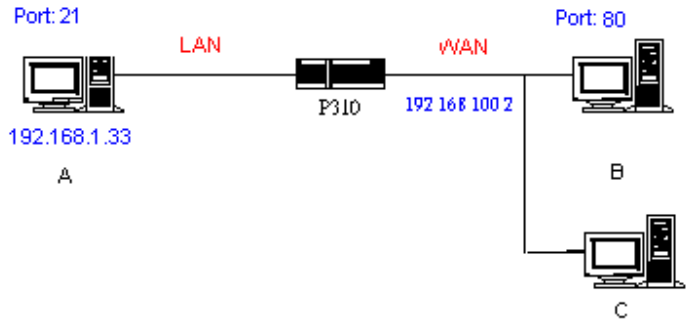
These triggered events can be timed so that they erase the port mapping as soon as they are done with the data transfer, so that the port mapping can be triggered by another Client computer. This gives the ***illusion*** that multiple computers can use the same port mapping at the same time, but the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

How to use it

Following table is a configuration table.

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

How it works



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

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

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

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

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

Notes

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

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

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

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

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

Example ouput:

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

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

Type	Description	Default mode
0	LAN to WAN	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 dail

Appendix 4 Traffic Redirect/Static Route Application Note

Why traffic redirect/static route be blocked by ZyWALL

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

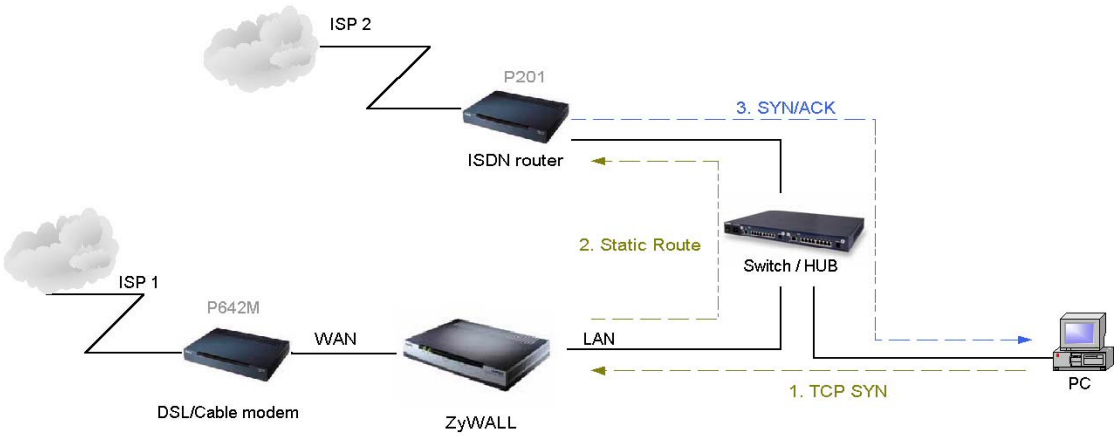


Figure 5-1 Triangle Route

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

Step 1. PC sends outgoing traffics through ZyWALL because default gateway assigned to it.

Step 2. Then, ZyWALL will redirect the traffics to another gateway (ISDN/Router) as we expect.

Step 3. But the return traffics do not go through ZyWALL because the gateway (say, P201) and the PC are on the same IP network. **Any traffic will easily inject into the protected network area through the unprotected gateway**.

Step 4. When firewall turns on, it could be worse. ZyWALL will check the outgoing traffics by ACL and create dynamic sessions to allow legal return traffics. For Anti-DoS reason, ZyWALL will send RST packets to the PC and the peer because it never received TCP SYN/ACK packet.

That causes all of outgoing TCP traffics being reset!

How traffic redirect/static route works under protection - Solutions

(1) Gateway on alias IP network

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

normal function.

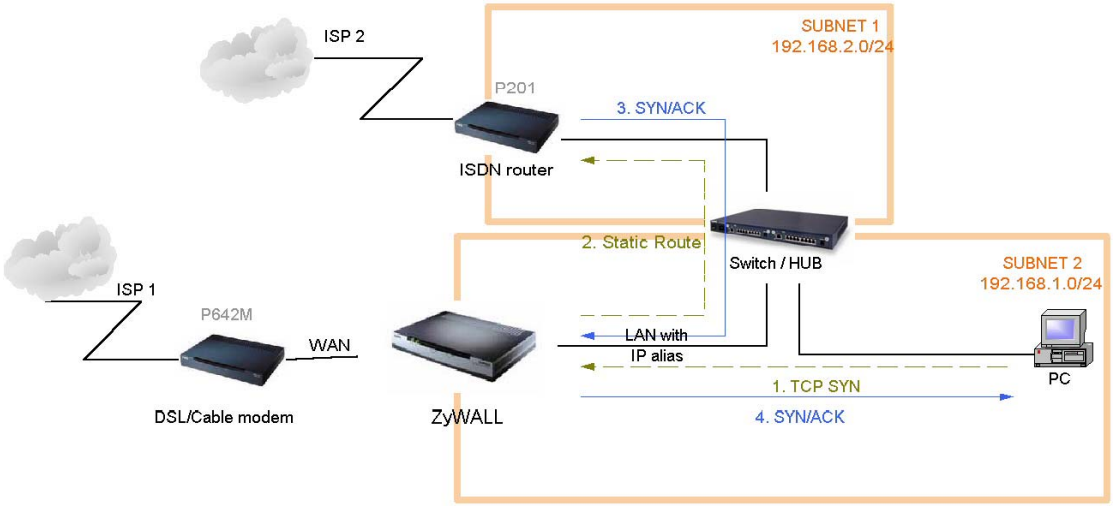


Figure 5-2 Gateway on alias IP network

(2) Gateway on WAN side

A working topology is suggested as below.

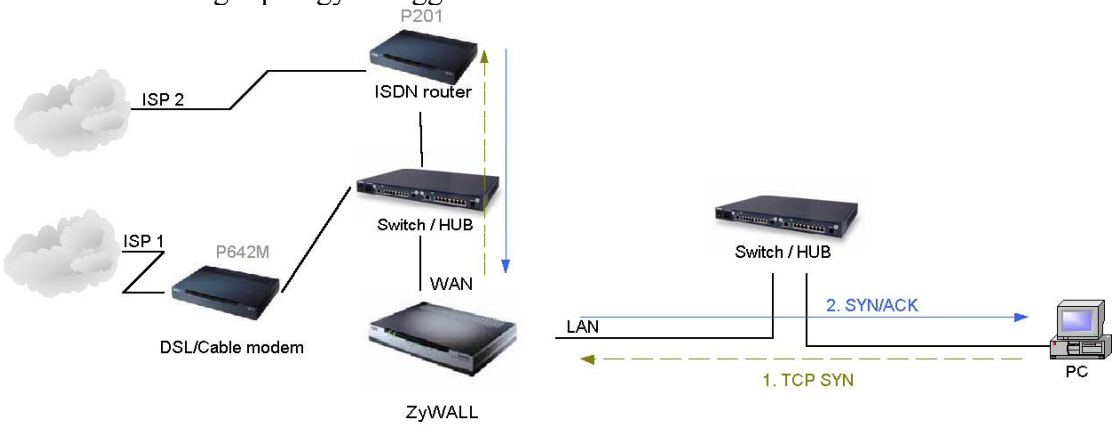


Figure 5-3 Gateway on WAN side

Appendix 5 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.

Appendix 7 Multiple WAN Access

Because of the expansion of broad band service, the bandwidth is more and more cheap. Some of audio and video applications become usable, such as VoIP and video conference. The company will subscribe several links for different application. They may use it for VoIP, Backup line, Load sharing, and extend bandwidth. Thus they will need a device to manage these kinds of application.

The ZyWALL has two independent WAN ports, so it offers the ability to configure a secondary WAN port for highly reliable network connectivity and robust performance. The user can connect WAN 1 to one ISP(or network), and connect the other to a second

ISP(or network). This secondary WAN port can be used in “active-active” load sharing or fail-over configuration providing a highly efficient method for maximizing total network bandwidth.

The default mode of the WAN 2 interface is “Active-Passive” or “Fail-Over” mode, that is the secondary WAN will automatically “bring-up” when the first WAN fails. The user can enter eWC/WAN/General page to select WAN to “Active/Active” mode. At “Active/Active” mode, ZyWALL can access internet through WAN 1 and WAN 2 simultaneously. The user also can setup policy route rule and static route rule to specify the traffic to certain link. ZyWALL Connectivity Check will check the connectivity of WAN 1, WAN 2 and Traffic Redirect. Please notice that even at the “Active/Active” mode, WAN 2 is still the backup line of WAN 1, and WAN 1 is also the backup line of WAN 2.

The user can use policy routing to specify the WAN port that specific services go through. If one WAN port’s connection goes down, the ZyWALL can automatically send its traffic through the other WAN port, if the user allows this traffic to use the other WAN port.

The ZyWALL NAT feature allows the user to give two separate sets of rules(NAT Mapping rules and Port Forwarding rules) for WAN 1 and WAN 2.

The DDNS also has the high availability feature based on Multiple WAN. That is the ZyWALL can use the other WAN interface for domain names if the original configured WAN interface goes down.

Appendix 8 Wi-Fi Protected Access

Wi-Fi Protected Access(WPA) is a subset of the IEEE 802.11i. WPA improves data encryption by using TKIP, MIC and IEEE 802.1X. Because WPA applies 802.1X to authenticate WLAN users by using an external RADIUS server, so you can not use the Local User Database for WPA authentication.

For those users in home or small office, they have no RADIUS server, WPA provides the benefit of WPA through the simple “WPA-PSK”. Pre-Shared Key(PSK) is manually entered in the client and ZyWALL for authentication. ZyWALL will check the client PSK and allow it join the network if it’s PSK is matched. After the client pass the authentication, ZyWALL will derived and distribute key to the client, and both of then will use TKIP process to encrypt exchanging data.

Annex A CI Command List

Last Updated: 2002/11/26

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

System Related Command Home

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

				2:crash save,not in debug mode 3:crash save,in debug mode
	event			
		display		display tag flags information
		trace		display system event information
			display	display trace event
			clear <num>	clear trace event
	extraphnum			maintain extra phone numbers for outcalls
		add	<set 1-3> <1st phone num> [2nd phone num]	add extra phone numbers
		display		display extra phone numbers
		node	<num>	set all extend phone number to remote node <num>
		remove	<set 1-3>	remove extra phone numbers
		reset		reset flag and mask
	feature			display feature bit
	fid			
		display		display function id list
	firmware			display ISDN firmware type
	hostname		[hostname]	display system hostname
	iface			
		disp	[#]	display iface list
	interrupt			display interrupt status
	logs			
		category		
			access [0:none/1:log/2:alert/3:both]	record the access control logs
			attack [0:none/1:log/2:alert/3:both]	record and alert the firewall attack logs
			display	display the category setting
			error [0:none/1:log/2:alert/3:both]	record and alert the system error logs
			ipsec [0:none/1:log/2:alert/3:both]	record the access control logs
			ike [0:none/1:log/2:alert/3:both]	record the access control logs
			javablocked [0:none/1:log]	record the java etc. blocked logs
			mten [0:none/1:log]	record the system maintenance logs
			packetfilter [0:none/1:log]	record the packet filter logs
			pki [0:none/1:log/2:alert/3:both]	record the pki logs
			tcpreset [0:none/1:log]	record the tcp reset logs
			upnp [0:none/1:log]	record upnp logs
			urlblocked [0:none/1:log/2:alert/3:both]	record and alert the web blocked logs
			urlforward [0:none/1:log]	record web forward logs
		clear		clear log
		display	[access|attack|error|ipsec|ike|javablocked|mten|packetfilter|pki|tcpreset|urlblocked|urlforward]	display all logs or specify category logs
		dispSvrIP		Display the IP address of email log server and syslog server

		errlog		
			clear	display log error
			disp	clear log error
			online	turn on/off error log online display
		load		load the log setting buffer
		mail		
			alertAddr [mail address]	send alerts to this mail address
			display	display mail setting
			logAddr [mail address]	send logs to this mail address
			schedule display	display mail schedule
			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
		updatePeriod	<second>	set the log table update period
		updateSvrIP	<minute>	If there is one parameter <minute>, it will change the dns timer task timeout value. Otherwise, do dns resolve to find email log server and syslog server IP.
	mbuf			
		link	link	list system mbuf link
		pool	<id> [type][num]	list system mbuf pool
		status		display system mbuf status
		disp	<address>[1|0]	display mbuf status
		cnt		
			disp	display system mbuf count
			clear	clear system mbuf count
		debug	[on|off]	
	memwrite		<address> <len> [data list ...]	write some data to memory at <address>
	memutil			
		usage		display memory allocate and heap status
		mqueue	<address> <len>	display memory queues
		mcell	mid [f|u]	display memory cells by given ID
		msecs	[a|f|u]	display memory sections
		mtstart	<n-mcell>	start memory test
		mtstop		stop memory test
		mtalloc	<size> [n-mcell]	allocate memory for testing
		mtfree	<start-idx> [end-idx]	free the test memory
	mode	<router/bridge>		switch router and bridge mode

	model			display server model name
	proc			
		display		display all process information
		stack	[tag]	display process's stack by a give TAG
		pstatus		display process's status by a give TAG
	pwc			sends information to PWC via telnet
	pwderrtm		[minute]	Set or display the password error blocking timeout value.
	queue			
		display	[a|f|u] [start#] [end#]	display queue by given status and range numbers
		ndisp	[qid]	display a queue by a given number
	quit			quit CI command mode
	reboot		[code]	reboot system code = 0 cold boot, = 1 immediately boot = 2 bootModule debug mode
	reslog			
		disp		display resources trace
		clear		clear resources trace
	rn			
		load	<entry no.>	load remote node information
		disp	<entry no.>(0:working buffer)	display remote node information
		nat	<none|sua|full_feature>	config remote node nat
		nailup	<no|yes>	config remote node nailup
		mtu	<value>	set remote node mtu
		save	[entry no.]	save remote node information
	smt			not support in this product
	stdio		[second]	change terminal timeout value
	time		[hour [min [sec]]]	display/set system time
	timer			
		disp		display timer cell
	tos			
		display		display all runtime TOS
		listPerHost		display all host session count
		debug	[on|off]	turn on or off TOS debug message
		sessPerHost	<number>	configure session per host value
		tcprst	<session>	send TCP RST to both source and dest IP
		timeout		
			display	display all TOS timeout information
			icmp <idle timeout>	set idle timeout value
			igmp <idle timeout>	set idle timeout value
			tcpsyn <idle timeout>	set idle timeout value
			tcp <idle timeout>	set idle timeout value
			tcpfin <idle timeout>	set idle timeout value
			udp <idle timeout>	set idle timeout value
			gre <idle timeout>	set idle timeout value
			esp <idle timeout>	set idle timeout value
			ah <idle timeout>	set idle timeout value
			other <idle timeout>	set idle timeout value
	trcdisp	parse, brief, disp		monitor packets

	trclog			
		switch	[on|off]	set system trace log
		online	[on|off]	set on/off trace log online
		level	[level]	set trace level of trace log #:1-10
		type	<bitmap>	set trace type of trace log
		disp		display trace log
		clear		clear trace
		call		display call event
		encapmask	[mask]	set/display tracelog encapsulation mask
	trcpacket			
		create	<entry> <size>	create packet trace buffer
		destroy		packet trace related commands
		channel	<name> [none|incoming|outgoing|bothway]	<channel name>=enet0,sdsl00, fr0 set packet trace direction for a given channel
		string		enable smt trace log
		switch	[on|off]	turn on/off the packet trace
		disp		display packet trace
		udp		send packet trace to other system
			switch [on|off]	set tracepacket upd switch
			addr <addr>	send trace packet to remote udp address
			port <port>	set tracepacket udp port
		parse	[[start_idx], end_idx]	parse packet content
		brief		display packet content briefly
	syslog			
		server	[destIP]	set syslog server IP address
		facility	<FacilityNo>	set syslog facility
		type	[type]	set/display syslog type flag
		mode	[on|off]	set syslog mode
	version			display RAS code and driver version
	view		<filename>	view a text file
	wdog			
		switch	[on|off]	set on/off wdog
		cnt	[value]	display watchdog counts value: 0-34463
		dead		let watch dog take place using while loop
	romreset			restore default romfile
	mrd			
		atwe	<mac> [country code] [debug flag] [featurebit]	configure mac, country code, debug flag, featurebit in the boot module
		atse		generate the engeneering debug flag password seed
		aten	<password>	enter the engeneering debug flag password
		atfl	<0:1>	set engeneering debug flag
		atsh		show mrd setting
	server			
		access	<telnet|ftp|web|icmp|snmp|dns> <value>	set server access type
		load		load server information
		disp		display server information
		port	<telnet|ftp|web|snmp> <port>	set server port

		save		save server information
		secureip	<telnet|ftp|web|icmp|snmp|dns> <ip>	set server secure ip addr
		certificate	<https|ssh> [certificate name]	set server certificate
		auth_client	<https> [on|off]	specifies whether the server authenticates the client
	fwnotify			
		load		load fwnotify entry from spt
		save		save fwnotify entry to spt
		url	<url>	set fwnotify url
		days	<days>	set fwnotify days
		active	<flag>	turn on/off fwnotify flag
		disp		display firmware notify information
		check		check firmware notify event
		debug	<flag>	turn on/off firmware notify debug flag
	spt			
		dump		dump spt raw data
			root	dump spt root data
			rn	dump spt remote node data
			user	dump spt user data
			slot	dump spt slot data
		set	<offset> <len> <value...>	set spt value in memory address
		save		save spt data
		size		display spt record size
		clear		clear spt data
	cmgr			
		trace		
			disp <ch-name>	show the connection trace of this channel
			clear <ch-name>	clear the connection trace of this channel
		data	<ch-name>	show channel connection related data
		cnt	<ch-name>	show channel connection related counter
	socket			display system socket information
	filter			
		clear		clear filter statistic counter
		disp		display filter statistic counters
		sw	[on|off]	set filter status switch
		rule	<iface>	display iface filter flag
		set	<set>	display filter rule
		addNetBios		add netbios filter
		removeNetBios		remove netbios filter
		netbios		
			disp	display netbios filter status
			config <0:Between LAN and WAN, 1: Between LAN and DMZ, 2: Between WAN and DMZ, 3:IPSec passthrough, 4:Trigger Dial> <on|off>	config netbios filter
		blockbc	[on|off]	set/display broadcast filter mode
	roadrunner			

		debug	<level>	enable/disable roadrunner service 0: diable <default> 1: enable
		display	<iface name>	display roadrunner information iface-name: enif0, wanif0
		restart	<iface name>	restart roadrunner
		logout	<iface name>	logout roadrunner
		set	<iface name>	set roadrunner
	ddns			
		debug	<level>	enable/disable ddns service
		display	<iface name>	display ddns information
		restart	<iface name>	restart ddns
		logout	<iface name>	logout ddns
	cpu			
		display		display CPU utilization
	upnp			
		active	[0:no/1:yes]	Activate or deactivate the saved upnp settings
		config	[0:deny/1:permit]	Allow users to make configuration changes. through UPnP
		display		display upnp information
		firewall	[0:deny/1:pass]	Allow UPnP to pass through Firewall.
		load		save upnp information
		reserve	[0:no/1:yes]	Reserve UPnP NAT rules in flash after system bootup.
		save		save upnp information
	mwan			
		load		Load the multiple wan common data to the memory
		mode	<0:Active/Passive|1:Active/ Active>	Change the Multiple WAN operation mode.
		save		Save the configuration
		Disp		Display the data

Exit Command Home

Command				Description
exit				exit smt menu

Device Related Command Home

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

Ethernet Related Command Home

Command				Description
ether				
	config			display LAN configuration information

	driver			
		cnt		
			disp <name>	display ether driver counters
			clear <name>	clear ether driver counters
		iface	<ch_name> <num>	send driver iface
		ioctl	<ch_name>	Useless in this stage.
		mac	<ch_name> <mac_addr>	Set LAN Mac address
		reg	<ch_name>	display LAN hardware related registers
		rxmod	<ch_name> <mode>	set LAN receive mode. mode: 1: turn off receiving 2: receive only packets of this interface 3: mode 2+ broadcast 5: mode 2 + multicast 6: all packets
		status	<ch_name>	see LAN status
		init	<ch_name>	initialize LAN
	version			see ethernet device type
	pkttest			
		disp		
			packet <level>	set ether test packet display level
			event <ch> [on|off]	turn on/off ether test event display
		sap	[ch_name]	send sap packet
		arp	<ch_name> <ip-addr>	send arp packet to ip-addr
	test		<ch_id> <test_id> [arg3] [arg4]	do LAN test
	ipmul		<num>	only receive ip multicast and broadcast packet
	pncconfig		<ch_name>	do pnc config
	mac		<src_ch> <dest_ch> <ipaddr>	fake mac address
	debug			
		disp	<ch_name>	display ethernet debug infomation
		reset	<ch_name>	reset ethernet debug state
		create	<ch_name> <num>	create ethernet debug state
		destory	<ch_name>	destory ethernet debug state
		level	<ch_name> <level>	set the ethernet debug level level 0: disable debug log level 1:enable debug log (default)
	edit			
		load	<ether no.>	load ether data from spt
		mtu	<value>	set ether data mtu
		speed	<speed>	set ether data speed
		save		save ether data to spt
	dynamicPort			
		dump		display the relation between physical port and channel.
		set	<port> <type>	set physical port belongs to which channel.
		spt		display channel setting stored in SPT.

POE Related Command Home

Command				Description
poe				
	debug		[on|off]	switch poe debug
	retry			
		count	[count]	set/display poe retry count
		interval	[interval]	set/display poe retry interval
	status		[ch_name]	see poe status

	master			
		promiscuous	[on|off]	provide pppoe server list to client
		easy	[on|off]	response for no service name request
	service			
		add	<service-name>	add poe service
		show		show poe service
	dial		<node>	dial a remote node
	drop		<node>	drop a pppoe call
	channel			
		enable	<channel>	enable a channel to carry pppoe traffic
		disable	<channel>	disable a pppoe channel
		show		show pppoe channel
	padt		[limit]	set/display pppoe PADT limit
	inout		<node_name>	set call direction to both
	ippool		[ip] [cnt]	set/display pppoe ippool information
	ether		[rfc|3com]	set /display pppoe ether type
	proxy	disp		Display PPPoE proxy client session table
		active	[on | off]	Turn on / off PPPoE proxy function
		debug	[on | off]	Turn on / off PPPoE proxy debug function
		time	<interval>	Set the time out interval, it's a count. Actual time is count * 5 seconds.
		init		Initialize PPPoE proxy client session table
		flush		Clear PPPoE proxy client session table

PPTP Related Command Home

Command				Description
pptp				
	debug		[on|off]	switch pptp debug flag
	dial		<rn-name>	dial a remote node
	drop		<rn-name>	drop a remote node call
	tunnel		<tunnel id>	display pptp tunnel information

AUX Related Command Home

Command				Description
aux				
	atring		<device name>	Command the AT command to the device.
	clearstat		<device name>	reset channel statistics
	cnt			
		disp	<device name>	display aux counter information
		clear	<device name>	clear aux counter information
	cond			
		disp	<device name>	display aux condition information
		clear	<device name>	clear aux condition information
	config			display aux config, board, line, channel information
	data			
	drop		<device name>	disconnect
	event			
		disp		aux event trace display
		clear		aux event trace clear
	init		<device name>	initialize aux channel
	mstatus		<device name>	display modem last call status

	mtype		<device name>	display modem type
	netstat		<device name>	prints upper layer packet information
	rate		<device name>	show tx rx rate
	redirect		<device name>	invalid
	ringbuf			
		cmd		
			clear <device name>	clear ringbuffer
			disp <device name>	display ringbuffer
		data		
			clear	clear command ringbuffer
			disp <start> <len>	display command ringbuffer
	signal		<device name>	show aux signal
	speed		<device name> <type> [value]	display/set aux speed

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
			logone <yes|no>		Switch on/off for one packet that create just one log message.
			rule <rule#>	permit <forward|block>	Edit whether a packet is dropped or allowed when it matches this rule
				active <yes|no>	Edit whether a rule is enabled or not
				protocol <0~255>	Edit the protocol number for a rule. 1=ICMP, 6=TCP, 17=UDP...
				log <none|match|not-match|both>	Sending a log for a rule when the packet none|matches|not match|both the rule
				alert <yes|no>	Activate or deactivate the notification when a DoS attack occurs or there is a violation of any alert settings. In case of such instances, the function will send an email to the SMTP destination address and log an alert.
				srcaddr-single <ip address>	Select and edit a source address of a packet which complies to this rule
				srcaddr-subnet <ip address> <subnet mask>	Select and edit a source address and subnet mask if a packet which complies to this rule.
				srcaddr-range <start ip address> <end ip address>	Select and edit a source address range of a packet which complies to this rule.
				destaddr-single <ip address>	Select and edit a destination address of a packet which complies to this rule

				destaddr-subnet <ip address> <subnet mask>	Select and edit a destination address and subnet mask if a packet which complies to this rule.
				destaddr-range <start ip address> <end ip address>	Select and edit a destination address range of a packet which complies to this rule.
				tcp destport-single <port#>	Select and edit the destination port of a packet which comply to this rule. For non-consecutive port numbers, the user may repeat this command line to enter the multiple port numbers.
				tcp destport-range <start port#> <end port#>	Select and edit a destination port range of a packet which comply to this rule.
				udp destport-single <port#>	Select and edit the destination port of a packet which comply to this rule. For non-consecutive port numbers, users may repeat this command line to enter the multiple port numbers.
				udp destport-range <start port#> <end port#>	Select and edit a destination port range of a packet which comply to this rule.
				desport-custom <desired custom port name>	Type in the desired custom port name
delete	firewall	e-mail			Remove all email alert settings
		attack			Reset all alert settings to defaults
		set <set#>			Remove a specified set from the firewall configuration
		set <set#>	rule <rule#>		Remove a specified rule in a set from the firewall configuration
insert	firewall	e-mail			Insert email alert settings
		attack			Insert attack alert settings
		set <set#>			Insert a specified rule set to the firewall configuration
		set <set#>	rule <rule#>		Insert a specified rule in a set to the firewall configuration
cli					Display the choices of command list.
debug	<1|0>				Turn on|off trace for firewall debug information.

IP Related Command Home

Command				Description
ip				
	address		[addr]	display host ip address
	alias		<iface>	alias iface
	aliasdis		<0|1>	disable alias
	arp			
		status	<iface>	display ip arp status
		add	<hostid> ether <ether addr>	add arp information
		resolve	<hostid>	resolve ip-addr
		replydif	[<0:No|1:yes>]	reply different inteface ip-addr's arp request
		drop	<hostid> [hardware]	drop arp
		flush		flush arp table
		publish		add proxy arp
		period	< value: 30~3000>	Set arp period.
		attpret	<on|off>	Switch receive APR from the different network or not.
		force	<on|off>	Switch the time out function of the APR.
	dhcp		<iface>	
		client		

			release	release DHCP client IP
			renew	renew DHCP client IP
		mode	<server|relay|none|client>	set dhcp mode
		relay	server <serverIP>	set dicp relay server ip-addr
		reset		reset dhcp table
		server		
			probecount <num>	set dhcp probe count
			dnsserver <IP1> [IP2] [IP3]	set dns server ip-addr
			winsserver <winsIP1> [<winsIP2>]	set wins server ip-addr
			gateway <gatewayIP>	set gateway
			hostname <hostname>	set hostname
			initialize	fills in DHCP parameters and initializes (for PWC purposes)
			leasetime <period>	set dhcp leasetime
			netmask <netmask>	set dhcp netmask
			pool <startIP> <numIP>	set dhcp ip pool
			renewaltime <period>	set dhcp renew time
			rebindtime <period>	set dhcp rebind time
			reset	reset dhcp table
			server <serverIP>	set dhcp server ip for relay
			dnsorder [router|isp]	set dhcp dns order
			release <entry num>	release specific entry of the dhcp server pool
		status	[option]	show dhcp status
		static		
			Delete <num>|all	delete static dhcp mac table
			display	display static dhcp mac table
			update <num> <mac> <ip>	update static dhcp mac table
	dns			
		query		
			address <ipaddr> [timeout]	resolve ip-addr to name
			Debug <num>	enable dns debug value
			Name <hostname> [timeout]	resolve name to multiple IP addresses
			Status	display dns query status
			Table	display dns query table
		server	<primary> [secondary] [third]	set dns server
		stats		
			Clear	clear dns statistics
			Disp	display dns statistics
		table		display dns table
		default	<ip>	Set default DNS server
		system		
			display	display dns system information
			edita <record idx> <FQDN> <isp group idx>	edit dns A record
			editns <record idx> <*|domain name> <0:from ISP|1:user defined(public)|2: user defined(private)> <isp group idx|dns server ip>	edit dns NS record
			inserta <before record idx|-1:new> <FQDN> <isp group idx>	insert dns A record
			insertns <before record idx|-1:new> <*|domain name> <0:from ISP|1:user defined(public)|2: user	insert dns NS record

			defined(private)> <isp group idx|dns server ip>	
			movea <record idx> <record idx>	move dns A record
			movens <record idx> <record idx>	move dns NS record
			dela <record idx>	delete DNS A record
			delns <record idx>	delete DNS NS record
		system cache		
			disp <0:none|1:name|2:type|3:IP|4:refCnt| 5:ttl> [0:increase|1:decrease]	display DNS cache table
			negaperiod <second(60 ~ 3600)>	set negative cache period
			negative <0: disable|1: enable>	enable/disable dns negative cache
			positive <0: disable|1: enable>	enable/disable dns positive cache
			ttl <second(60 ~ 3600)>	set positive cache maximum ttl
	Httpd			
		debug	[on|off]	set http debug flag
	icmp			
		echo	[on|off]	set icmp echo response flag
		data	<option>	select general data type
			cmd [on|off]	check icmp echo reply command data
			rsp [on|off]	check icmp response
			indication [i|r|l|p]	set icmp indication
		status		display icmp statistic counter
		trace	[on|off]	turn on/off trace for debugging
		discovery	<iface> [on|off]	set icmp router discovery flag
	ifconfig		[iface] [ipaddr] [broadcast <addr> |mtu <value>|dynamic]	configure network interface
	ping		<hostid>	ping remote host
	pong		<hostid> [<size> <time-interval>]	pong remote host
	route			
		status	[if]	display routing table
		add	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add route
		addiface	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add an entry to the routing table to iface
		addprivate	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add private route
		drop	<host addr> [/<bits>]	drop a route
		flush		flush route table
		lookup	<addr>	find a route to the destination
		errcnt		
			disp	display routing statistic counters
			clear	clear routing statistic counters
	smtp			
		server	[addr]	set smtp server
		destmail	[addr]	set destination mail addr
		srcmail	[addr]	set source mail addr
		sendmail		send mail
		addrlist		list smtp server, dest, return addr
		addrreset		reset smtp server, dest, return addr
	status			display ip statistic counters
	stroute			
		display	[rule # | buf]	display rule index or detail message in rule.
		load	<rule #>	load static route rule in buffer

		save		save rule from buffer to spt.
		config		
			name <site name>	set name for static route.
			destination <dest addr>[/<bits>] <gateway> [<metric>]	set static route destination address and gateway.
			mask <IP subnet mask>	set static route subnet mask.
			gateway <IP address>	set static route gateway address.
			metric <metric #>	set static route metric number.
			private <yes|no>	set private mode.
			active <yes|no>	set static route rule enable or disable.
	adjTcp		<iface> [<mss>]	adjust the TCP mss of iface
	adjmss		[mss]	adjust all system TCP mss of iface
	udp			
		status		display udp status
	rip			
		accept	<gateway>	drop an entry from the RIP refuse list
		activate		enable rip
		merge	[on|off]	set RIP merge flag
		refuse	<gateway>	add an entry to the rip refuse list
		request	<addr> [port]	send rip request to some address and port
		reverse	[on|off]	RIP Poisoned Reverse
		status		display rip statistic counters
		trace		enable debug rip trace
		mode		
			<iface> in [mode]	set rip in mode
			<iface> out [mode]	set rip out mode
		dialin_user	[show|in|out|both|none]	show dialin user rip direction
	sidepath			
		clear		clear side path
		disp		display side path
		set	<iface> <gateway>	set side path
	tcp			
		ceiling	[value]	TCP maximum round trip time
		floor	[value]	TCP minimum rtt
		irtt	[value]	TCP default init rtt
		kick	<tcb>	kick tcb
		limit	[value]	set tcp output window limit
		mss	[value]	TCP input MSS
		reset	<tcb>	reset tcb
		rtt	<tcb> <value>	set round trip time for tcb
		status	[tcb] [<interval>]	display TCP statistic counters
		syndata	[on|off]	TCP syndata piggyback
		trace	[on|off]	turn on/off trace for debugging
		window	[tcb]	TCP input window size
	samenet		<iface1> [<iface2>]	display the ifaces that in the same net
	uninet		<iface>	set the iface to uninet
	telnet		<host> [port]	execute telnet clinet command
	tftp			
		support		pritn if tfpt is support
		stats		display tftp status
	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

	anitprobe		<0|1> 1:yes 0:no	set ip anti-probe flag
	forceproxy		<display|set> [on|off] [servicePort] [proxyIp] [proxyport]	enable TCP forceproxy
	ave			anti-virus enforce
	urlfilter			
		enable		enable/disable url filter function
		reginfo		
			display	display urlfilter registration information
			name	set urlfilter registration name
			eMail <size>	set urlfilter registration email addr
			country <size>	set urlfilter registration country
			clearAll	clear urlfilter register information
		category		
			display	display urlfilter category
			webFeature [block|nonblock] [activex|java|cookei|webproxy]	block or unblock webfeature
			logAndBlock [log|logAndBlock]	set log only or log and block
			blockCategory [block|nonblock] [all|type(1-14)]	block or unblock type
			timeOfDay [always|hh:mm] [hh:mm]	set block time
			clearAll	clear all category information
		listUpdate		
			display	display listupdate status
			actionFlags [yes|no]	set listupdate or not
			scheduleFlag [pending]	set schedule flag
			dayFlag [pending]	set day flag
			time [pending]	set time
			clearAll	clear all listupdate information
		exemptZone		
			display	display exemptzone information
			actionFlags [type(1-3)][enable|disable]	set action flags
			add [ip1] [ip2]	add exempt range
			delete [ip1] [ip2]	delete exempt range
			reset	clear exemptzone information
		customize		
			display	display customize action flags
			actionFlags [filterList|disableAllExceptTrusted| unblockRWFToTrusted|keywordBlock|fullPath|caseInsensitive|fileName][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
			reset	clear all information
		logDisplay		display cyber log
		ftplist		update cyber list data
		listServerIP	<ipaddr>	set list server ip
		listServerName	<name>	set list server name
		general		
			enable	enable|disable url filter function
			display	display content filer's general setting

			webFeature	[block|nonblock] [activex|java|cookei|webproxy]
			timeOfDay[always|hh:mm] [hh:mm]	set block time
			exemptZone display	display exemptzone information
			exemptZone actionFlags [type(1-3)][enable|disable]	set action flags
			exemptZone add [ip1] [ip2]	add exempt range
			exemptZone delete [ip1] [ip2]	delete exempt range
			exemptZone reset	clear exemptzone information
			reset	reset content filter's general setting
		webControl		
			enable	enable cbr_filter
			display	display cbr_filter's setting
			logAndBlock [log|block|both]	set log or block on matched web site
			category	set blocked categories
			serverList display	display current cbr_filter servers
			serverList refresh	refresh cbr_filter servers
			queryURL [url][Server|localCache]	query url need to block or forward according the database on server or local cache
			cache display	display the local cache entries
			cache delete [entrynum|All]	delete the local cache entries
			cache timeout [hour]	Set timeout value of cache entries
			blockonerror [log|block][on|off]	choose log or block when server is unavailable
			unratedwebsite[block|log][on|off]	hoose log or block for unrated web site
			waitingTime [sec]	set waiting time for server
			reginfo display	display the license key with cerberian
			reginfo	No used
			zssw	change the zssw's URL
	tredir			
		failcount	<count>	set tredir failcount
		partner	<ipaddr>	set tredir partner
		target	<ipaddr>	set tredir target
		timeout	<timeout>	set tredir timeout
		checktime	<period>	set tredir checktime
		active	<on|off>	set tredir active
		save		save tredir information
		disp		display tredir information
		debug	<value>	set tredir debug value
	rpt			
		start		start report
		stop		stop report
		url	[num]	top url hit list
		ip	[num]	top ip addr list
		srv	[num]	top service port list
	dropIcmp		[0 | 1]	to drop ICMP fragment packets
	nat			
		period	[period]	set nat timer period
		port	[port]	set nat starting external port number
		checkport		verify all server tables are valid
		timeout		
			gre [timeout]	set nat gre timeout value
			iamt [timeout]	set nat iamt timeout value
			generic [timeout]	set nat generic timeout value
			reset [timeout]	set nat reset timeout value

			tcp [timeout]	set nat tcp timeout value
			tcpother [timeout]	set nat tcp other timeout value
			udp [port] <value>	set nat udp timeout value of specific port
		update		create nat system information from spSysParam
		iamt	<iface>	display nat iamt information
		iface	<iface>	show nat status of an interface
		lookup	<rule set>	display nat lookup rule
		new-lookup	<rule set>	display new nat lookup rule
		loopback	[on|off]	turn on/off nat loopback flag
		reset	<iface>	reset nat table of an iface
		server		
			disp	display nat server table
			load <set id>	load nat server information from ROM
			save	save nat server information to ROM
			clear <set id>	clear nat server information
			edit active <yes|no>	set nat server edit active flag
			edit svrport <start port> [end port]	set nat server server port
			edit intport <start port> [end port]	set nat server forward port
			edit remotehost <start ip> [end ip]	set nat server remote host ip
			edit leasetime [time]	set nat server lease time
			edit rulename [name]	set nat server rule name
			edit forwardip [ip]	set nat server server ip
			edit protocol [protocol id]	set nat server protocol
			edit clear	clear one rule in the set
		service		
			irc [on|off]	turn on/off irc flag
			xboxlive [on|off]	turn on/off xboxlive flag
		resetport		reset all nat server table entries
		incikeport	<iface>[on|off]	turn on/off increase ike port flag
		session	[session per host]	set nat session per host value
		deleteslot	<iface> <slot>	delete specific slot of iface
		debug		
			natTraversal [on|off]	set NAT traversal debug flag
			hash [on|off]	set NAT hash table debug flag
			session [on|off]	set NAT session debug flag
		hashtable	<enifX, X=0, 1, 2, …>	show the NAT hash table of enifX
	igmp			
		debug	[level]	set igmp debug level
		forwardall	[on|off]	turn on/off igmp forward to all interfaces flag
		querier	[on|off]	turn on/off igmp stop query flag
		iface		
			<iface> 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			

		clear		clear ip pr table counter information
		disp		display policy route set and rule information
		move		move specific policy route rule to another rule
		dispCnt		dump ip pr table counter information
		switch		turn on/off ip pr table counter flag

IPSec Related Command Home

Command				Description
ipsec				
	debug	<1|0>		turn on|off trace for IPsec debug information
	ipsec_log_disp			show IPSec log, same as menu 27.3
	route	dmz	<on|off>	After a packet is IPSec processed and will be sent to DMZ side, this switch is to control if this packet can be applied IPSec again.
				Remark: Only supported in ZyWALL100
		lan	<on|off>	After a packet is IPSec processed and will be sent to LAN side, this switch is to control if this packet can be applied IPSec again.
				Remark: Command available since 3.50(WA.3)
		wan	<on|off>	After a packet is IPSec processed and will be sent to WAN side, this switch is to control if this packet can be applied IPSec again.
				Remark: Command available since 3.50(WA.3)
	show_runtime	sa		display runtime phase 1 and phase 2 SA information
		spd		When a dynamic rule accepts a request and a tunnel is established, a runtime SPD is created according to peer local IP address. This command is to show these runtime SPD.
	switch	<on|off>		As long as there exists one active IPSec rule, all packets will run into IPSec process to check SPD. This switch is to control if a packet should do this. If it is turned on, even there exists active IPSec rules, packets will not run IPSec process.
	timer	chk_my_ip	<1~3600>	- Adjust timer to check if WAN IP in menu is changed
				- Interval is in seconds
				- Default is 10 seconds
				- 0 is not a valid value
		chk_conn.	<0~255>	- Adjust auto-timer to check if any IPsec connection has “only outbound traffic but no inbound traffic” for certain period. If yes, system will disconnect it.
				- Interval is in minutes
				- Default is 2 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
		chk_input	<0~255>	- Adjust input timer to check if any IPSec connection has no inbound traffic for a certain period. If yes, system will disconnect it.

				- Interval is in minutes
				- Default is 2 minuets
				- 0 means never timeout
				Remark: Command available since 3.50(WA.3)
	updatePeerIp			Force system to update IPSec rules which use domain name as the secure gateway IP right away.
				Remark: Command available since 3.50(WA.3)
	dial	<rule #>		Initiate IPSec rule <#> from ZyWALL box
				Remark: Command available since 3.50(WA.3)
	display	<rule #>		Display IPSec rule #
	remote	key	<string>	I add a secured remote access tunnel with pre-shared key. It is a dynamic rule with local: the route's WAN IP. The algorithms with it are fixed to phase1: DES+MD5, DH1 and SA lifetime 28800 seconds; phase2: DES+MD5, PFS off, no anti-replay and SA lifetime 28800 seconds. The length of pre-shared key is between 8 to 31 ASCII characters.
		switch	<on|off>	Activate or de-activate the secured remote access tunnel.
	keep_alive	<rule #>	<on|off>	Set ipsec keep_alive flag
	load	<rule #>		Load ipsec rule
	save			Save ipsec rules
	config	netbios	active <on|off>	Set netbios active flag
			group <group index1, group index2…>	Set netbios group
		name	<string>	Set rule name
		active	<Yes | No>	Set active or not
		keeyAlive	<Yes| No>	Set keep alive or not
		natTraversal	<Yes| No>	Enable NAT traversal or not.
		lcIdType	<0:IP | 1:DNS | 2:Email>	Set local ID type
		lcIdContent	<string>	Set local ID content
		myIpAddr	<IP address>	Set my IP address
		peerIdType	<0:IP | 1:DNS | 2:Email>	Set peer ID type
		peerIdContent	<string>	Set peer ID content
		secureGwAddr	<IP address | Domain name>	Set secure gateway address or domain name
		protocol	<1:ICMP | 6:TCP | 17:UDP>	Set protocol
		lcAddrType	<0:single | 1:range | 2:subnet>	Set local address type
		lcAddrStart	<IP>	Set local start address
		lcAddrEndMask	<IP>	Set local end address or mask
		lcPortStart	<port>	Set local start port
		lcPortEnd	<port>	Set local end port
		dnsServer	<IP>	Set DNS server for IPSec VPN
		rmAddrType	<0:single | 1:range | 2:subnet>	Set remote address type
		rmAddrStart	<IP>	Set remote start address

		rmAddrEndMask	<IP>	Set remote end address or mask
		rmPortStart	<port>	Set remote start port
		rmPortEnd	<port>	Set remote end port
		antiReplay	<Yes | No>	Set 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
			authMethod <0:PreSharedKey | 1:RSASignature	Set authentication method in phase 1 in IKE
			preShareKey <string>	Set pre shared key in phase 1 in IKE
			certFile <FILE>	Set certificate file if using RSA signature as authentication method.
			p1EncryAlgo <0:DES | 1:3DES>	Set encryption algorithm in phase 1 in IKE
			p1AuthAlgo <0:MD5 | 1:SHA1>	Set authentication algorithm in phase 1 in IKE
			p1SaLifeTime <seconds>	Set sa life time in phase 1 in IKE
			p1KeyGroup <0:DH1 | 1:DH2>	Set key group in phase 1 in IKE
			activeProtocol <0:AH | 1:ESP>	Set active protocol in phase 2 in IKE
			p2EncryAlgo <0:Null | 1:DES | 2:3DES>	Set encryption algorithm in phase 2 in IKE
			p2AuthAlgo <0:MD5 | 1:SHA1>	Set authentication algorithm in phase 2 in IKE
			p2SaLifeTime <seconds>	Set sa life time in phase 2 in IKE
			encap <0:Tunnel | 1:Transport>	set encapsulation in phase 2 in IKE
			pfs <0:None | 1:DH1 | 2:DH2>	set pfs in phase 2 in IKE
		manual	activeProtocol <0:AH | 1:ESP>	Set active protocol in manual
		manual ah	encap <0:Tunnel | 1:Transport>	Set encapsulation in ah in manual
			spi <decimal>	Set spi in ah in manual
			authAlgo <0:MD5 | 1:SHA1>	Set authentication algorithm in ah in manual
			authKey <string>	Set authentication key in ah in manual
		manual esp	encap <0:Tunnel | 1:Transport>	Set encapsulation in esp in manual
			spi <decimal>	Set spi in esp in manual
			encryAlgo <0:Null | 1:DES | 2:3DES>	Set encryption algorithm in esp in manual
			encryKey <string>	Set encryption key in esp in manual

			authAlgo <0:MD5 | 1:SHA1>	Set authentication algorithm in esp in manual
			authKey < string>	Set authentication key in esp in manual
	swSkipOverlapIp		<on|off>	- When a VPN rule with remote range overlaps with local range, the switch decides if a local to local packet should apply this rule. - Default value is “off” which means “no skip”.
	adjTcpMss		<off|auto|user defined value>	- After a tunnel is established, system will automatically adjust TCP MSS. - After all tunnels are drops, the MSS will adjust to the original value. - The default value is auto.

PPP Related Command Home

Command				Description
ppp				
	bod			
		remote	<iface>	show remote bod information
		reset		reset bod
		setremote	<iface>	set remote bod
		status	<wan_iface>	show wan port bod status
		clear	<wan_iface>	clear wan port bod data
		on		set bod flag on
		off		set bod flag off
		node	<node> <dir>	config the statistic method for remote node bod traffic data
		debug	[on|off]	show bod debug flag
		cnt		
			disp	show bod state
			clear	clear bod state
	ccp		[on|off]	set/display dial-in ccp switch
	lcp			
		acfc	[on|off]	set address/control field compression flag
		pfc	[on|off]	set protocol field compression flag
		mpin	[on|off]	set incoming call MP flag
		callback	[on|off]	set callback flag
		bacp	[on|off]	set bandwidth allocation control flag
		echo		
			retry <retry_count>	set/display retry count to send echo-request
			time <interval>	set/display time interval to send echo-request
	ipcp			
		close		close connection on ppp interface
		list	<iface>	show ipcp state
		open		open fsm link
		timeout	[value]	set timeout interval when waiting for response from remote peer
		try		
			configure [value]	set/display fsm try config
			failure [value]	set/display fsm try failure

			terminate [value]	set/display fsm try terminate
		compress	[on|off]	set compress flag
		slots	[slot_num]	set number of slots
		idcompress	[on|off]	set/display slot id compress
		address	[on|off]	set/display ip one address option
	mp			
		default		show link default flag
			rotate	set link default to rotate
			split	set link default to split
		split	[0|1]	set/display link split
		rotate	[0|1]	set/display link rotate
		sequence		set/display mp start sequence
	configure			
		ipcp		
			compress [on|off]	enable/disable compress
			slots [slot_num]	select number of slots
			idcompress [on|off]	enable/disable slot id compress
			address [on|off]	set/display ip one address option
		atcp		apple talk feature not supported anymore
		ccp		
			ascend [on|off]	set/display ascend stac flag
			history <count>	set/display stac history count
			check [argv]	set/display stac check mode
			reset <mode>	set/display stac reset mode
			pfc [on|off]	set/display pfc flag
			debug [on|off]	set/display ccp debug flag
	iface			
			<iface> ipcp	show the ipcp status of the given iface
			<iface> ipxcp	show the ipxcp status of the given iface
			<iface> atcp	
			<iface> ccp [reset|skip|flush]	show the ccp status of the given iface
			<iface> mp	show the mp status of the given iface
	show		<channel>	show the ppp channel status
	fsm			
		trace		
			break [num] [count] [flag]	set the fsm log break value
			clear	clear the fsm log data
			disp	display the fsm log data
			filter [mask] [protocol]	set the fsm log filter value
		tdata		
			filter [protocol1] [protocol2] …	set the fsm filter data
			disp	display the fsm data
			clear	clear the fsm data
		struc		dump fsm data structure
	delay		[inteval]	set the delay timer for sending first PPP packet after call answered

Bridge Related Command Home

Command				Description
bridge				
	mode		<1/0> (enable/disable)	turn on/off (1/0) LAN promiscious mode
	blt			related to bridge local table
		disp	<channel>	display blt data

		reset	<channel>	reset blt data
		traffic		display local LAN traffic table
		monitor	[on|off]	turn on/off traffice monotor. Default is off.
		time	<sec>	set blt re-init interval
	brt			related to bridge route table
		disp	[id]	display brt data
		reset	[id]	reset brt data
	cnt			related to bridge routing statistic table
		disp		display bridge route counter
		clear		clear bridge route counter
	iface			Related to “bridge mode” access interface
		active	<yes/no>	Active bridge mode iface or not
		address	[ip]	Remote access IP address
		dns1	[ip]	First DNS server
		dns2	[ip]	Second DNS server
		dns3	[ip]	Third DNS server
		mask	[network mask]	Network mask
		gateway	[gateway ip]	Network gateway
		display		Display whole interface information
	stat			related to bridge packet statistic table
		disp		display bridge route packet counter
		clear		clear bridge route packet counter
	disp			display bridge source table
	fcs		<BriFcsCtl>	set bridge fcs control flag

Bandwidth management Related Command Home

Command						Description
bm						
	interface	lan	enable	<bandwidth xxx>		Enable bandwidth management in LAN with bandwidth xx If the user doesn’t set the bandwidth, the default value is 100Mbps.
				<wrr|prr>		Select fairness-based(WRR) or priority-based(PRR) mecha 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 xx If the user doesn’t set the bandwidth, the default value is 100Mbps.
				<wrr|prr>		Select fairness-based(WRR) or priority-based(PRR) mecha 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 xx If the user doesn’t set the bandwidth, the default value is 100Mbps.
				<wrr|prr>		Select fairness-based(WRR) or priority-based(PRR) mecha 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 bps. If the user doesn’t set the bandwidth, the default value 100Mbps.
				<wrr|prr>		Select fairness-based(WRR) or priority-based(PRR) mecha 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 f users' information.
					<priority x>	Set the class' priority. The range is between 0 (the lowest) t highest). The default value is 3.
					<borrow on|off>	The class can borrow bandwidth from its parent class when 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 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) t highest). The priority is unchanged if the user doesn't set a value.
				<borrow on|off>		The class can borrow bandwidth from its parent class when borrow is set on, and vice versa. The borrow is unchanged i user doesn't set a new value.
			del #			Delete the class # and its filter and all its children class and filters in LAN.
		wan	add #	bandwidth xxx	<name xxx>	Add a class with bandwidth xxx bps in WAN. The name is users' information.
					<priority x>	Set the class' priority. The range is between 0 (the lowest) t highest). The default value is 3.
					<borrow on|off>	The class can borrow bandwidth from its parent class when 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 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) t highest). The priority is unchanged if the user doesn't set a value.
				<borrow on|off>		The class can borrow bandwidth from its parent class when borrow is set on, and vice versa. The borrow is unchanged i user doesn't set a new value.
			del #			Delete the class # and its filter and all its children class and filters in WAN.
		dmz	add #	bandwidth xxx	<name xxx>	Add a class with bandwidth xxx bps in DMZ. The name is users' information.
					<priority x>	Set the class' priority. The range is between 0 (the lowest) t highest). The default value is 3.
					<borrow on|off>	The class can borrow bandwidth from its parent class when 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 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) t highest). The priority is unchanged if the user doesn't set a value.
				<borrow on|off>		The class can borrow bandwidth from its parent class when borrow is set on, and vice versa. The borrow is unchanged i user doesn't set a new value.
			del #			Delete the class # and its filter and all its children class and filters in DMZ.
		wlan	add #	bandwidth xxx	<name xxx>	Add a class with bandwidth xxx bps in WLAN. The name i users' information.

					<priority x>	Set the class' priority. The range is between 0 (the lowest) t highest). The default value is 3.
					<borrow on|off>	The class can borrow bandwidth from its parent class when borrow is set on, and vice versa. The default value is off.
			mod #	<bandwidth xxx>		Modify the parameters of the class in WLAN. The bandwid 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) t highest). The priority is unchanged if the user doesn't set a value.
				<borrow on|off>		The class can borrow bandwidth from its parent class when borrow is set on, and vice versa. The borrow is unchanged i user doesn't set a new value.
			del #			Delete the class # and its filter and all its children class and 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 destinati address (netmask), destination port, source address (netmas source port and protocol. You may set the value as 0 if you 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 destinat address (netmask), destination port, source address (netmas source port and protocol. You may set the value as 0 if you 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 destinati address (netmask), destination port, source address (netmas source port and protocol. You may set the value as 0 if you 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 destin address (netmask), destination port, source address (netmas source port and protocol. You may set the value as 0 if you 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 secon you will set it off, and so on.
		wan	<#>			Monitor the bandwidth of class # in WAN. If the class is no specific, all the classes in WAN will be monitored. The first time you key the command will set it on; the secon you will set it off, and so on.
		dmz	<#>			Monitor the bandwidth of class # in DMZ. If the class is no specific, all the classes in DMZ will be monitored. The first time you key the command will set it on; the secon you will set it off, and so on.
		wlan	<#>			Monitor the bandwidth of class # in WLAN. If the class is r specific, all the classes in WLAN will be monitored. The first time you key the command will set it on; the secon you will set it off, and so on.
	config	save				Save the configuration.
		load				Load the configuration.
		clear				Clear the configuration.

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.
		dynamicrule			
		tcprst			
			rst		Set TCP reset sending on/off.
			rst113		Set TCP reset sending for port 113 on/off.
			display		Display TCP reset sending setting.
		dos			
			smtp		Set SMTP DoS defender on/off
			display		Display SMTP DoS defender setting.
			ignore		Set if firewall ignore DoS in lan/wan/dmz/wlan
		ignore			
			dos		Set if firewall ignore DoS in lan/wan/dmz/wlan
			triangle		Set if firewall ignore triangle route in lan/wan/dmz/wlan
		schedule			
			load [set # rule #]		Load firewall ACL schedule by rule.
			display		Display ACL schedule in buffer.
			save		Save buffer date and update runtime firewall ACL rule.
			week		
				monday [on/off]	Set schedule on or off by day – Monday.
				tuesday [on/off]	Set schedule on or off by day – Tuesday.

				wednesday [on/off]	Set schedule on or off by day – Wednesday.
				thursday [on/off]	Set schedule on or off by day – Thursday.
				friday [on/off]	Set schedule on or off by day – Friday.
				saturday [on/off]	Set schedule on or off by day – Saturday.
				sunday [on/off]	Set schedule on or off by day – Sunday.
				allweek [on/off]	Quick set schedule on or off by week.
			timeOfDay [always/hh:mm]		Set firewall ACL schedule block time of day.

Certificate Management (PKI) Command [Home]

Command				Description
certificates				
	my_cert			
		create		
			selfsigned <name> <subject> [key size]	Create a self-signed local host certificate. <name> specifies a descriptive name for the generated certificate. <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn;{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.
			request <name> <subject> [key size]	Create a certificate request and save it to the router for later manual enrollment. <name> specifies a descriptive name for the generated certification request. <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn;{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.
			scep_enroll <name> <CA addr> <CA cert> <auth key> <subject> [key size]	Create a certificate request and enroll for a certificate immediately online using SCEP protocol. <name> specifies a descriptive name for the enrolled certificate. <CA addr> specifies the CA server address. <CA cert> specifies the name of the CA certificate. <auth key> specifies the key used for user authentication. If the key contains spaces, please put it in quotes. To leave it blank, type "". <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn;{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.
			cmp_enroll <name> <CA addr> <CA cert> <auth key> <subject> [key size]	Create a certificate request and enroll for a certificate immediately online using CMP protocol. <name> specifies a descriptive name for the enrolled certificate. <CA addr> specifies the CA server address. <CA cert> specifies the name of the CA certificate. <auth key> specifies the id and key used for user authentication. The format is "id:key". To leave the id and key blank, type ":". <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn;{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.
		import [name]		Import the PEM-encoded certificate from stdin. [name] specifies the descriptive name (optional) as which the imported certificate is to be saved. For my certificate importation to be successful, a

				certification request corresponding to the imported certificate must already exist on ZyWALL. After the importation, the certification request will automatically be deleted. If a descriptive name is not specified for the imported certificate, the certificate will adopt the descriptive name of the certification request.
		export <name>		Export the PEM-encoded certificate to stdout for user to copy and paste. <name> specifies the name of the certificate to be exported.
		view <name>		View the information of the specified local host certificate. <name> specifies the name of the certificate to be viewed.
		verify <name> [timeout]		Verify the certification path of the specified local host certificate. <name> specifies the name of the certificate to be verified. [timeout] specifies the timeout value in seconds (optional). The default timeout value is 20 seconds.
		delete <name>		Delete the specified local host certificate. <name> specifies the name of the certificate to be deleted.
		list		List all my certificate names and basic information.
		rename <old name> <new name>		Rename the specified my certificate. <old name> specifies the name of the certificate to be renamed. <new name> specifies the new name as which the certificate is to be saved.
		def_selfsigned [name]		Set the specified self-signed certificate as the default self-signed certificate. [name] specifies the name of the certificate to be set as the default self-signed certificate. If [name] is not specified, the name of the current self-signed certificate is displayed.
	ca_trusted			
		import <name>		Import the PEM-encoded certificate from stdin. <name> specifies the name as which the imported CA certificate is to be saved.
		export <name>		Export the PEM-encoded certificate to stdout for user to copy and paste. <name> specifies the name of the certificate to be exported.
		view <name>		View the information of the specified trusted CA certificate. <name> specifies the name of the certificate to be viewed.
		verify <name> [timeout]		Verify the certification path of the specified trusted CA certificate. <name> specifies the name of the certificate to be verified. [timeout] specifies the timeout value in seconds (optional). The default timeout value is 20 seconds.
		delete <name>		Delete the specified trusted CA certificate. <name> specifies the name of the certificate to be deleted.
		list		List all trusted CA certificate names and basic information.
		rename <old name> <new name>		Rename the specified trusted CA certificate. <old name> specifies the name of the certificate to be renamed. <new name> specifies the new name as which the certificate is to be saved.
		crl_issuer <name> [on|off]		Specify whether or not the specified CA issues CRL. <name> specifies the name of the CA certificate. [on|off] specifies whether or not the CA issues CRL. If [on|off] is not specified, the current crl_issuer status of the CA.
	remote_trusted			
		import <name>		Import the PEM-encoded certificate from stdin. <name> specifies the name as which the imported remote host certificate is to be saved.
		export <name>		Export the PEM-encoded certificate to stdout for user to copy and paste. <name> specifies the name of the certificate to be exported.
		view <name>		View the information of the specified trusted remote host certificate. <name> specifies the name of the certificate to be viewed.

		verify <name> [timeout]		Verify the certification path of the specified trusted remote host certificate. <name> specifies the name of the certificate to be verified. [timeout] specifies the timeout value in seconds (optional). The default timeout value is 20 seconds.
		delete <name>		Delete the specified trusted remote host certificate. <name> specifies the name of the certificate to be deleted.
		list		List all trusted remote host certificate names and basic information.
		rename <old name> <new name>		Rename the specified trusted remote host certificate. <old name> specifies the name of the certificate to be renamed. <new name> specifies the new name as which the certificate is to be saved.
	dir_service			
		add <name> <addr[:port]> [login:pswd]		Add a new directory service. <name> specifies a descriptive name as which the added directory server is to be saved. <addr[:port]> specifies the server address (required) and port (optional). The format is "server-address[:port]". The default port is 389. [login:pswd] specifies the login name and password, if required. The format is "[login:password]".
		delete <name>		Delete the specified directory service. <name> specifies the name of the directory server to be deleted.
		view <name>		View the specified directory service. <name> specifies the name of the directory server to be viewed.
		edit <name> <addr[:port]> [login:pswd]		Edit the specified directory service. <name> specifies the name of the directory server to be edited. <addr[:port]> specifies the server address (required) and port (optional). The format is "server-address[:port]". The default port is 389. [login:pswd] specifies the login name and password, if required. The format is "[login:password]".
		list		List all directory service names and basic information.
		rename <old name> <new name>		Rename the specified directory service. <old name> specifies the name of the directory server to be renamed. <new name> specifies the new name as which the directory server is to be saved.
	cert_manager			
		reinit		Reinitialize the certificate manager.