ZyXEL

Firmware Release Note

ZyWALL 35

Release 3.64(WZ.3)

Date: **Jun. 21, 2005**
Author: **Tim Tseng**
Project Leader: **Tim Tseng**

ZyXEL ZyWALL 35 Standard Version release 3.64(WZ.3) Release Note

Date: Jun. 21, 2005

Supported Platforms:

ZyXEL ZyWALL 35

Versions:

ZyNOS F/W Version : V3.64(WZ.3) | 06/21/2005
BootBase : V1.08 | 01/30/2005
Vantage Agent Version : 1.0.0

Note:

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 and 802.1X 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 roles for LAN/DMZ ports setting are: port 1 to 4 = LAN ports.
10. If the encapsulation type of WAN1 and WAN2 are both PPTP, The PPTP IP settings (My IP Addr, My IP Mask and Server IP Addr) on WAN1 and WAN2 must be different subnet.
11. For users using the default ROMFILE in former release, please remove “ip nat session 1300” from autoexec.net by CI command “sys edit autoexec.net”.
12. The first two entries for static route are reserved for creating WAN1 and WAN2

default routes and are READ-ONLY.

13. The default max NAT session number per host is changed to 10000.
14. 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.
15. Under Bridge Mode, all LAN ports will behave as a hub, and all DMZ ports will also behave as another hub.
16. The DMZ TxPkts counter increment at about 1 pkt/min even without any Ethernet cables ever connected. This is because RIP on DMZ port is turned on by default.
17. In previous 3.64 firmware, the VID value of DPD is not correct. VID change will cause current version doesn't work with the wrong value. Please be sure to connect with devices which has updated VID, or the DPD may not work correctly.
18. In previous 3.64 firmware, the VID value of DPD is not correct. VID change will cause current version doesn't work with the wrong value. Please be sure to connect with devices which has updated VID, or the DPD may not work correctly.

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. If the metric of dial-backup is smaller (has higher priority) than the metric of Traffic-Redirect, Traffic-Redirect can't be triggered any more.
3. Sometimes on screen the "Local Area Connection" icon for UPnP disappears. The icon shows again when restarting PC.
4. 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..
5. On the SUA/ Address Mapping Edit page, the user can give the same local IP and global IP.
6. 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).
7. Bandwidth Management doesn't work on wireless LAN.
8. Sometimes, modify an active IPSec rule (the VPN tunnel was created) will crash the system, if this tunnel is going the re-key process.
9. Symptom: LAN host can ping Internet while LAN host change cable from LAN port to DMZ port.
   Condition:
   (1) Host connect to LAN port and get DHCP address from router.
   (2) Unplug LAN host cable and plug it into DMZ port.
   (3) The host can still ping Internet using LAN DHCP address
   (4) The scenario will continue about 30secs.

10. At SMT24.1, the collisions for WAN2, LAN and DMZ port are not really counted.
11. Can't block ActiveX in some case. (Windows will cache it in C:\WINNT\Downloaded Program Files\)
12. 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.
13. 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.
14. G-100 WLAN card, does not support the fragment size below 800.
15. Bandwidth management H.323 service does not support Netmeeting H.323 application.
16. Device sometimes crashes when use wireless for a long time.
17. Router sometimes crashes after running 35 VPN tunnels for a long time.
18. Some limitations on Firewall CLI configuration, (1) User can not delete specific address or custom port entry from a rule. (2) CLI doesn't support Modify and Move for rules implemented in eWC. (3) eWC can not display firewall rule field correctly if rule is added by CI command and its type is port/address range.
19. In eWC->Statistics, Tx data for Dial Backup is not correct.
20. SMT shows weird message when enabling WLAN security. At the same time, if WLAN is dead, we need to restart WLAN.
21. Bandwidth Management works abnormally when using Fairness/Priority scheduler and "borrow" is enabled on all classes.
22. 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.
23. The gateway domain name update timer for VPN sometimes can not work correctly. (GUI/VPN/Global Setting)

Features:

Modifications in V 3.64(WZ.3) | 06/21/2005

Modify for formal release

Modifications in V 3.64(WZ.3)b2 | 06/16/2005

1. [BUG FIX] 050613567
Symptom: There is no conflict check between VPN dynamic rule and static rule on local ip address.
Condition:
(1) Goto CUI VPN page, add one dynmaic IKE rule and static IKE rule.
(2) Add one policy with local ip set as 192.168.1.0/24 into dynamic rule.
(3) Add one policy with local ip set as 192.168.1.1/32 into static rule.
(4) The static rule's policy can be saved without conflict error.

Modifications in V 3.64(WZ.3)b1 | 06/15/2005

2. [BUG FIX]
Symptom: IPSec input idle timer does not work correctly.

Condition:
Topology:
PC1-ZWA--Intranet--ZWB-PC2
Add normal VPN rule in both side.
(1) In ZWB, set "Input Idle Timeout" as "30" seconds.
(2) Dial the tunnel up, there is no traffic in the tunnel.
(3) In ZWB, SMT 24.8, type "ipsec sho sa", the "input idle count" in "INBOUND" will be decreasing, it works correctly.
(4) Now, In PC1, ping PC2 from PC1 with one packet then stop the traffic in the tunnel.
(5) In ZWB, SMT 24.8, type "ipsec sho sa", the "input idle count" in "INBOUND" stay unchanged.
(6) The input idle timeout mechanism will not work anymore.

3. [BUG FIX]
   Symptom: Output idle timer doesn't work correctly.
   Condition:
   PC1--(L)ZW-A(W)--Intranet--(W)ZW-B(L)--PC2
   (1) ZW-A and ZW-B had established VPN tunnel.
   (2) Output idle timer=120 secs, input idle timer=30 secs.
   (3) Disconnect the WAN link between ZW-A and ZW-B, make a ICMP echo request to PC2 from PC1.
   (4) ZW-A doesn't send out "are u there" packets to peer gateway after 120 seconds.
4. [BUG FIX]
   Symptom: IPSec check rule conflict on IP 0.0.0.0 is incorrect.
   Condition:
   (1) Restore default romfile.
   (2) Configure the two IPSec rules shown as follow:
   Rule A: local:0.0.0.0 remote:192.168.3.33
   Rule B: local:192.168.70.94 remote:192.168.3.33
   these two IPSec rules conflict and we should add check for it.
5. [BUG FIX] 050613567
   Symptom: There is no conflict check between VPN dynamic rule and static rule on local ip address.
   Condition:
   (1) Goto CUI VPN page, add one dynmaic IKE rule and static IKE rule.
   (2) Add one policy with local ip set as 192.168.1.0/24 into dynamic rule.
   (3) Add one policy with local ip set as 192.168.1.1/32 into static rule.
   (4) The static rule's policy can be saved without conflict error.
6. [BUG FIX]
   Symptom: DNS Address Record must case-insensitive
   Condition:
   Topology:
   PC – ZW35 – network --- www.hinet.net (61.219.38.89)
   |-www.hinet.net(1.1.1.1)
   (1) Restore default romfile.
   (2) Add a Address record www.hinet.net IP is 1.1.1.1

(3) LAN DHCP First DNS is Relay Second and Third is none.
(4) LAN PC release and renew.
(5) LAN PC ping www.hinet.net will resolving IP 1.1.1.1 (right)
(6) LAN PC ping www.HINET.net will resolving IP 61.219.38.89 (wrong) DNS must case-insensitive

7. [BUG FIX]
   Symptom: Router crash.
   Condition:
   (1) Use router for a long time.
   (2) Sometimes Router will crash and the console shows "Common TOS: Free queue session number > max session number..\tos.c:960 sysreset()".
8. [BUG FIX] 050615687
   Symptom: The ”Log Consolidation Period” field in “log setting” page display wrong vaule.
   Condition:
   1. Goto eWC->LOGS->Log Settings page, input the vaule, 300, into ”Log Consolidation Period” field then apply the setting.
   2. Refresh the Log Settings page, the value in ”Log Consolidation Period” field show as 44.

Modifications in V 3.64(WZ.2) | 06/07/2005
Modify for formal release

Modifications in V 3.64(WZ.2)b2 | 05/30/2005
1. [BUG FIX] 050527747
   Symptom: DNS of Dail backup has some problems if WAN's Encapsulation= PPTP mode.
   Condition:
   (1) Restore default romfile.
   (2) WAN is configured as PPTP, and WAN is connected.
   (3) Configure Dial backup.
   (4) Unplug the WAN, and WAN is disconnected, and Dial backup is connected.
   (5) In eWC/DNS/System, DNS server keep old DNS IP (Assigned from PPTP server).

Modifications in V 3.64(WZ.2)b1 | 05/25/2005
1. [BUG FIX]
   Symptom: Dynamic rule with more than two initiators has problem.
   Condition:
   (1) ZyWALL as responder has one dynamic rule.
   (2) Two initiators (two devices or two vpn clients..).
   (3) Dial one of them, the packets can be transmitted through the tunnel correctly.
   (4) Dial the second, only one of them can work correctly.
2. [BUG FIX] 050328353
   Symptom: Trigger dial fail in dial backup.
   Condition:

(1) Restore default rom file.
(2) Setup dial backup account and phone number, and make sure it can work.
(3) Put a PC in router's LAN and ping 168.95.1.1 continually.
(4) Unplug modem's phone line and wait for 5 mins.
(5) Plug it and router will not dial from modem automatically.

3. [BUG FIX] 050425199
   Symptom: Dial back-up does not support FULL-FEATURE NAT.
   Condition:
   (1) Enter SMT menu 11.3 for ”dial backup” remote node
   (2) Go to ”Edit IP” and change NAT selection to FULL Feature. (will see the NAT Lookup Set= 3)
   (3) Go to SMT menu 15.1 and found there is no NAT_SET 3.
4. [BUG FIX] 050502013
   Symptom: VPN tunnel can't be up with dynamic rule.
   Condition:
   Initiator: One IKE with one policy. And in policy, local ID type = Subnet. Dest ID type = Subnet.
   Responder: One dynamic IKE with two policies:
   (1) Policy 1: Encryption is wrong. Local ID type = Subnet. Local starting IP Address is wrong.
   (2) Policy 2: All setting is correct.
5. [BUG FIX] 050506314
   Symptom: Modification to existing WANtoWAN rule (with IKE and BOOTP) can not work
   Condition: In the example, use SSH
   (1) Change SSH port to 2222 in Remote MGMT.
   (2) Go to WAN to WAN / ZyWALL and create a custom service, TCP/UP 2222.
   (3) Add the rule in the default rule that has IKE and Bootp. <===
   (4) Try to connect with Putty or other prefered SSH client. ===> doesn’t work
   (5) Now add the standard SSH (or any other predefined TCP rule) service to the same firewall rule. It to work
6. [BUG FIX]
   Symptom: Router crash.
   Condition:
   (1) Turn on firewall.
   (2) Sometimes router will crash when suffer attack.
7. [BUG FIX]
   Symptom: DNS cannot work after switching WAN and Dial backup.
   Condition:
   (1) Restore default romfile.
   (2) WAN is configured as PPTP, and nail-up, and WAN is connected.
   (3) Configure Dial backup, and is always-on.
   (4) Unplug the WAN, and WAN is disconnected, and Dial backup is connected.
   (5) Plug in the WAN line again, and PPTP is connected, get an IP.
   (6) Go to eWC->DNS->DHCP page, DNS from ISP is none; if PC DNS is ZyWALL, it cannot browse to the internet.

8. [BUG FIX]
   Symptom: Input more than 20 number of source address or destination address in Firewall rule, but only the first 20 rules will be shown on GUI.
   Condition:
   (1) Entered more than 20 source addresses in a firewall rule and saved that rule.
   (2) After saving, only the first 20 source addresses are shown in the list.
9. [BUG FIX] 050502041
   Symptom: Daylight Saving problem: Current Time is faster 2 hours than Taiwan during daylight saving.
   Condition:
   (1) Restore default romfile.
   (2) Go to eWC->Maintenance->TimeAndDate. and the problem happened only when
   (3) Apply the "Time Zone" = "(GMT+08:00)", activate "Enable Daylight Saving" and set the date range include the current time.
   (4) Click the "Apply" button and the page will be refreshed.
   (5) The current time is faster 2 hours than Taiwan, it should be faster 1 hour only.
10. [BUG FIX]
    Symptom: PPTP does not work successfully.
    Condition:
    (1) Edit web eWC/WAN/WAN1, Encapsulation=PPTP, User Name=test, Password=test, Retype to Confirm=test, My IP Address=192.168.65.222, My IP Subnet Mask=255.255.255.0, Server IP Address=192.168.65.33, Connection ID/Name=C:1, WAN IP Address Assignment=Get Automaticlly from ISP.
    (2) Dial WAN1 form eWC/HOME. It works successfully.
    (3) Edit web eWC/WAN/WAN1, Encapsulation=Ethernet.
    (4) Edit web eWC/WAN/WAN2，Encapsulation=PPTP, User Name=test, Password=test, Retype to Confirm=test, My IP Address=192.168.65.223, My IP Subnet Mask=255.255.255.0, Server IP Address=192.168.65.33, Connection ID/Name=C:1, WAN IP Address Assignment=Get Automaticlly from ISP.
    (5) Dial WAN2 form eWC/HOME, and it fails.
    (6) If we dial WAN2 first, then dial WAN1, both WAN1 and WAN2 success. If fails when we dial WAN1 first then dial WAN2.

Modifications in V 3.64(WZ.1) | 05/04/2005
Modify for formal release.

Modifications in V 3.64(WZ.1)b1 | 04/26/2005
1. [ENHANCEMENT]
   Enlarge content filter web site, forbidden key word and trusted website size to 100.
2. [ENHANCEMENT]
   Add sequence number and SPI in log for ESP / AH packets
3. [ENHANCEMENT]
   Change DNS Address Record size from 8 to 30
4. [EHNANCEMENT] 050419889
   Add IP information for my IP address and Secure Gateway address. In CI command, "ipsec ikeDisp #" will show IKE rule configuration. When my IP address or secure

gateway address is domain name, the resolved IP will show after domain name.

5. [BUG FIX] 050128770
   Symptom: When users remotely manage the ZyWALL via a PPTP connection, a strange firewall session (between PPTP server and PPTP client) timeout log may be observed.
   Condition:
   (1) Configure the ZyWALL's WAN port to use PPTP encapsulation.
   (2) Remotely login eWC (http/https) via the PPTP connection.
   (3) After a few minutes, check the centralized logs or syslogs, you will observe a sequence of firewall logs of http/https session timeout.
6. [BUG FIX] 040507153
   Symptom: Telnet function takes too much time.
   Condition:
   (1) Type the CI command "ip telnet host_A".
   (2) When telnet from router to non-exist server host_A, it always takes about 40 seconds or more to connect. And users cannot interrupt the router and can do nothing.
7. [BUG FIX] 041004064
   Symptom: P2000W and P2000W can not talk to each other in P2P mode.
   Condition:
   (1) Topology:
   P2000W----DUT---Internat---DUT---P2000W
   (2) P2000W and P2000W can not talk to each other in P2P mode.
8. [BUG FIX] 050302164
   Symptom: In bridge mode, after device synchronized the defined NTP server, the result displayed failed.
   Condition:
   (1) PC(192.168.1.33) --- DUT(192.168.1.254) --- NAT(192.168.12.106) --- Internet.
   (2) In eWC/Maintenance/Time and Date, get from Time Server: Time Protocol=NTP (RFC 1305), Time Server Address= a.ntp.alphazed.net, then clicked "Synchronize Now" button.
   (3) The result displayed failed. ("System Time and Date Synchronization Fail")
   (4) However, a successful log showed in eWC/LOGS.
   (5) Actually, the device was successful to synchronize the defined NTP server.
9. [BUG FIX] 050217478
   Symptom: Netbios packet cannot pass through VPN tunnel .
   Condition:
   (1) Configure a VPN tunnel as follows:
   1.1 local subnet mask is 192.168.1.1/255.255.0.0.
   1.2 remote subnet mask is 192.169.1.1/255.255.0.0.
   1.3 Enable ”Netbois pass through” in local and remote gateway.
   1.4 PC A(Local)------ZyWALLA------ZyWALLB---PC B(Remote)192.168.1.1/24 192.169.1.1/24
   (2) Establish the VPN tunnel.
   (3) In PC A, Search PC B’s computer name.
   (4) PC A will send a broadcast packet to search PC B.
   (5) ZyWALL A will change destination IP address from 192.168.255.255 to

192.169.255.255 and send to ZyWALL B after encryption. Horever, ZyWALL A should adjust the UDP checksum but it didn't.
(6) PCB will drop the received broadcast UDP pcket from PC A due to error UDP checksum.

10. [BUG FIX] 050214274
    Symptom: VPN My IP Addr will resolving fail
    Condition:
    (1) Add a VPN rule and My IP Address and Remote Gateway Address are domain type.
    (2) Click Dial button, it will fail to build tunnel first time (second time is ok)
    (3) Check log will display "Cannot resolve My IP Addr for rule xxx"
11. [BUG FIX] 050304284
    Symptom: There is no log for replay packets
    Condition:
    (1) Enable "Anti-Replay" function.
    (2) Sniffer an ESP packet and replay it.
    (3) This ESP packet will be dropped by there is no log.
    (4) There should be log to show this action.
12. [BUG FIX] 050316859
    Symptom: ZyWALL (3.64) crashes while remote VPN software (ZyWALL VPN Client) make a VPN connection
    Condition:
    (1) ZyWALL start negotiating with remote VPN software.
    (2) The remote VPN software sends too long VID size.
    (3)device will crash.
13. [BUG FIX] 050221575
    Symptom: Max. Concurrent Sessions Per Host problem.
    Condition:
    (1) In eWC->NAT , change Max. Concurrent Sessions Per Host to 300
    (2) Use ipscan tool to make session
    (3) Log show "192.168.1.33 exceeds the max. number of session per host! " when exceeds the max. number of session per host, but Max. Concurrent Sessions Per Host (Historical high since last startup: 286), it's not reach 300
14. [BUG FIX] 050407160
    Symptom: PC cannot ping remote secure gateway's LAN IP via VPN tunnel
    Condition:
    PC A (1.33) – (1.1)ZW70 --- LAB ---- ZW5 (2.1) ----(2.33) PC B
    (1) Add a VPN rule(ZW70), and in IPsec rule Local Network select Subnet Address, Starting IP is 192.168.1.0 / 255.255.255.0. Remote Network select Subnet Address Starting IP is 192.168.2.0 / 255.255.255.0.
    (2) ZW5 had opposite setting.
    (3) Build up this tunnel, PC A can ping PC B, but PC A can't ping 192.168.2.1(ZW5 gateway LAN IP)
15. [BUG FIX] 050301086
    Symptom: Remote gateway Address can't configure as domain type when ipsec Nail-Up option is on.

Condition:
(1) Add a VPN rule(Static rule) with Remote gateway Address set as domain type.
(2) In Ipsec rule, enable Nail-Up option.
(3) Return to IKE rule page, change some fields and click Apply. The Status will show “This ipsec rule bounds to dynamic IKE rule. Please inactive nail up.” and it can’t be saved.

16. [BUG FIX] 050309435
    Symptom: Router crash when recieve UDP packets which comes from TfGen.
    Condition:
    (1) Restore default rom file.
    (2) In WAN side, place a PC and open TfGen tool to send packets to router's WAN.
    (3) The TfGen's setting in my PC is: Ultilization: 4kbps, Destion: 192.168.70.34, Port: 500.
17. [BUG FIX] 050214258
    Symptom: DNS inverse query causes system crash.
    Condition:
    (1) Set A PC on the device LAN site.
    (2) The DNS server of the PC sets to the device.
    (3) The PC sends DNS inverse query continually, the device will crash sometimes.
18. [BUG FIX] 050204235
    Symptom: Responder receive duplicate package when VPN tunnel established
    Condition:
    (1) At Initiator edit one VPN rule and Extended Authentication=enable=client mode
    (2) At responder edit one VPN rule and Extended Authentication=enable=server mode
    (3) when VPN tunnel established ,Responder log show “Rule[IKE1] receives duplicate packet”
19. [BUG FIX] 050412413
    Symptom: There is no “Ping of Dead” log message when performing “Consolidate every 10 seconds（Attack: ping of death）”
    Condition:
    (1) Dos command ”ping 192.168.1.1 -l 2000”
    (2) User can not see ”ping of death” consolidation log on eWC/LOGS page
    (3) Bridge mode only.
20. [BUG FIX] 050303203
    Symptom: DNS inverse query causes memory leak.
    Condition:
    (1) Set A PC on the ZyWALL LAN site.
    (2) The DNS server of the PC sets to the ZyWALL.
    (3) The PC sends DNS inverse query continually (ex: 140.113.23.1), the system will generate memory leak.
21. [BUG FIX] 050201040
    Symptom: "Gateway Domain Name Update Timer" in eWC --> VPN --> Global Setting didn't work.
    Condition:
    (1) Set one IKE rule which secured gateway address is domain name.

(2) Set "Gateway Domain Name Update Timer" to 15 minutes and apply.
(3) System will not update secured gateway domain name according to the setting unless system reboot.

22. [BUG FIX] 050415692
    Symptom: Resolving a domain name which start with number (for example 4youcard.com) will fail.
    Condition: CI command "ip ping 4youcard.com" and it will fail.
23. [BUG FIX] 050314705
    Symptom: FTP cannot work after setting a policy route with IP gateway.
    Condition:
    (1) Restore default rom file.
    (2) Set WAN as A/A mode and add a policy route with "protocol=TCP" and "Gateway=192.168.70.250". Note: My WAN status is: WAN IP:172.21.2.101,WAN 2 IP:192.168.70.32.
    (3) Ftp:ftp.ncu.edu.tw (account:anonymous/a@a.a.a) in LAN side and it cannot work.
    (4) Disable this policy route and the ftp is OK.
24. [BUG FIX] 050406055
    Symptom: ZyWALL VPN traffic will lose from time to time
    Condition:
    (1) To create tunnel from zw70 to peer.
    (2) To ping the LAN PC of peer VPN gateway fom the LAN PC of zw70 via the tunnel.
    (3) About 1 min, it will re-key again.
    (4) The tunnel loses packet.
25. [BUG FIX] 041201001
    Symptom: Router will crash when receive an unrecognizable DNS response
    Condition:
    Environment:
    PC(192.168.1.33)-----(192.168.1.1)ZW70---Internet
    (1) Set ZW70's system DNS server as "164.67.128.1"
    (2) From PC, send a DNS query to ZW70. The DNS format is as following:
    cf 07 01 00 00 01 00 00 00 00 00 00 04 75 63 6c
    61 03 65 64 75 00 00 ff 00 01
    (3) ZW70 will relay the DNS query to "164.67.128.1".
    (4) ZW70 will crash after receive DNS response from "164.67.128.1"
26. [BUG FIX] 050311685
    Symptom: Firewall WAN to DMZ Reject can't work.
    Condition: PC A ---- (W)ZW70 (DMZ) 10.1.1.1 --- 10.1.1.100 ZW10W
    (1) In eWC Firewall Default Action WAN to DMZ select Reject. And enable Log
    (2) One ZW10W connect to ZW70 DMZ port and IP is 10.1.1.100
    (3) Add default server 10.1.1.100.
    (4) PC A also can ftp to DMZ ZW10W.
    (5) Check Picture [ZW70]Firewall W2D item 3->1
27. [BUG FIX] 050420986
    Symptom: External content filter cannot work.
    Condition

(1) Enable external content filter.
(2) Use external content filter for a long time.
(3) System cannot create socket anymore and external content filter cannot work.
(4) Use CI command "ip ping 168.95.1.1", there will be a message "Can't create socket' in console.
(5) You can see there are many used sockets via CI command "sys socket".

28. [BUG FIX]
Symptom: For firewall ACL schedule, if two rules have the same policies except "schedule", only the first rule will work.
Condition:
(1) Set two firewall rules have same policies except schedule.
(2) Only the first rule will work.

Modifications in V 3.64(WZ.0) | 03/04/2005
Modify for formal release.

Modifications in V 3.64(WZ.0)b4 | 02/24/2005

1. [BUG FIX]
Symptom: In bandwidth management priority base, FTP transfer speed slow down until to disconnect .
2. [BUG FIX]
Symptom: Custom traffic will send over 100 kbps in bridge mode.
Condition:
(1)In bridge mode, set WAN as 1000 kbps with fairness mode.
(2)Create a custom class, budget=50, priority=2, no borrow.
(3)Create a ftp class, budget=200, priority=3, no borrow.
(4)Use tfgen to generate UDP traffic to match custom class.
(5)Use ftp to generate TCP traffic to match ftp class.
(6)In GUI statistics page, custom class will be over 100 kbps.
3. [BUG FIX]
Symptom: VPN XAuth rule swap fail.
Condition:
DUT1：
(1) Edit web eWC/VPN，add gateway policy，Name=IKE1，Remote Gateway Address=192.168.11.101， Pre-Shared Key=12345678，Enable Extended Authentication=enable，Client Mode/User Name=dut1，Client Mode/Password=dut1
(2) Edit web eWC/VPN，add network policy for IKE1，Active=enable，Name=IPSec1，Local Network/Starting IP Address=192.168.1.33，Remote Network/Starting IP Address=192.168.2.33
DUT2：
(1)Edit web eWC/AUTH SERVER/Local User Database，index1/Active=enable
(2)Edit web eWC/VPN，add gateway policy，Name=IKE1，Remote Gateway Address=192.168.12.100， Pre-Shared Key=12345678
(3)Edit web eWC/VPN，add gateway policy，Name=IKE2，Remote Gateway Address=0.0.0.0， Pre-Shared Key=12345678，Enable Extended

Authentication=enable，Client Mode/User Name=dut1， Client Mode/Password=dut1
(4)Edit web eWC/VPN，add gateway policy，Name=IKE3，Remote Gateway Address=0.0.0.0， Pre-Shared Key=12345678，Enable Extended Authentication=enable，Server Mode=enable
(5)Edit web eWC/VPN，add network policy for IKE1，Active=enable，Name=IPSec1，Local Network/Starting IP Address=192.168.2.43，Remote Network/Starting IP Address=192.168.1.33
(6)Edit web eWC/VPN，add network policy for IKE2，Active=enable，Name=IPSec2，Local Network/Starting IP Address=192.168.2.53
(7)Edit web eWC/VPN，add network policy for IKE3，Active=enable，Name=IPSec3，Local Network/Starting IP Address=192.168.2.33

4. [BUG FIX]
   Symptom: In eWC->Wireless, When select WPA or WPA PSK, the Authentication Databases field always says: Local User first then RADIUS.
   Condition: Go to eWC>WLAN>Wireless, when select WPA or WPA PSK, the Authentication Databases field always says: "Local User first then RADIUS". But it shouldn't.
   (1)When selecting "WPA", we should show "Authentication Database = RADIUS" instead of "Authentication Databases Local User first then RADIUS"
   (3) When selecting "WPA+PSK", "Authentication Databases" should be hidden.
5. [BUG FIX]
   Symptom: Upgrade firmware from 3.63 to 3.64, the wildcard field of address records on the DNS page will be enabled.

Modifications in V 3.64(WZ.0)b3 | 02/03/2005

1. [BUG FIX]
   Symptom: DPD vendor ID is not correct.
   Condition: VID value of DPD is not compatible with RFC3706.
2. [BUG FIX]
   Symptom: OpenPhone H.323 traffic will be blocked by Firewall if connection is initiated from WAN side to LAN side.
3. [BUG FIX]
   Symptom: Device will crash.
   Condition: Use IXIA to simulate 1012 ip address to access web site (every ip has 10 sessions), device will crash.

Modifications in V 3.64(WZ.0)b2 | 01/30/2005

1. [BUG FIX]
   Symptom: The name of Domain name does not check properly in SMT 1.
   Condition:
   (1)In SMT 1->Edit Dynamic DNS->Edit Host, fill the record 1's "domain name" with "xxx.dyndns.org". and record 2's "domain name" with "xxx.dyndns.org ". (the domain

name of record 2 contains a space at the end)
(2)The domain should not contain space, we should have a filter to check this.
(3)Set record 1's "Update policy" with "Use WAN IP Address" and record 2's "Update policy" with "Let DDNS Server Auto Detect".
(4)After the DDNS process updating, the domain name "xxx.dyndns.org" will be resolved by the policy "Let DDNS Server Auto Detect" not "Use WAN IP Addrsss". (the first DDNS query result was overwritten by the second executed, "xxx.dyndns.org" is the first, "xxx.dyndns.org " is the second)

2. [ENHANCEMENT] On eWC>BW MGMT>Class Setup, add a popup warning message "Delete Class : class name ?" before user delete a Class.
3. [ENHANCEMENT] Add a active checkbox for ipsec rule on VPN wizard.
4. [BUG FIX]
   Symptom: The wording of Dial Backup in SMT is not consistent with GUI.
   Condition:
   (1) In "eWC->WAN->Dial Backup", one of the wording in "Budget" is "Always On".
   (2) In SMT, the wording is "Nailed-Up Connection".
5. [BUG FIX]
   Symptom: The content of "My IP Address" should show domain name on eWC/VPN/VPN Rules(IKE).
   Condition:
   (1) Go to eWC->DNS->DDNS, fill the "domain name" with "aaa.com" then click "Apply".
   (2) Go to eWC->VPN->VPN Rules (IKE), Add a gateway policy, fill the "name" with "test", select "My domain name" as "aaa.com", fill the "pre-share key" with "12345678" then click "Apply".
   (3) In the VPN rules summary, my IP Address should be "aaa.com" but the router shows "0.0.0.0".
6. [BUG FIX]
   Symptom: Enter special URL will cause device crash.
   Condition: Form LAN site, enter http://192.168.1.1/Forms/rpAuth_1?ZyXEL%20ZyWALL%20Series<script>top.location.pathname=%20""</script> on browser, the device will crash.
7. [BUG FIX]
   Symptom: The CI command "ip nat service irc" may display strange Enable state.
   Condition:
   (1) Execute "ip nat service irc he_is_good".
   (2) Execute "ip nat service irc 0".
   (3) Execute "ip nat service irc he_is_bad".
   After Step 3, you will see that a strange Enable state, e.g., "IRC enable = 12".
8. [BUG FIX]
   Symptom: The eWC>Firewall>Rule Summary>EDIT RULE page might be corrupted.
   Condition:
   (1) Go to eWC>Firewall>Rule Summary.
   (2) Add or Edit a firewall rule.

(3)Try to delete a Source Address (or Destination Address) without first selecting an address.
(4) Or try to delete a Service without first selecting a service.
(5) With 3 or 4, you will see an error message on the status bar.
(6) Click on any button of this page, then you will see that the values of some fields on this page are lost. Also you won't be able to escape this page by clicking on the Cancel button.

9. [ENHANCEMENT] Add SIP protocol in service list in firewall rule edit page.
10. [BUG FIX]
    Symptom: In SMT 15.1 address mapping rule error message not correct.
    Condition:
    (1) In SMT 15.1, configure NAT address mapping many to many overload(or many one to one).
    (2) Configure local address from 0.0.0.0 to 255.255.255.255.
    (3) Configure global address from 0.0.0.0 to 255.255.255.255.
    (4) Save the configuration =>error message show "The end IP address must be great than the start IP address " not correct.
11. [BUG FIX]
    Symptom: Configure WAN page, and WAN priority will become 1.
    Condition:
    (1) In "eWC->WAN->General", set WAN1 priority to 5.
    (2) In "eWC->WAN->WAN"., set encapsulation type to PPTP or PPPoE.
    (3) Go to "eWC->WAN->General", WAN's priority will become 1.
12. [ENHANCEMENT] Give a warning message when user configure FTP/SIP/H.323 filter on BWM but FTP/SIP/H.323 ALG is not enabled.
    GUI : Save the filter and show the warning message. Warning: This is a SIP(FTP, H.323) filter, you have to enable SIP(FTP, H.323) ALG by CI command "ip alg enable".
    CI command : After running "bm config save", the router will save the configuration and check all filters in all interface. Then show a list of filters which are conflicted.
13. [ENHANCEMENT] NAT address mapping need prevent user configure local IP range and global IP range overlap.
14. [BUG FIX]
    Symptom: SIP WiFi-Phone's voice communication failed.
    Condition:
    (1) Use following topology to test.
    WiFi A-DUT----Internet(SIP server)---DUT----WiFi B
    (2) Both ZyWALL reset to default romfile.
    (3) In SMT 24.8 CI command, both type "ip alg enable ALG_SIP" to enable SIP ALG.
    (4) WiFi A make a phone call to WiFi B, voice communication works fine.
    (5) Terminate the phone call ,then WiFi B make a phone call to WiFi A, voice communication fail.
    (6) Fail status: WiFi A can hear voice, but WiFi B can't.
15. [BUG FIX]
    Symptom: The device crashes while the user is changing the SNMP access right

configuration.
Condition:
(1) Restore default romfile.
(2)Set the SNMP Access = Disable.
(3) Use MS-SOFT to query the device.
(4) Before the query timeout, change Access = ALL, the device will crash.

16. [BUG FIX]
Symptom: In authentication server, the local user database should check if the input user name is duplicate.
Condition:
(1) Restore to default romfile.
(2) In record 1, active = yes, name = test, password = 1234 In record 2, active = yes, name = test, password = 5678
(3) Press Save and this configuration will be accept by router.

17. [BUG FIX]
Symptom: BWM linear search can not find first match filter.
Condition:
PC1 ------------ (LAN) DUT(WAN) ----- PC2
(1) Enable BWM on WAN, setup two classes for WAN Root class:
Root 1000kbps
|-------Class 1: 200kbps
|-------Class 2: 200kbps
Filters table:
Class 1: FTP SrcIP = 192.168.1.0/24
Class 2: FTP DstIP = 192.168.70.0/24
(2) FTP upload file from PC1 to PC2.
(3) In this case, BWM will match Class 2's filter. But it's wrong, in linear search algorithm, we should return the first match filter for traffic.

18. [BUG FIX]
Symptom: When manual mode encapsulation is Tunnel, responder can't build up tunnel. Condition:
(1) PC A – DUT ---- DUT - PC B
(2) On eWC/VPN/Manual add two manual rules in DUT and DUT. Rule 1 is inactive. Rule 2 is active and encapsulation is Tunnel.
(3) PC A ping PC B, check SA Monitor, ZW70 tunnel had been built up but no tunnel is up in ZW5, vice versa.
(4) If PC B ping PC A this time, tunnel can be built up in both sides and traffic can be transferred.

19. [BUG FIX]
Symptom: LAN static DHCP can save the same data.
Condition:
(1) Restore default rom file.
(2) In GUI>LAN>Static DHCP, add two record as MAC: 01:01:01:01:01:01, IP: 192.168.1.33 MAC: 02:02:02:02:02:02, IP: 192.168.1.66 and apply it.
(3) Change these two record as MAC: 03:03:03:03:03:03, IP: 192.168.1.99 and apply it.

(4) It can be saved and it is wrong.

20. [BUG FIX]
    Symptom: Nail up warning message does not show correctly in eWC->WAN->WAN.
    Condition:
    (1) Edit a VPN rule and enable nail up
    (2) In eWC->WAN->WAN, set encapsulation with PPPoE and no nailed-up enabled, click "apply" to save, the status will show "Warning: VPN Nailed-Up may trigger dial WAN links."
    (3) Click "apply" again, the status will show "Nothing changed; no need to perform save"
21. [BUG FIX]
    Symptom: VPN tunnel can not be disconnected.
    Condition:
    (1) PC1-DUT-----HUB-----ZW10W(V362WH7)--PC2
    (2) DUT has one IKE and two IPSec rules
    (3) ZW10W has two VPN rules
    (4) ZW10W initiates these two VPN rules
    (5) ZW10W delete these two VPN tunnels but one of DUT VPN tunnels still exist.
22. [BUG FIX]
    Symptom: When out of call schedule, the device still cannot send traffic out.
    Condition:
    (1) Set WAN 1 encapsulation is Ethernet.
    (2) Edit SMT menu 24.10, Time Protocol = Manual, New Time (hh:mm:ss) = 10:00:00, New Date (yyyy-mm-dd) = 2004-06-01.
    (3) Edit SMT menu 26, enter Schedule Set Number to Configure = 1, Edit Name = FD-Once.
        - How often = Once
        - Once Date = 2004-06-01
    - Start Time = 10:05
    - Duration = 00:02
    - Action = Force Down
    (4) Edit SMT menu 11.1, schedule = 1.
    (5) However, when out of schedule about 5 minutes, device still cannot send traffic out.
23. [ENHANCEMENT] In bridge mode, add "Session Table is Full!" log message, when TOS session is full.
24. [BUG FIX]
    Symptom: Wireless CI command "wlan active 100" can be save.(The value should be 1 or 0)
    Condition:
    (1) Plug in B120 and reboot router.
    (2) Use "wlan active 100" and it can be save.
    (3) Go to smt3-5, router will crash.
25. [BUG FIX]
    Symptom: The centralized log shows the strange DHCP entry with hex IP address.
    Condition:

(1) Reset to default rom file.
(2) A PC is set on device LAN site with dynamic IP and no system hostname.
(3) The PC sends DHCP request to device.
(4) The device will show the strange log message have the hex IP address. (ex: 101 01/15/ 2005 10:15:50 DHCP server assigns 0xa0a01e6 to 00:0E:08:AA:B6:B3)

26. [ENHANCEMENT] When router crashes, console will display the restart date and time.
27. [BUG FIX]
    Symptom: VPN page cannot be configured.
    Condition:
    (1) Add a IKE rule.
    (2) Add 10 IPSec rules, and bind them to step1 IKE.
    (3) Delete IKE rule.
    (4) VPN page can't be configured anymore.
28. [BUG FIX]
    Symptom: Enhance the VPN error description
    Condition:
    (1) On eWC VPN, add a IKE rule Dynamic rule (Remote Gateway Address is 0.0.0.0)
    (2) Add a IPSec rule, and fill some value instead of 0.0.0.0 in "Remote Network" fields.
    (3) Status will show "This policy cannot bound to the dynamic rule"
    (4) User may not know where is wrong.
29. [FEATURE CHANGE] Enhance Gateway Domain Name Update Timer. If Gateway Domain Name Update Timer is enabled. The ZyWALL will resolve the IP from a VPN gateway policy whose IKE remote gateway is domain name type in every cycles. If the ZyWALL finds that the new remote gateway IP is different from the old one(which is used by tunnel now), the ZyWALL will delete this tunnel.
30. [BUG FIX]
    Symptom: Save a legal VPN gateway policy but the ZyWALL shows an error message.
    Condition:
    (1) GO to eWC>VPN>GATEWAY POLICY - EDIT
    (2) Save a GATEWAY POLICY whose name = GW, My Address = www.abc.com.tw, Remote Gateway Address = www.cde.com.tw and Pre-Shared Key = 12345678
    (3) GO to eWC>VPN>NETWORK POLICY - EDIT
    (4) Save a NETWORK POLICY whose name = NW, Active = Yes, Starting IP Address = 192.168.1.33, Starting IP Address = 192.168.2.33 and Pre-Shared Key = 12345678
    (5) Go back to eWC>VPN>Rules and edit rule "GW" and set its My Address as 0.0.0.0, then save
    (6) The ZyWALL shows an error message "This IKE rule has static policy rules.", but it should not.
31. [BUG FIX]
    Symptom: There are no logs in eWC>Logs>Log Settings when SMTP authentication fail .
    Condition:

(1) Go to eWC>Logs>Log Settings. Configure a wrong Mail Server/Send Log to/Send Alerts to/ User Name of SMTP Authentication/Password of SMTP Authentication and save.
(2) Go to eWC>Logs>View Log. There are no logs about SMTP Auth failures/SMTP failures.
(3) If the configuration is correct. There is also no log to tell users that the result is successful.

32. [ENHANCEMENT] Add port information in centralized log message when a netbios packet was blocked.
33. [ENHANCEMENT] After the device rebooting, the system will synchronize Time server until any WAN is up or all WAN links are failed exceed 5 minutes.
34. [BUG FIX]
    Symptom: VPN tunnel can establish but traffic cannot go through tunnel.
    Condition: PC1 – DUT -- internet – DUT -- PC2
    (1) Configure corresponding VPN setting in both DUT.
    (2) Dial VPN tunnel
    (3) After tunnel established, PC1 cannot ping PC2 .
35. [BUG FIX]
    Symptom: The router can not flush correctly in eWC->LOGS->Reports.
    Condition:
    (1) In Bridge Mode.
    (2) In eWC->LOGS->Reports, enable "Collect Statistics", interface = LAN, Report type= "Host IP Address".
    (3) When pressing "Flush" button, there is still one record existing "192.168.70.123 Outgoing 3913 bytes". "192.168.70.123" is router's IP address.
    (4) It has the same problem when changing interface from "LAN" to "DMZ" if we do the same action.
36. [BUG FIX]
    Symptom: In bridge mode, SIP traffic can not be managed by BWM.
    Condition: SIP Phone1 ----- (LAN)DUT(WAN) ------ SIP Phone2
    (1) Change router to Bridge Mode.
    (2) Enable BWM, and add a SIP filter at WAN interface.
    (3) SIP Phone1 call SIP Phone2.
    (4) After connection is established, go to eWC->BW MGMT->Monitor, you will see SIP traffic falls into Default class, it's wrong.
37. [BUG FIX]
    Symptom: Router crashes after VPN tunnel is built and start to transfer data.
    Condition:
    (1) PC1-----ZW35------ZW70------PC2.
    (2) Create a simple VPN tunnel between ZW35 and ZW70, ZW35 as Initiator, ZW70 as Responder.
    (3) PC1 ping PC2 to trigger VPN tunnel.
    (4) Tunnel is built but crashes immediately after Ping go through tunnel.
38. [BUG FIX]
    Symptom: Packet still can send out through NAT router when there is no unused port for it.

Condition:
(1) Configure an active port forwarding rule with incoming port range 10000 to 29999.
(2) Send a packet out of NAT router.
(3) The packet can still send out.

39. [BUG FIX]
Symptom: BWM highest priority class can not borrow residual bandwidth from parent class (using tfgen tool)
Condition:
(1) In WAN interface. Enable Priority-based Scheduler.
(2) Class Setup on WAN.
Root 100000 Kbps
|-----WAN 2000 Kbps (No Borrow, No Filter, Priority = 3)
|-----WAN1-1 500 Kbps (Borrow; Filter: SrcIP:0, DestIP:0, SrcPort:0, DestPort:90: Protocol: 17; Priority = 3)
|-----WAN1-2 300 Kbps (Borrow, Filter: SrcIP:0, DestIP: 192.168.70.0/24, SrcPort:0, DestPort:0, Protocol: 17; Priority= 6)
(3) From LAN host, use tfgen (UDP packet generator) to generate two session to match class WAN1-1 and WAN1-2.
session 1: Utilization = 2000Kbps, Destination = WAN host (192.168.70.57), port=90. This will match WAN1-1 class.
session 2: Utilization = 2000Kbps, Destination = WAN host(192.168.70.57), port = default. This will match WAN1-2 class
(4) From Monitor, WAN1-1 should be protected at 500Kbps, and WAN1-2 should borrow remaining bandwidth from parent class.
But you will see WAN1-1 still borrow remaining bandwidth and WAN1-2 almost borrow nothing from parent class.

40. [BUG FIX]
Symptom: There is no response from DMZ after set system name by SNMP.
Condition:
(1) Reset to factory default setting.
(2) Disable firewall.
(3) Ping router's DMZ IP address continuity.
(4) Set DUT's system name by SNMP tool "MG-SOFT MIB browser".
(5) There is no response from DMZ anymore.

41. [BUG FIX]
Symptom: BM filter can not be deleted via CI command.
Condition:
(1) On eWC->BW MGMT->Class Setup, create 3 classes on LAN interface and all class's filter is enabled.
(2) Go to SMT 24.8, delete the third filter by "bm filter lan del 3" and then save data by "bm config save"
(3) By typing, "bm show filter", you will see the third filter still exists.

42. [BUG FIX]
Symptom: Memory leak in DNS query.
Condition:

(1) Set the device as the network gateway.
(2) Some PCs assign the DNS server to the device.
(3) After some days, the DNS query will cause memory leak.

43. [BUG FIX]
    Symptom: Executing CI command "ip nat service irc" will make the router crash.
    Condition:
    (1) In SMT 24.8, type "ip nat service irc" then press enter.
    (2) The router crash.
44. [BUG FIX]
    Symptom: NAT address mapping functionality fail.
    Condition:
    (1) Restore to factory default.
    (2) In SMT4, set "Network Address Translation" as "Full Feature".
    (3) In SMT 15.1.1, insert a rule in rule 1. Take an example with my setting: Type: One to One. Local IP: 192.168.1.33 Global IP: 192.168.70.111
    (4) In PC/192.168.1.33, ftp to server/192.168.70.8. In FTP server, you can find the incoming IP is 192.168.70.111.
    (5) Change step3 address mapping rule, Global IP: 192.168.70.123
    (6) Repeat step 4, you can find the incoming still 192.168.70.111. This is wrong, it should be 192.168.70.123.
45. [FEATURE CHANGE] Extend "devID" field to six hexadecimal numbers(12 characters) in syslog format.
46. [BUG FIX]
    Symptom: Netmeeting H.323 traffic will be blocked by Firewall if connection is initiated from WAN side to LAN side.
    Condition:
    PC1(Netmeeting)--------(LAN) ZyWALL (WAN) --------- PC2(Netmeeting)
    (1) Enable Firewall, setup a WAN2LAN firewall rule for H.323 service
    (2) Enable NAT port forwarding for port 1720(H.323) to PC 192.168.1.33
    (3) PC1 and PC2 use Netmeeting, PC2 call PC1.
    (4) Netmeeting application traffic will be blocked by Firewall, you will see a lot of Firewall blocked log in Centralized LOG.
47. [ENHANCEMENT]
    BWM children's bandwidth's sum will not exceed parent's.

Modifications in V 3.64(WZ.0)b1 | 12/17/2004

1. [ENHANCEMENT]
   IPSec enhancement :
   (1) Remove SMT27 for VPN setup.
   (2) Redesign CI commands for VPN
   (3) One IKE rule(Gateway policy) bind with multi IPSEC rules(Network Policy).
   (4) Add the log for "VPN connectivity check"
   (5) Support Multiple Proposals.
   (6) On eWC>VPN>Global Settings, add IPSec timers configuration.
   (7) For Network Policy, add Netbios passthrough field.
   (8) For Gateway Policy , add FQDN field for My Address.

2. [FEATURE CHANGE]
   Support (Port Restricted) Cone NAT
3. [ENHANCEMENT]
   Bandwidth Management add “Filter List”. Classifier will search Filter List sequentially to find matching class.
4. [FEATURE CHANGE]
   For wireless feature, remove WPA mixed mode function.
5. [ENHANCEMENT]
   Add eWC>Content Filter>Cache page to display URL cache.
6. [ENHANCEMENT]
   New Wizard design for VPN and Internet Access
7. [ENHANCEMENT]
   Enhance ZyWALL GUI according to beta testers' feedbacks.
   (1) To allow more than two child windows open from multiple ZyWALLs, the second parameter (windowName) of the JavaScript function Window.open() will be the MAC address of the ZyWALL that is currently being managed. The child windows include the following.
   1). Wizards
   2). Help
   3). Show Statistics
   4). Show DHCP Table
   5). VPN Status
   6). BWM statistics
   (2) For identification purpose, the title of the eWC parent window, as well as its child windows, will contain the system FQDN of the ZyWALL that is currently being managed.
8. [ENHANCEMENT]
   Integration of TOS & NAT information
   (1) Current concurrent sessions = max(TOS current concurrent sessions, NAT current concurrent sessions)
   (2) Historical high since last startup = max(TOS historical high since last startup, NAT historical high since last startup)
9. [ENHANCEMENT]
   In eWC>HOME>Show Statistics page, the ZyWALL will keep the configuration modified by users. Therefore, next time when users access this page, they don't have to configure the settings in order to see proper info again.
10. [ENHANCEMENT]
    Add Log Consolidation into eWC>Logs>Settings.
11. [ENHANCEMENT]
    Remove the metric configuration field from eWC>WAN Traffic Redirect and Dial Backup Pages
12. [ENHANCEMENT]
    Add VT6105 and NPE Speed Configuration function. User can force VT6105 or NPE 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.
3. ZyWALL 35 LAN/DMZ not support this feature.

13. [ENHANCEMENT]
    Enable "ip alg" command in bridge mode.
14. [ENHANCEMENT]
    In eWC>DNS>System>Address Record, add Wildcard.
15. [ENHANCEMENT]
    1.In eWC>Home>Current Time, add GMT timezone + DST offset.
    2.In eWC>Date&Time>Current Time, GMT add timezone + DST offset.
16. [ENHANCEMENT]
    Add GUI for LAN DHCP Relay feature.
17. [ENHANCEMENT]
    Add a API function to move rules for NAT address mapping table. CI command: ip nat acl move <set#> <rule# from> <rule# to>
18. [FEATURE CHANGE]
    For Manual IPSec rule, remove My Domain Name and change Secure Gateway Address into IP field
19. [ENHANCEMENT]
    On eWC>HOME>VPN wizard, My ZyWALL address supports Domain Name.

Modifications in V3.63(WZ.0) | 12/02/2004

Formal release

Modifications in V3.63(WZ.0)b3 | 11/17/2004

1. [BUG FIX]
   Symptom: Bandwidth Management sub class cannot borrow budget from parent.
   Condition:
   甲、Add a subclass on WAN and set budge 2048Kbps
   乙、Enable “Borrow bandwidth from parent class”
   丙、Upload file to WAN site’s FTP server=>Fail, “Borrow bandwidth from parent class” can not work correctly
2. [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.
3. [BUG FIX]
   Symptom: Cannot find help pages.
   Condition:
   (1) In “eWC->POLICY ROUTE”, the help page cannot be found.
   (2) In “eWC->POLICY ROUTE->Edit”, the help page cannot be found.
4. [BUG FIX]
   Symptom: No "Forward web site" log.
   Condition:
   (1) In "eWC->CONTENT FILTER->General", enable content filter.

(2) In "eWC->LOGS->Log Settings", select "Forward Web Sites".
(3) Access an allowed web site.
(4) In "eWC->LOGS->View Log", there is no "forward web site" log entry.

5. [BUG FIX]
   Symptom: session.exe causes ZyWALL to crash.
   Condition:
   (1) Run session.exe tool.
   (2) On session.exe console, execute the command "session.exe -ip_destination 192.168.1.1 -port_destination 443", where 192.168.1.1 could be the address of ZyWALL's any (LAN/DMZ/WAN) interface.
   (3) After a while, the system will crash because it runs out of available timers.
6. [BUG FIX]
   Symptom: While LAN MAC address last byte is 0xFF, the WAN MAC address isn't correct.
   Condition: If the LAN MAC address is 00:A0:C5:01:FF:FF, the WAN MAC address should be 00:A0:C5:02:00:00. But the WAN MAC address is 00:A0:C5:01:FF:00.
7. [FEATURE CHANGE]
   Change default setting of SMT 15.1.2
   Was: The default “Set Name” is NULL.
   Is: The default “Set Name” is NAT_SET.
8. [FEATURE CHANGE]
   Modify CI command "ip arp add" from hidden to visible.

Modifications in V3.63(WZ.0)b2 | 10/23/2004

1. [ENHANCEMENT] Support CI command “ip alg…” in bridge mode.
2. [BUG FIX]
   Symptom: The eWC idle timeout mechanism sometimes may malfunction.
   Condition:
   (1) Log onto the ZyWALL eWC.
   (2) Go to eWC>Maintenance>General and set the "Administrator Inactivity Timer" to 1 minute.
   (3) Go to eWC>Maintenance>Time&Date and manually adjust the system time backward 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.
3. [BUG FIX]
   Symptom: Help page can’t show picture
   Condition: On eWC HOME>> Show Statistics >>Help page ,it first Label lack a picture.
4. [BUG FIX]
   Symptom: Use IXIA create session cause zw35 crash
   Condition: Use IXIA create 10100 session and run about 20 minutes, device crash2.
5. [BUG FIX]
   Symptom: Throughput of VPN IKE DES by SmartBits and IXIA both fail
6. [BUG FIX]
   Throughput of LAN to WAN by IXIA occur fail in frame size 64/128/256.

7. [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.
8. [BUG FIX]
   Symptom: WAN cannot send RIP packets.
   Condition:
   (1) Enable WAN 1 RIP and Multicast, and capture packet on WAN side, but device cannot send RIP packets.
   (2) Enable WAN 2 RIP and Multicast, and capture packet on WAN side, but device cannot send RIP packets.
9. [BUG FIX]
   Symptom: WAN 2 does not get RIP packets.
   Condition:
   (1) In Failover mode, the WAN 2 priority is 1 and the WAN 1 priority is 3.
   (2) Enable WAN 2 RIP and Multicast and capture packets at WAN side, the device cannot get RIP packets anymore.
10. [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.
11. [BUG FIX]
    Symptom: LAN DHCP Server cannot work after CI command "sys rn save" for dial backup.
    Condition:
    (1) Reset default rom file
    (2) On SMT menu 24.8 , CI command:
        a. "sys rn load 3".
        b. "sys rn accessblock 1".
        c. "sys rn save"
    (3) On SMT menu 3.2, LAN DHCP option will change from "Server" to "None", and we cannot change this option to "Server" forever.
12. [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 ZyWALL'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".

13. [BUG FIX]
    Symptom: WAN2 can not get ip address from DHCP server.
    Condition:
    (1) Restore default rom file and plug in with WAN1.
    (2) Set BM=>Summary=>WAN1 enable and add a subclass and enable it.
    (3) Set BM=>Summary=>WAN1 disable,BM=>Summary=>WAN2 enable.
    (4) Pull out WAN1 and plug in WAN2.
    (5) WAN2 can not get ip address from DHCP server anymore.
14. [BUG FIX]
    Symptom: SMT shows strange message ”[error] Failed to send message.
    Condition:
    (1) Restore default rom file.
    (2) Go to SMT 24.1, and press ”9” to reset counter many times, the message ”[error] Failed to send message” shows.
15. [FEATURE CHANGE][INTERNAL]
    Was: The default ROM file has default DNS server of WAN1.
    Is: Remove the default DNS server of WAN1 from default ROM file.
16. [BUG FIX]
    Symptom: eWC will fill the "Connection ID/Name" field with "C:1" when the fetch data is empty.
    Condition:
    (1) In eWC, set "Connection ID/Name" as empty in PPTP mode and apply it.
    (2) Go go another page and go back the WAN page, the "Connection ID/Name" field is filled with "C:1" even we set the field as empty.
17. [FEATURE CHANGE] In eWC->LOG->Log settings->Active Log and Alert, remove the options (Asymmetrical Routes, Multicasts/Broadcasts, TCP Reset, Packet Filter, UPnP, Forward Web Sites) in default ROM file.
18. [FEATURE CHANGE] In eWC->FIREWALL->Anti-Probing, change the value of “Respond on PING on” to “LAN & WAN & DMZ” in default ROM file.
19. [FEATURE CHANGE] In eWC->FIREWALL->Rule Summary, “WAN to LAN” packet direction, add a non-active rule that will forward BOOTP_CLIENT(UDP:68) from WAN to LAN for DHCP service in bridge mode.
20. [FEATURE CHANGE] Change the default behavior of URL checking mechanism in Content Filter’s Customization page in default ROM file. Now, we extend the URL checking range from domain name to entire URL (fullpath plus filename) and it is case insensitive.
21. [BUG FIX]
    Symptom: SMT NAT trigger port cannot save
    Condition: Check SMT menu15.3.1, save flash rom seems fail.
22. [BUG FIX]

Symptom: In eWC, wizard Spoof MAC does not work when encapsulation is PPPoE/PPTP.
Condition:
(1) In eWC>HOME>Internet Access, select PPPoE/PPTP and enable the "Spoof this computer's MAC Address - IP Address".
(2) Go to SMT 24.1 and check WAN MAC. not be spoofed.

23. [BUG FIX]
Symptom: PPPoE/PPTP can't set Fixed IP Address
Condition:
(1) Restore default ROM.
(2) PPPoE / PPTP can't set fixed IP Address in WAN 1 or WAN 2. In PPTP and PPPoE mode, set the WAN IP only(do not set the mask and REM IP) and we can not apply it.
24. [BUG FIX]
Symptom: In bridge mode, the device should not check route assessments.
Condition:
(1) In router mode, enable the ICMP check for route assessments.
(2) Switch to bridge mode.
(3) The device still runs the ICMP check.
25. [BUG FIX]
Symptom: Device Mode does not show status.
Condition:
(1) Under Router mode, in MAINTANCE > Device Mode does not show status.
(2) Under Bridge mode, in MAINTANCE > Device Mode status shows router mode.
26. [BUG FIX]
Symptom: In centralized log, the router shows wrong gateway IP for policy route.
Condition:
(1) WAN1 use PPPoE/PPTP and the packets can go through WAN1 successfully.
(2) Go to eWC->POLICY ROUTE, edit a rule.
(3) Criteria block: Active the rule, select LAN interface, fill the Destination Starting IP Address and Ending IP Address with "168.95.1.1".
(4) Routing Action Block: Select WAN Interface with WAN1 and Log with Yes then save the rule.
(5) Ping "168.95.1.1" in the PC.
(6) Go to eWC->LOGS, we got a log "Policy route rule matched: ICMP, rule: 1, GW: "0.0.0.0".
27. [BUG FIX]
Symptom: WAN 2 MSN Messenger 6.2 some function cannot work.
Condition:
(1) Use WAN 2 and enable UPnP.
(2) MSN Messenger 6.2, voice, white board, program cannot work.
28. [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.
29. [BUG FIX][INTERNAL]

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.

30. [BUG FIX]
Symptom: Firewall “WAN to LAN” log does not show.
Condition:
(1) In eWC->LOG->Log setting->Active Log and Alert, disable “Multicasts / Broadcasts” option .
(2) Check eWC->LOG, the packets belong to “WAN to LAN” category will not be shown.

31. [BUG FIX]
Symptom: Datetime calibration failed to sync with user-defined NTP server.
Condition:
丁、Restore default ROM file.
戊、Go to eWC->MAINTENANCE->Time and Date, set Time Server Address with "time.stdtime.gov.tw".
己、Reboot the router.
庚、Go to eWC->LOG, the router will start time synchronization process, it does not sync user-defined server first (no log).

32. [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.

33. [BUG FIX]
Symptom: The policy route log shown on GUI has some problem.
Condition:
Topology : The WAN 1 uses ethernet and is down, a PC connects to ZyWALL LAN-side.
(1) Go to eWC->POLICY ROUTE, edit a rule.
(2) Criteria block: Active the rule, select LAN interface, fill the Destination Starting IP Address and Ending IP Address with "168.95.1.1".
(3) Routing Action Block: Select WAN Interface with WAN1 and Log with Yes then save the rule.
(4) Ping "168.95.1.1" in the PC.
(5) Go to eWC->LOGS, we got a log "Policy route rule matched: ICMP, rule: 1, GW: 168.95.1.1".
(6) The ping is failed and the router should not show the log, the GW in the log is wrong (168.95.1.1).

Modifications in V3.63(WZ.0)b1 | 09/23/2004

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 see Appendix 8.
6. [FEATURE CHANGE] New feature, Firewall>NAT>Bandwidth Management ALG for SIP/H.323.
7. [ENHANCEMENT] Support up to 35 IPSec VPN connections simultaneously. User can configure 40 IPSec policies.
8. [ENHANCEMENT] Support 48 policy route rules.
9. [ENHANCEMENT] Support 10000 NAT sessions.
10. [ENHANCEMENT] Support up to 50 NAT rules and 50 port forwarding rules.
11. [ENHANCEMENT] Firewall ACL buffer size is up to 40K bytes, the user can configure up to 100 customer ports.
12. [ENHANCEMENT] The size of the cache of Cerberian content filter is up to 2048K bytes.
13. [ENHANCEMENT] Support to use ZyAIR B-120 and ZyAIR G-100 WLAN card.
14. [ENHANCEMENT] Add call schedule for dial backup. The SMT 11.3, for dial backup, has the "Schedules=" option to enable schedule rules.
15. [ENHANCEMENT] Add a new firewall service type - Roadrunner(TCP/UDP:1026) in eWC>FIREWALL>EDIT RULE.
16. [ENHANCEMENT] In eWC>Home page, add a new entry for displaying Dial Backup status into the Network Status table.
17. [FEATURE CHANGE] In eWC>LAN>LAN page, those settings for DNS Server address has been moved to eWC>DNS>LAN page.
18. [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.
19. [ENHANCEMENT] In eWC>WAN, the “Route” tag has been changed to “General” tag.
20. [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 Appendix 7 to know more information about ZyWALL Multiple WAN.
21. [ENHANCEMENT] In eWC>WAN>General page, the wording, “Route Assessment” has been changed to “Connectivity Check”.
22. [FEATURE CHANGE] In eWC>WAN>WAN 1 and WAN 2 page, NAT Full Feature selection has been moved to eWC>NAT>NAT overview page.

23. [FEATURE CHANGE] In eWC>WAN>WAN 1 and WAN 2 page, the Windows Networking group has been moved to eWC>WAN>General page.
24. [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.
25. [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.
26. [ENHANCEMENT] Changing the format of daylight saving to correspond with the popular configuration.
    daylight save: old config: start month – day
    end month - day
    new config: start month - nth week - weekday – hour
    end month - nth week - weekday – hour
27. [ENHANCEMENT] Enhance HOME GUI.
    (1) Add LAN and DMZ IP Alias information. Users can expand or collapse LAN and DMZ to show or hide the IP Alias information by clicking the [+]/[-] icon at the beginning of each entry in Home Network Status Table.
    (2) Remove NAT sessions and add TOS sessions information.
    (3) Merge Current Date and Current Time into System Time and append GMT Time Zone information at the end.
28. [ENHANCEMENT] Add warning message on login page GUI.
    Add warning message "You must enable JavaScript on your browser to access the web configurator." to remind users that Scripting should be turned on if Scripting is not enabled on browser.
29. [ENHANCEMENT] Enhance NAT GUI.
    In NAT>NAT Overview page, add Concurrent Session per Host Historical High information since Startup.
30. [ENHANCEMENT] Enhance eWC>Logs>Report GUI.
    (1) Add a checkbox field "Collect statistics" to eWC>Logs>Reports Page. Next time after reboot, users don't need to click "Start collection".
    (2) Add a checkbox field "Send raw traffic statistics to syslog server for analysis" to eWC>Logs>Reports Page.
    (3) Add a flush button for users to clear the report.
31. [ENHANCEMENT] Add VPN dial on VPN GUI.
    (1) Add a "Dial" icon at the end of each VPN rule in VPN Summary page to dial a selected rule.
    (2) There are warning messages shown on the status bar if users dial an inactive VPN rule or a dynamic rule or manual key rule, or etc.
    (3) A "VPN DIAL" page will be displayed after users click the "Dial" icon at the end of each dial-able rule.
32. [ENHANCEMENT] Enhance LOGS GUI.
    (1) In LOGS>Log Settings page, add "Asymmetrical Routes", "Multicasts / Broadcasts" log setting items under Access Control.
    (2) In LOGS>View Logs page, if users check any sub log under the Access

Control, but doesn't check Access Control, the checked logs will not include in the Display List field.

33. [ENHANCEMENT] The ZyWALL now records the time adjustment offset in the time synchronization successful log.
34. [ENHANCEMENT] Add log for dial backup starting and ending.
35. [ENHANCEMENT] Modify Logout screen.
    If users click on LOGOUT, a popup window asking "Are you sure you want to log out?" will be displayed. And if users click "Yes", the ZyWALL will get back to the login screen, if users click "Cancel", it will go back to the previous screen.
36. [ENHANCEMENT] Add interface options (DMZ/LAN) in eWC>Logs>Reports.
37. [FEATURE CHANGE] For Connectivity Monitor,
    Before: If the check point of route DNS resolve failed, the route status will be assigned to pending.
    Now: If the check point of route DNS resolve failed, the route status will be assigned to DNS resolve failed and its state is down.
38. [FEATURE CHANGE]
    Before:
    (1) The system hides the roadrunner entry from being seen at nat/port forward menu.
    (2) This entry active state is set to TRUE at initialization and negotiation state.
    Now:
    (1) This entry will appear at the end of NAT/port forward menu.
    (2) This entry will be set to TRUE if encapsulation type is Ethernet and service type is not standard, otherwise set to FALSE.
39. [ENHANCEMENT] Remove the metric configuration field from eWC>WAN Traffic Redirect and Dial Backup Pages.
40. [ENHANCEMENT] The error message of eWC>Firewall>Summary will always be displayed on the status bar.
41. [ENHANCEMENT] Content Filtering enhancement.
    Redirect Content Filtering blocked page to a user specified URL for displaying policy.
42. [ENHANCEMENT]
    (1) Support user config for SIP session timeout value
    (2) Support SIP SDP multiple RTP port
    (3) Delete unused ALG type
    (4) CI Command for ALG enable/disable and sip timeout
43. [ENHANCEMENT] Add PAT(Port Address Translation) configuration on GUI.
44. [FEATURE CHANGE]
    Before: In Call Schedule, if the "How Often" = "Once", then the "Once Date" must be bigger than "Start Date".
    Now: When the "How Often" = "Once", the system will disable and ignore the "Start Date" setting.
45. [ENHANCEMENT] Add Log Consolidation into eWC>Logs>Settings GUI.
46. [ENHANCEMENT] On eWC>NAT>Port Forwarding, add Road-Runner server reserved rule to the last in Port Forwarding Rule Table.
47. [ENHANCEMENT] For LAN DHCP server, if user changes LAN IP or LAN alias 1, LAN alias 2 IPs to cause the static DHCP IP Addresses not valid. DHCP server cannot

give the clients the requested STATIC IP, system will generate a centralized log.

48. [ENHANCEMENT] For LAN DHCP server, user can set static IP address in the subnet of LAN alias 1 or LAN alias 2.
49. [ENHANCEMENT] When NAT is enabled and the packet does not match any NAT rule then the packets will pass device in routing mode.
50. [ENHANCEMENT] ZyReport record DMZ and its 2 aliases logs.
    Note:
    (1) For URL, Packet, Port, change their link lists and hashes to link list arrays and hash arrays. 0 for LAN, 1 for DMZ.
    (2) for CI command,
        ip rpt active [0:lan|1:dmz][1:yes|0:no]
        ip rpt start [0:lan|1:dmz]
        ip rpt stop [0:lan|1:dmz]
        ip rpt url [0:lan|1:dmz] maxnum
        ip rpt ip [0:lan|1:dmz] maxnum
        ip rpt srv [0:lan|1:dmz] maxnum
51. [ENHANCEMENT] Tuning the performance for IP Policy Route.
52. [ENHANCEMENT] Consolidate "Exceed maximum sessions per host" logs.
53. [ENHANCEMENT] Firewall can bypass AX.25 (protocol #93) & IPv6 (protocol #41) protocols.
54. [ENHANCEMENT] External content filtering supports full URL checking.
    Was: External content filtering only takes domain name or IP address of URL into category checking.
    Is: External content filtering put entire URL into category checking.
55. [ENHANCEMENT] Add CNM agent version control. Vantage agent needs a mechanism to maintain bug fix or feature change. When agent has any bug fix or feature change , the agent version will be updated and checked in into trunk. User can check the agent version using ci command "cnm version".
56. [ENHANCEMENT] Firewall ACL: add source port support.
57. [ENHANCEMENT] Enhance eWC>Home "System Statistics" GUI.
    (1) In eWC> Home page, users can click "Show Statistics" button to see the system statistics with "Table Chart" mode.
    (2) If users want to see with "Line Chart" mode, they can click a "Line Chart" icon at the beginning of this page.
58. [ENHANCEMENT] Each unified ALG can be enabled/disabled.
    CI command:
    (1) "ip alg display" to display the enable/disable information of each ALG.
    (2) "ip alg enable <ALG_FTP|ALG_H323|ALG_SIP>" to enable an ALG.
    (3) "ip alg disable <ALG_FTP|ALG_H323|ALG_SIP>" to disable an ALG.
59. [ENHANCEMENT] Centralized log add
    (1) Triangle route log switch.
    (2) Broadcast/Multicast log switch.
    Note:
    Add CI commands:
    (1) "sys logs switch".
    (2) "sys logs switch display".

(3) "sys logs switch bmlog <0:no|1:yes>".
(4) "sys logs switch trilog <0:no|1:yes>".

60. [ENHANCEMENT] Add Source Interface check for Policy Route.
    Note: The error message is "At least one Source Interface must be assigned."
61. [ENHANCEMENT] ZyReport can show LAN IP alias information.
62. [ENHANCEMENT] ZyReport can show service name by Firewall custom port.
63. [ENHANCEMENT] Modify eWC>Bridge GUI.
    Add a JavaScript range check(0-240) for Bride RSTP Port Priority. Users just can input 0-240 number in RSTP Port Priority field.
64. [ENHANCEMENT] Router will show a warning message "Warning! No NAT address mapping rule configured in system" when user does not configure any NAT address mapping rule in full feature NAT.
65. [ENHANCEMENT]
    (1) On the My Certificates>Trusted CAs>Trusted Remote Hosts, if the subject/issuer name is too long for display, it will be truncated by 3 trailing dots.
    (2) On a certificate's Details page, the internal buffers are enlarged in order to fully display the Certification Path as well as the Certificate Information.
    (3) On the My Certificate Create page, the max lengths of the Host Domain Name/E-Mail/Organizational Unit/Organization/Country fields are adjusted to 63 bytes.
66. [ENHANCEMENT]
    (1) Remove the redundant log: "Time calibration is successful"
    (2) Change wording: "Time initialized by XXX server" ==> "Time set from XXX server"
67. [ENHANCEMENT] Perform a range check on the port triggering rule ports. If an NAT port triggering rule entry has been configured (i.e., name is not empty), then its start port should be greater than 0.
68. [ENHANCEMENT]
    Enhance FIREWALL > FIREWALL > EDIT RULE page.
    (1) In FIREWALL > FIREWALL > EDIT RULE page, add hour (0 - 23) and minute (0 - 59) check for firewall schedule. If users configure the value out of the range and click Apply, the error message will be displayed in the status bar.
    (2) The End time should always be greater than Start time. If users set the End time less than Start time, an error message will be displayed in the status bar.
69. [ENHANCEMENT] In Home page, set the percentage string to the center of each usage bar by using JavaScript. This modification applies to Memory, TOS Session and Policy Route usage bars.
70. [ENHANCEMENT] Modifies the default settings of Connectivity check.
    Note:
    (1) Default Fail Tolerance value from 2 to 3.
    (2) Period range is between 5 and 300 (seconds).
    (3) Timeout range is between 1 and 10 (seconds).
    (4) Fail Tolerance range is between 1 and 10 (successive checks).
71. [ENHANCEMENT] Modify WLAN MAC Filter log
    WLAN MAC Filter Success=>WLAN STA allowed by WLAN MAC Filter
    WLAN MAC Filter Fail=>WLAN STA denied by WLAN MAC Filter

72. [ENHANCEMENT] Certificate GUI wording changes:
    (1) "My Certificates Setting" ==> " My Certificates"
    (2) "Trusted CA Setting" ==> "Trusted CA Certificates"
    (3) "Trusted Remote Hosts Setting" ==> "Trusted Remote Host Certificates"
    (4) "Directory Services Setting" ==> "Directory Services"
73. [ENHANCEMENT] NAT GUI wording change: "Trigger Port" ==> "Port Triggering"
74. [ENHANCEMENT] Modify the WAN GUI.
    (1) In WAN > DialBackup page, when users click "Edit" button to setup advanced modem configuration, the WAN > Advanced Setup page will be displayed in the main frame instead of a pop-up window.
    (2) If users click "Cancel" button in WAN > Advanced Setup page, it will go to the previous WAN > DialBackup page.
    (3) When users click "Apply" button in WAN > Advanced Setup page, if there is an error, a message will be displayed in the status bar; if no error, the configuration will be saved and then go to the previous WAN > DialBackup page.
75. [ENHANCEMENT] The ZyWALL now uses GMT+0000 time zone when it verifies if a certificate is within its validity period. The GMT+0000 time is not adjusted to reflect changes either to or from Daylight Saving Time.
76. [ENHANCEMENT] Remove the eWC>Remote MGMT>DNS page when the ZyWALL is in Bridge Mode.
77. [ENHANCEMENT] Enhancement NAT GUI.
    (1) In WAN1, WAN2 and Dial Backup page, change the wordings of "Enable Network Address Translation (NAT)" to "Enable NAT (Network Address Translation)".
    (2) Change the wordings of "Port Forwarding Setup" to "Port Forwarding Rules" in Port Forwarding page.
    (3) Change the wordings of "Trigger Port Setup" to "Port Triggering Rules" in Port Triggering page.
    (4) In Address Mapping page, change the wordings of "Address Mapping Setup" to "Full Feature Address Mapping Rules" and add "Default Address Mapping Rules" section at the beginning of this page to display the 2 SUA default rules.
    (5) In NAT Overview page, when users click the "Copy to WAN 1" or "Copy to WAN 2" button, it will pop-up a confirm window to remind users whether to do this action or not.
78. [ENHANCEMENT] Supports Intel TE28F640 J3C120 and TE28F128 J3C150 Flash ROM when ZyWALL is programming flash and displaying flash type information by using "sys atsh".
79. [ENHANCEMENT] Modify VPN to support multiple WAN.
    (1) My IP Address is not 0.0.0.0
        a) Support My IP address is x.x.x.x type.
        b) Support My IP address is DDNS host name.
    (2) My IP Address is 0.0.0.0 and secure gateway IP address is configured.
        a) Secure gateway is in the same network with a WAN interface.
           Ex: Secure gateway is 1.0.0.2 and WAN2 IP Address is 1.0.0.3
        b) A configured Policy Route Rule
           Ex: Policy Route Rule destination IP 1.0.0.x and Secure gateway 1.0.0.2

80. [ENHANCEMENT] Add "Copy to WAN 1" and "Copy to WAN 2" buttons to copy the settings of port forwarding table and trigger port table of WAN 1 or WAN 2 to that of WAN 2 or WAN 1.
81. [FEATURE CHANGE]
    Before: If router set default server in port forwarding, users will see duplicated messages while tracerouting. For example:
    [c:\]tracert -d 172.21.0.254
    Tracing route to 172.21.0.254 over a maximum of 30 hops
    1 <1 ms <1 ms <1 ms 192.168.1.1
    2 1 ms <1 ms <1 ms 172.21.0.254
    3 1 ms <1 ms <1 ms 172.21.0.254
    Trace complete.

    Now: Users will see only one message while tracerouting no matter if the router set default server.
    Note: The change is that if there is an ICMP packet and its destination is the same with default server, router will not decrease TTL.
82. [FEATURE CHANGE] Remove the "Phone Number" field from SMT Menu 2.
83. [FEATURE CHANGE] Change UPnP device name for ZyWALL35
    WAS: "ZyXEL ZyWALL 35 Internet Security Gateway"
    IS: "ZyXEL ZyWALL 35 Internet Security Appliance"
84. [FEATURE CHANGE] If the SGID of device is changed then device will reset SGMP state machine (cnm reset).
    This is modified as follows:
    (1) If SGID is changed when SGMP is in the state of SGMP_STATE_ACTIVE, then device will reset SGMP state machine.
    (2) If SGID is changed when SGMP is in other states, such as registering to Vantage, then device will not reset SGMP state machine.
85. [FEATURE CHANGE] Vantage doesn't support new DDNS in 3.63 firmware version currently.
86. [ENHANCEMENT] In eWC>WAN>WAN1/WAN2>PPPoE/PPTP, if users check the Nailed-Up, the Idle Timeout field will be grayed out by scripting.
87. [ENHANCEMENT] In eWC>Firewall>Rule Summary, if users input an invalid range of firewall rule and click "Apply", an error message "Valid firewall rule number: 1~xxx" will be displayed on the status bar, instead of the pop-up scripting.
88. [ENHANCEMENT] For DNS HA and Proxy, if the name of DNS query is NULL, the system will drop the packet.
89. [ENHANCEMENT] eWC>DNS>Cache table columns title should display an underline when the mouse moves over, in order to indicate that the table can be sorted by different column title.
90. [ENHANCEMENT] If users plug in wireless card and enable wireless LAN, the status of WLAN in eWC>Home>Network Status Table will display the speed of the wireless card.
91. [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.

92. [ENHANCEMENT] Supports SIP ALG for ZyXEL Wi-Fi phone under P-2-P condition.
93. [ENHANCEMENT] Supports SIP ALG for ZyXEL P2002 device.

Modifications in V3.62(WZ.2) | 06/28/2004
Formal release.

Modifications in V3.62(WZ.2)b1 | 06/08/2004
1. [ENHANCEMENT] Support Vantage CNM 2.0 (Vantage Centralized Network Management).
2. [BUG FIX]
   Symptom: Trigger port will disappear after system reboot.
   Condition:
   (1) Configure Trigger port rule.
   (2) System reboots.
   (3) The configured Trigger port rule disappeared.

Modifications in V3.62(WZ.1) | 05/25/2004
Formal release.

Modifications in V3.62(WZ.1)b1 | 05/13/2004
1. [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.
2. [BUG FIX] Symptom: Bandwidth management "barrow bandwidth" mechanism is not correct
   Condition:
   (1) Set up a sub-class A under root. A's priority is 3.
   (2) Set up two sub-classes under A, call them B and C. Both B and C's priority is 3, too.
   (3) When B and C are running, they can't borrow bandwidth even their "Borrow bandwidth from parent class" is checked.

Modifications in V3.62(WZ.0) | 04/07/2004

1. Formal release.

Modifications in V3.62(WZ.0)b5 | 04/06/2004

1. [BUG FIX]
   Symptom: NAT address mapping rule disappears after router reboots.
   Condition:
   (1) In eWC→SUA/NAT→Address Mapping page
   (2) Adds 50 rules.
   (3) Reboots router, user can only see the first 22 rules and the other rules disappear.
2. [BUG FIX]
   Symptom: The behavior in priority-based Bandwidth Management is not correct.
   Condition:
   (1) In eWC→BW MGMT→Summary, activates WAN1 root class with Speed = 1500 kbps and Scheduler = Priority-Based
   (2) In eWC→BW MGMT→Class Setup, Adds two sub-classes under WAN1 root class. Where WAN1-1 : Bandwidth Budget = 200, Priority = 7(higher than WAN1-2), and "Borrow bandwidth from parent class" is selected; WAN1-2 : Bandwidth Budget = 500, Priority = 1, "Borrow bandwidth from parent class" is also selected.
   (3) First generates traffic that satisfies WAN1-2 class, users will find WAN1-2 borrow the whole available bandwidth from parent, and the traffic is bound at about 1500kbps.
   (4) Then generates traffic that satisfies WAN1-1 class. Users will find WAN1-1 can not borrow bandwidth from parent class and bandwidth is bound at about 200kbps even though WAN1-1 has higher priority than WAN1-2.

Modifications in V3.62(WZ.0)b4 | 03/24/2004

1. [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.
2. [BUG FIX]
   Symptom: The daylight saving feature does not function normally. When leaving the daylight saving period, the system will not automatically adjust time.
   Condition:
   (1) Configure current time in daylight saving.
   (2) After the current time leaves the end date of daylight saving, the system does not adjust to correct time.
3. [BUG FIX]
   Symptom: Fixed a wording error "Use WAN IP Address" in SMT1.1.
   Condition:
   (1) Go to SMT1.1 (Dynamic DNS).

(2) The words "Use WAN IP Address" should be "Use IP Address".

4. [ENHANCEMENT]
   In eWC→MAINTENANCE→Time and Date :
   (1) The original page is separated into three parts
      (a) Current Time and Date only displays the information about the system time and date and it's read-only.
      (b) Time and Date Setup includes:
         - Manual (None, use no time protocol)
         - Get from Time Server (Use protocol Daytime, Time or NTP)
      (c) Time Zone Setup: users can configure the time zone and the daylight saving.
   (2) After pressing 'Synchronize Now' button, ZyWALL not only synchronizes with time server immediately but also stores the configurations. After pressing the synchronize button, a warning screen will appear.
   (3) There are two different behaviors when configuring the date and time.
      (a) If users only change the time zone and daylight saving but don't change the original time and date. The new time and date will be updated based on the new time zone and if it is in the daylight saving period.
      (b) If users change the time or date, no matter if users change the time zone and daylight saving, ZyWALL will store the new date and time directly, regardless of the time zone and daylight saving which were configured by the user.
   (4) In Daytime and Time protocol process, set the TCP connection timeout as 6 seconds.
   (5) In NTP protocol process, every time server in ZyWALL's default time server list is tried 3 times at most.
5. [ENHANCEMENT]
   In eWC→HOME,
   (1) Let text boxes of 'current time' and 'current date' looked like labels.
   (2) Changed the wording from "NAT Session" to "NAT Concurrent Session".
6. [BUG FIX]
   Symptom: Router will crash.
   Condition: Use CI command "ip urlfilter webControl cache timeout"
7. [BUG FIX]
   Symptom: SMT menu 25 shows 6 more policy route entries than predefined entry number.
   Condition:
   (1) Login SMT and go to menu 25
   (2) Press Next Page until the last page
   (3) Assume we define 24 as policy route rule number, we will see 30 rules on the last page.
8. [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.
9. [ENHANCEMENT]
   In eWC→MAINTENANCE→Time and Date:

(1) Changed the warning message displayed when router is synchronizing with Time Server.
(2) Removed the data format for current time and current date.
(3) Added a note for reminding users of that "Time Server Address" is Optional. There is a pre-defined NTP time server list.

10. [ENHANCEMENT]
    The ZyWALL now also records the time server address (domain name or IP address) in the time synchronization result (successful or failed) logs.
11. [BUG FIX]
    Symptom: After successful time synchronization with LAN side NTP server, the "Destination" IP address for LOG message "Time initialized by NTP server" is WAN IP address.
    Condition:
    (1) Go to eWC→MAINTENANCE→Time Setting
    (2) Choose "Time Protocol" as "NTP(RFC-1305)"
    (3) Setup "Time Server Address" as a server located at LAN side.
    (4) Click Apply and then press "Synchronize Now".
    (5) Go to eWC→LOGS→View Log, will see a log "Time initialized by NTP server" where the "Destination" address is router's WAN IP address, it should be router's LAN IP address.
12. [FEATURE CHANGE]
    Was: When user access web sites which is in LAN IP alias or DMZ, content filter will check these traffic need to block or not.
    Is: Content filter does not block web traffic if the web site is in router's LAN/LAN IP Alias/DMZ.
13. [BUG FIX]
    Symptom: Some trusted web sites' pictures cannot be seen.
    Condition:
    (1) In "eWC→CONTENT FILTER→Customization", select "Disable all Web traffic except for trusted Web sites" and "Don't block Java/ActiveX/Cookies/Web proxy to trusted Web sites".
    (2) At the same page, add "kobeoffshore.com" to "Trusted Web Sites".
    (3) Open web browser to access "kobeoffshore.com".
    (4) All the pictures cannot be seen.
14. [BUG FIX]
    Symptom: The router crashes after the user configures the log setting.
    Condition:
    (1) Go to eWC→LOGS→Log settings page.
    (2) Configure Mail Server, Mail Subject, Send log to, Active Syslog Logging fields and choose all check boxes under "Send Immediate Alert".
    (3) Connect WAN1 to network.
    (4) The system will crash after getting DHCP address.
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. [ENHANCEMENT]
If the Local/Remote Address Type is "Subnet Mask", the "Local/Remote IP Address" in VPN summary table must be like "1.1.1.1 / 255.0.0.0".
WAS: "1.1.1.1 - 255.0.0.0"
IS: "1.1.1.1 / 255.0.0.0"
17. [BUG FIX]
Symptom: In SSH connection, if users paste a large number data into CI command then the system will crash.
Condition:
(1) Create SSH connection.
(2) Enter the CI command mode.
(3) Paste a large number data as command.
(4) The system will crash.
18. [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.
19. [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.
For centralized log:
Was: The blocked log displays "domain" in the message filed.
Is: The blocked log display <domain>: <reason> in the message files. The wording of reasons contains:
(1) "Waiting content filter server timeout"
(2) "DNS resolving failed"
(3) "Creating socket failed"
(4) "Connecting to content filter server fail"
(5) "License key is invalid"
For block message:
Was: The blocked page only shows a deny message if the license key of external content filter is invalid.

Is: The blocked page will show <Deny message> : "License key is invalid" in this case.

20. [FEATURE CHANGE]
    Give different returned error message between timeout and invalid license in eWC→CONTENT FILTER→Categories→Test Against Internet Server
    Was: It returns "Request error" if the license key of external content filtering is invalid or the request is timeout.
    Is:
    (1) It returns "Request timeout" if the request is timeout
    (2) It returns "License key is invalid" if the license key is invalid.
21. [BUG FIX]
    Symptom: Router will crash.
    Condition:
    (1) In eWC→CONTENT FILTER→General, select "Enable Content Filter" and click "Apply"
    (2) In eWC→CONTENT FILTER→Categories, select "Enable External Database Content Filtering" and at least one category in "Select Categories". Click "Apply" after selection.
    (3) Open web browser and access a web site which belongs to 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.
22. [BUG FIX]
    Symptom: No firewall checking when using dial backup connection.
    Condition:
    (1) Setup dial backup environment.
    (2) Enable firewall and block WAN to WAN traffic.
    (3) Pull out the WAN line and make dial backup turn on.
    (4) Try to FTP to firewall WAN ip address from outside workstation.
    (5) Firewall will not block the ftp connection.
    Note: to enable Firewall checking for Dial Backup, please re-configure and save Dial Backup configuration again.
23. [BUG FIX]
    Symptom: Content filter cannot work under traffic redirect.
    Condition:
    (1) Set router's traffic redirect check point as a PC or router in LAN or DMZ
    (2) Force router to traffic redirect.
    (3) All web traffic will bypass content filter.
24. [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: static rule with wrong phase 2 ID.

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.

25. Symptom: Responder will jump to wrong rule when phase 1 parameter of current rule is wrong.
    Condition: There is one rule in initiator and three rules in responder.
    Initiator:
    Rule 1==> Negotiation mode = pre-shared key. Encapsulation mode = Tunnel mode.
    Responder:
    Rule 1==> Negotiation mode = Certificate. Encapsulation mode = Tunnel mode.
    Phase 2 local ID is wrong.
    Rule 2==> Negotiation mode = pre-shared key. Encapsulation mode = Transport mode.
    Phase 2 local ID is wrong.
    Rule 3==> Negotiation mode = pre-shared key. Encapsulation mode = Tunnel mode.
    Phase 2 ID is correct. (This rule should be chosen eventually).
    When trigger tunnel from initiator, responder will use Rule 1 to negotiate and then jump to Rule 2. And eventually tunnel won't be up because initiator ID mismatches during phase 2 negotiation.
26. [BUG FIX]
    Symptom: Firewall eWC available service only shows max 60 entries, including predefined ports(services) and custom ports. Currently there are 43 predefined ports. If user defines more than eighteen custom ports, some of the predefined ports will not be on the eWC list.
    Condition:
    (1) There are 43 predefined ports on the firewall eWC available services.
    (2) Add more than 18 custom ports. Some of the predefined ports will not be on the eWC list.
27. [BUG FIX]
    Symptom: CI command error, ZyWALL will show some CI commands which don't belong to current command set.
    Condition:
    (1) Go to SMT 24.8, CI command mode.
    (2) Type "ip dns system", ZyWALL will correctly print two available commands, "edit" and "display".
    (3) Type "ip dns sys", ZyWALL will unexpectedly print nine available commands instead of two. Those extra seven commands are not under "ip dns system".
28. [BUG FIX]
    Symptom: DHCP client cannot get address from router.
    Condition:
    (1) In eWC→LAN→LAN, configure router as a DHCP server and set IP pool starting address as 192.168.1.33
    (2) In eWC→LAN→Static DHCP, configure all rules in static DHCP table and the IP addresses are 192.168.1.33~192.168.1.40.
    (3) Use a PC which MAC address is not in the static DHCP table to get a IP address from router.
    (4) The PC cannot get the IP address.

29. [BUG FIX]
    Symptom: The ZyWALL will reset the current eWC HTTP session even when the LAN IP configuration is not successfully changed. Under this situation, users have to re-log in the ZyWALL.
    Condition:
    (1) Log in ZyWALL eWC, and go to eWC→LAN.
    (2) Deliberately configure the LAN IP address as within the WAN subnet.
    (3) Click Apply, then the status will show an error message indicating address conflict.
    (4) The ZyWALL will then automatically break the current eWC HTTP session. To access the ZyWALL, users have to log in again.
30. [ENHANCEMENT]
    Support Intel 16Mbytes Flash ROM.
31. [ENHANCEMENT]
    In WC→LAN→Port Roles and eWC→DMZ→Port Roles :
    (1) When users change port roles. ZyWALL needn't be rebooted.
    (2) Add a waiting page to warn users that the ZyWALL is re-configuring its hardware, and during this period, users might not access ZyWALL momentarily.

Modifications in V3.62(WZ.0)b3 | 02/16/2004

1. [FEATURE CHANGE] Extend eWC→static route number from 30 to 50
2. [FEATURE CHANGE] Change eWC→policy route number from 72 to 48
3. [FEATURE CHANGE] Extend rule number in eWC→SUA/NAT→SUA Server from 30 to 50.
4. [FEATURE CHANGE] Extend NAT session number from 2,048 to 10,000
5. [FEATURE CHANGE] Extend Firewall max rule number from 100 to 200
6. [FEATURE CHANGE] Extend Cerberian content filter max connection number from 20 to 50
7. [FEATURE CHANGE] Extend number of classes from 20 to 50 for Bandwidth Management
8. [FEATURE CHANGE] Extend number of filters from 20 to 50 for Bandwidth Management
9. [FEATURE CHANGE] Extend max depth of classes in the tree from 1 to 3 for Bandwidth Management
10. [FEATURE CHANGE] Extend Certificate buffer size from 32K to 64K
11. [ENHANCEMENT]
    Support wireless driver B100+B120+G100
12. [ENHANCEMENT]
    Content filter supports to block two kinds of special URL.
    (1) URL has the '@' sign. For example, http://zyxel@209.247.228.201
    (2) IP address is transfered to decimal. For example, http://209.247.228.201 ==> http://3522684105
13. [ENHANCEMENT]
    Enhance fatal error log. When a fatal error occurs, system will reboot. In the past, there is no useful information before rebooting. Now, there will be some error logs shown on

console before system reboots.

14. [BUG FIX]
    Symptom: SMT Menu 27.1.1 "Peer ID Type" behavior is wrong when authentication method is pre-shared key.
    Condition:
    (1) In Menu 27.1.1, change "Peer ID Type". For example, change "Peer ID Type" from IP to DNS.
    (2) Go to Menu 27.1.1.1
    (3) Go back to Menu 27.1.1 by pressing "Esc" button.
    (4) "Peer ID Type" is still "IP" , which should be "DNS" in this case.
15. [BUG FIX]
    Symptom: SSH can't restrict server access.
    Condition: In eWC-->Remote Management-->SSH: Whatever users choose in "Server Access", users can always access server in any interface.
16. [ENHANCEMENT]
    The centralized log mechanism will merge repeated content filter license error logs into a single log, instead of showing the log repeatedly.
    Note: System will count the number of repeated content filter license error logs, and append this information to the log message.
17. [BUG FIX]
    Symptom: If there are more than 10 VPN tunnels, the 10th tunnel in Current IPSec Security Associations table (eWC>Home>VPN Status) will be covered by the bottom frame.
    Condition:
    (1) Open eWC.
    (2) Go to "Home" page.
    (3) Click VPN Status button.
    (4) If there are more than 10 VPN tunnels, the 10th tunnel in Current IPSec Security Associations table will be covered by the bottom frame.
18. [BUG FIX]
    Symptom: IKE negotiation will success when PFS parameter is different between Initiator and Responder.
    Condition:
    (1) Initiator has only one rule without PFS.
    (2) Responder has only one rule with PFS parameter is DH1.
    (3) Initaitor dial to Responder.
    (4) Tunnel establishment will success, but should fail in this case.
19. [BUG FIX]
    Symptom: EWC wording error.
    Condition: In eWC -> "Login" page -> "Replace Factory Default Certificate" page: wording "Ingore" spelling error.
20. [BUG FIX]
    Symptom: EWC wording error.
    Condition: In eWC -> "MAINTENANCE" page -> "Time Setting" page: wording "Dalight" spelling error.
21. [BUG FIX]

Symptom: EWC cannot show correct NAT session usage in "HOME" page of backup line mode.
Condition:
(1) Switch active WAN to WAN2 or Dial Backup in backup line mode.
(2) In eWC -> "HOME" page, the NAT session usage is incorrect.

22. [BUG FIX]
    Symptom: Router will reply the ping packet on behave of the NAT default server located on LAN.
    Condition:
    (1) Set NAT default server IP address to an address on LAN.
    (2) Ping from WAN side to the NAT default server IP address.
    (3) Router will reply the ping on behave of the NAT default server, which then never receives the ping packet and thus never replies it.
23. [BUG FIX]
    Symptom: In ZW35 eWC home page, the NAT session is always 2048.
    Condition: When ZW35 boots up, the NAT session number is always 2048.
24. [BUG FIX]
    Symptom: In eWC, the system cannot display the login page when the eWC connection has timed out (or disconnected) and the user clicks on an eWC button.
    Condition:
    (1) Log in eWC.
    (2) Enter console mode to disconnect eWC.
    (3) Click buttons, such as Apply and Refresh, in eWC.
    (4) The browser will show "Object Not Found".
25. [BUG FIX]
    Symptom: In the SMT menu 11 and eWC, the user cannot assign the Ethernet static IP of the WAN2.
    Condition:
    (1) Log in SMT.
    (2) Enter menu 11 to configure WAN2.
    (3) Configure a Ethernet static IP in the menu 11.3
    (4) The router cannot store this configuration.
26. [BUG FIX]
    Symptom: PC can't setup TCP connections via ZyWall to the internet when ZyWALL's WAN encapsulation is PPTP.
    Condition:
    (1) Set WAN encapsulation with PPTP.
    (2) Setup a TCP connection to the internet. For example : Use browser to create an HTTP connection.
    (3) Browser won’t retrieve any information because ZyWALL always resets TCP connections.
27. [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)".

28. [ENHANCEMENT]
    (1) Re-layout the zw35 Port Roles pages to fix the out of alignment problem when users set Windows OS font size to "Large".
    (2) Modify the CSS by adding IP field width to fix the problem that the IP Address field will become two lines when users set Windows OS font size to "Large".
29. [BUG FIX]
    Symptom: X-Auth behavior in VPN rule setting page isn't correct.
    Condition:
    (1) eWC-->VPN-->Extended Authentication: Do not select "Enable Extended Authentication" (X-Auth is disabled).
    (2) Select "Client mode" and keep "User name" and "Password" empty.
    (3) VPN rule can't be saved and message "Both User Name and Password are required " shows on "Status".
30. [BUG FIX]
    Symptom: On IE, the BWM (Bandwidth Management) tree view can be expanded and collapsed. But on Mozilla, BWM tree can't be expanded or collapsed.
    Condition:
    (1) Go to eWC>BW MGMT>Class Setup
    (2) If there is no any sub-class, use the 'Add Sub-Class' button to add one.
    (3) Go back to eWC>BW MGMT>Class Setup, click the hyperlink in BWM tree, the tree can't be expanded.
31. [ENHANCEMENT]
    (1) After the ZyWALL sends an update request to DDNS server and receives a return code from DDNS server, the ZyWALL will record the return code in centralized log.
    (2) The IP address of the last update request will be recorded in centralized log.
    (3) Once the user changes the hostname in the SMT menu 1.1 or Web, ZyWALL will send an update request to DDNS.
    (4) When the ZyWALL receives an error code from the DDNS server, ex: "badauth", "nohost", "abuse", it will stop updating.
    (5) When the user chooses the option (Let the DNS server auto detect the IP Address) to use CheckIP (Server Auto Detect) to determine the current IP address, the request string to checkip.dyndns.org sent by the ZyWALL is ended with "CRLF CRLF".
    (6) By DyDNS.org's abuse policy, the force update period is changed from 5 days to 28 days.
    (7) Let wordings in SMT1.1 and the DDNS web page to be consistent.
32. [BUG FIX]
    Symptom: The ZyWALL will send updates when the user has not entered a userid or password or all host names.
    Condition: Set a userid or password or host names as empty one in the SMT menu 1.1 or Web.
33. [BUG FIX]
    Symptom: Fixed a wording error "domian name" in eWC>CONTENT FILTER>Categories.
    Condition:
    (1) Go to eWC>CONTENT FILTER>Categories>Test Web Site Attribute>Test Web

Site Attribute (an edit box).
(2) The words next to the edit box is mis-spelled as "Domian name".

34. [BUG FIX]
    Symptom: Fixed a wording error "DNS Server" in eWC>WAN>DDNS.
    Condition:
    (1) Go to eWC>WAN>DDNS>IP Address Update Policy> DNS server auto detect IP Address(a radio button). Or go to SMT1.1>DNS Server Auto Detect IP Address.
    (2) The words "DNS server" in "DNS server auto detect IP Address" should be "DDNS server".
35. [BUG FIX]
    Symptom: Router will crash.
    Condition:
    (1) A host connects to router.
    (2) User accesses website then disconnect.
    (3) After 2 hours, user accesses website again.
36. [BUG FIX]
    Symptom: In eWC->UPnP->UPnP Setup, the "Note: For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP." is missing, the <HR> is missing, the Apply and Reset buttons are aligned left.
    Condition:
    (1) Go to eWC->UPnP->UPnP Setup page.
    (2) "Note: For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP." is missing.
    (3) <HR> HTML line is missing.
    (4) Apply and Reset buttons are aligned left on this page.
37. [BUG FIX]
    Symptom: LAN host cannot access Internet.
    Condition: When one host continuously tries to setup a new connection, sometimes it fails and the host never can access Internet.
38. [ENHANCEMENT]
    Pause console display when the NAT session information fills a console screeen.
39. [BUG FIX]
    Symptom: Console hangs when editing VPN rule at SMT menu 27.1
    Condition:
    (1) Go to SMT menu 27.1 and edit a new rule.
    (2) Leave "Name" field blank, enter "Edit IKE Management Setup" directly.
    (3) Press ESC return to previous menu.
    (4) Console hangs.
40. [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 a very long time.
    (3) System will run out of memory and become very unstable.
41. [BUG FIX]
    Symptom: Warning message of the SMT11 and WAN web page is wrong.

Condition:
(1) Configure WAN1 IP address to be a static IP address in the SMT11.3 or WAN web page.
(2) Confinue to configure WAN2 IP address to be a static IP address that is in the same network with LAN or DMZ or WAN1.
(3) The warning message of the SMT or WEB will keep appearing "WAN must not be on same subnet as LAN" even it may be in the same network with WAN1 or DMZ.

42. [BUG FIX]
Symptom: Internet access wizard is always opened in the Ethernet mode.
Condition:
(1) Go to eWC>Home>Inter net Access Wizard or eWC>WAN>WAN1 and configure settings as the PPTP or PPPoE mode.
(2) Go back to eWC>Home>Wizard and click the Internet Access button.
(3) Wizard always display in Ethernet mode no matter ZyWALL is in PPTP/PPPoE.
43. [BUG FIX]
Symptom: Internet access wizard displays the wrong value of remote IP/subnet mask in PPTP/PPPoE mode.
Condition:
(1) Go to eWC>Home>Internet Access Wizard or eWC>WAN>WAN1 and configure PPTP's My IP Address.
(2) Go back to eWC>Home>Wizard and click the Internet Access button.
(3) Change to PPTP mode.
(4) Remote IP/subnet mask of PPTP/PPPoE mode are different from eWC>WAN>WAN1 and SMT11.1.
44. [BUG FIX]
Symptom: eWC>LOGS>Log Settings,E-mail Log Settings, if Log Schedule = None, the "Day for Sending Log" option is not grayed out.
Condition:
(1) Go to eWC>LOGS>Log Settings>E-mail Log Settings on Netscape, Mozilla or Firebird.
(2) The checkbox 'Day for Sending Log' needs to be grayed out when the checkbox 'Log Schedule' is not chosen as 'weekly'.
45. [BUG FIX]
Symptom: Router crashed and reboot when editing SMT menu 3.5
Condition:
(1) Insert WLAN card, then restart router.
(2) In CI command, enter "wlan active 11" instead of "wlan active 1" to active WLAN on router.
(3) Enter SMT 3.5, router crashed and reboot.
46. [BUG FIX]
Symptom: ZyWALL cannot establish IPSec connection to SSH Sentinel.
Condition: When ZyWALL and Sentinel both enable XAUTH, the IKE negotiattion will fail.
47. [BUG FIX]
Symptom: IPSec XAUTH cannot work with SoftRemote version 8.0.0
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.

48. [FEATURE CHANGE]
    Modify wireless channel ID mapping table with Country code setting.
49. [FEATURE CHANGE]
    Modify the Time & Date setting policy.
    (1) Wording in SMT menu 24.10: Time Protocol= None -> Manual.
    (2) Only under Manual mode, users can set the New Time & New Date.
    (3) If users change the Time Zone without modifying the New Time or New Date, the system time will automatically be shifted according to new Time Zone.
    (4) If users change the Time Zone and also modify the New Time or New Date, the system time will be updated to the New Time and New Date, disregarding the new Time Zone.
    Note: This enhancement only works in SMT24.10 now.
50. [BUG FIX]
    Symptom: Router will crash.
    Condition: When using "ip nat hash" command, router will crash.
51. [BUG FIX]
    Symptom: When the Ethernet chip VT6105 operates under Half Duplex mode, its TX functionality might hang permanently due to severe collisions.
    Condition:
    (1) Connect the ZW35 WAN1 (or LAN 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 ZW35 WAN1 port (or LAN port) continuously transmit a lot of packets.
    (4) After an indefinite time period, the ZW35 WAN1 port (or LAN port) might permanently fail to transmit packets, as a result of too severe collisions.
52. [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.
53. [BUG FIX]
    Symptom: Rule swap failed when NAT-Traversal is on.
    Condition:
    (1) Initiator setup one NAT-Traversal rule and transport encapsulation mode.
    (2) Responder setup two NAT-Traversal rules, the first is tunnel mode, and the second is transport mode.
    (3) Initiator starts to establish connection for the transport mode rule.
    (4) IKE negotiation will fail.
54. [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.

55. [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".
56. [FEATURE CHANGE]
Change behavior when router detects that the external content filter's license key is invalid.
Was: Disable external content filter and add a centralized log "Content filter's license key expired! disable web control."
Is: Don't disable external content filter and add a centralized log "External content filtering's license key is invalid."
57. [FEATURE CHANGE]
When user registers external content filter, the traffic will not be blocked by "blocking JAVA" option.
Was: When user registers external content filtering and content filter's "blocking JAVA" option is selected, the traffic will be block by content filtering.
Is: The web traffic to content filter's registration site is always forwarded by content filtering.
Note: The protection does not work when system's DNS servers are not set properly.
58. [ENHANCEMENT]
Implement the timeout mechanism on content filter's local cache. Once the cache entry is timeout, it will be delete.
Note: User can set the cache time via CI command "ip urlfilter webControl cache timeout". The unit of setting is hour. Router checks whether there are timeout entries every 30 minutes.

Modifications in V3.62(WZ.0)b2 | 01/13/2004

1. [BUG FIX]
Symptom: Configure VPN rule at eWC fails
Condition:

(1) Edit an VPN rule, choose Certifiacte authentication method and E-mail as Peer ID Type.
(2) Fill in the Content field with peer's E-Mail ID Content value generated by default certificate.
(3) eWC will show "The maximum ID Content length of DNS or E-Mail is 32 characters" at Status bar.

2. [ENHANCEMENT] On Log Settings page (Send Log - Time for Sending Log), added range check for time format.
3. [BUG FIX] In eWC Firewall->Threshold, the field 'Deny new connection request for ... minutes' can't store the value 256. And also added a range checking in the fix.
4. [ENHANCEMENT] Added a blank space in Perfect Forward Secrecy(PFS) of VPN - VPN RULE - EDIT - ADVANCED.
5. [BUG FIX]
   Symptom: Nat incikeport command can not work in autoexec.net.
   Condition:
   (1) Goto SMT 24.8
   (2) Type "sys edit autoexec.net" and add "ip nat incikeport enif1 on" after "ip nat lookback on".
   (3) Reboot ZyWall
   (4) After reboot, the error message "The nat table of iface enif1 is not allocated" will pop up.
6. [ENHANCEMENT] Add a new firewall service type - Roadrunner(TCP/UDP:1026)
7. [BUG FIX]
   Symptom: Content filter cannot block cookie content for some web sites.
   Condition:
   (1) Enable "block cookie" in eWC.
   (2) Access http://www.tomshardware.com from PC.
   (3) PC has cookie contents which are written from the web site. The cookie contents should be blocked by router.
8. [BUG FIX]
   Symptom: When system's WAN mac is changed to any PC's mac attached on LAN, LAN traffic will be blocked and can not access Internet for a period of time.
   Condition:
   (1) Change system's WAN mac to any PC's mac attached on LAN.
   (2) PC ping system's LAN IP.
9. [BUG FIX]
   Symptom: HOME/Internet Access , the Ethernet service type is always "Standard", and can not set other service type
   Condition:
   (1) In eWC, HOME->Internet Access
   (2) Choose Ethernet encapsulation and change service type
   (3) After refreshing page, service type was not be changed
10. [BUG FIX]
    Symptom: In eWC, HOME->Internet Access , the ethernet fixed ip address is always 0.0.0.0
    Condition:

(1) Goto eWC->WAN, setup a fixed up with Ethernet Encapsulation
(2) Goto HOME->Internet Access, Press Next
(3) IP address is always 0.0.0.0, it should be IP address configured in step 1

11. [BUG FIX]
    Symptom: In eWC, HOME->Internet Access , the default Login Server IP Address of Ethernet service type RR-Toshiba / RR-Manager / RR-Telstra is "0.1.0.0"
    Condition:
    (1) Goto eWC->HOME->Internet Access.
    (2) Choose Enternet nncapsulation and service type RR-Toshiba / RR-Manager / RR-Telstra
    (3) The default Login Server IP is 0.1.0.0
12. [BUG FIX]
    Symptom: The "Show Statistics" button is missing on eWC->HOME page
    Condition:
    (1) Goto eWC->HOME
    (2) "Show Statistics" button is missing.
13. [BUG FIX]
    Symptom: Router will display "File size is changing: done" everytime the router is rebooting.
    Condition:
    (1) Reboot system.
    (2) Router will display "File size is changing: done" even without processing rom convert.
    (3) It happens everytime when rebooting system.
14. [ENHANCEMENT]
    Add GUI for the new feature of configurable port setting. Using this new feature, users can dynamically set LAN/DMZ port roles.

Modifications in V3.62(WZ.0)b1 | 12/29/2003
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
                  Secure Client IP = 0.0.0.0
FTP Server:       Port = 21        Access = ALL
                  Secure Client IP = 0.0.0.0
SSH Server:       Certificate = auto_generated_self_signed_cert
                  Port = 22        Access = ALL
                  Secure Client IP = 0.0.0.0
HTTPS Server:     Certificate = auto_generated_self_signed_cert
                  Authenticate Client Certificates = No
                  Port = 443       Access = ALL
                  Secure Client IP = 0.0.0.0
HTTP Server:      Port = 80        Access = ALL
                  Secure Client IP = 0.0.0.0
SNMP Service:     Port = 161       Access = ALL
                  Secure Client IP = 0.0.0.0
DNS Service:      Port = 53        Access = ALL
                  Secure 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.

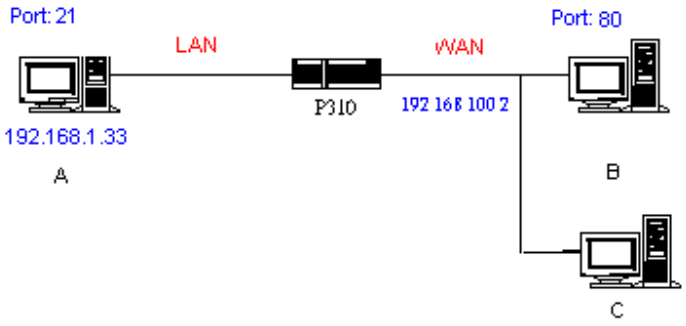
These triggered events can be timed so that they erase the port mapping as soon as they are done with the data transfer, so that the port mapping can be triggered by another Client computer. This gives the ***illusion*** that multiple computers can use the same port mapping at the same time, but the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

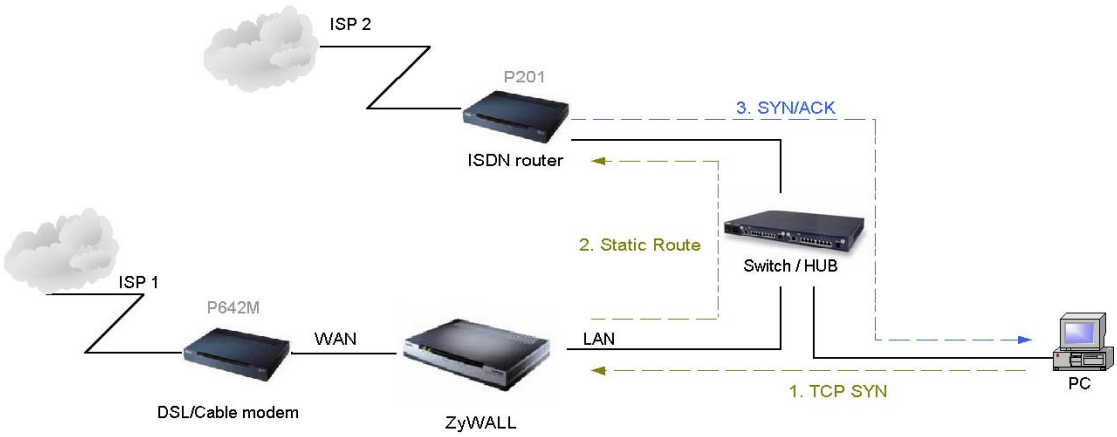


Figure 5-1 Triangle Route

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.

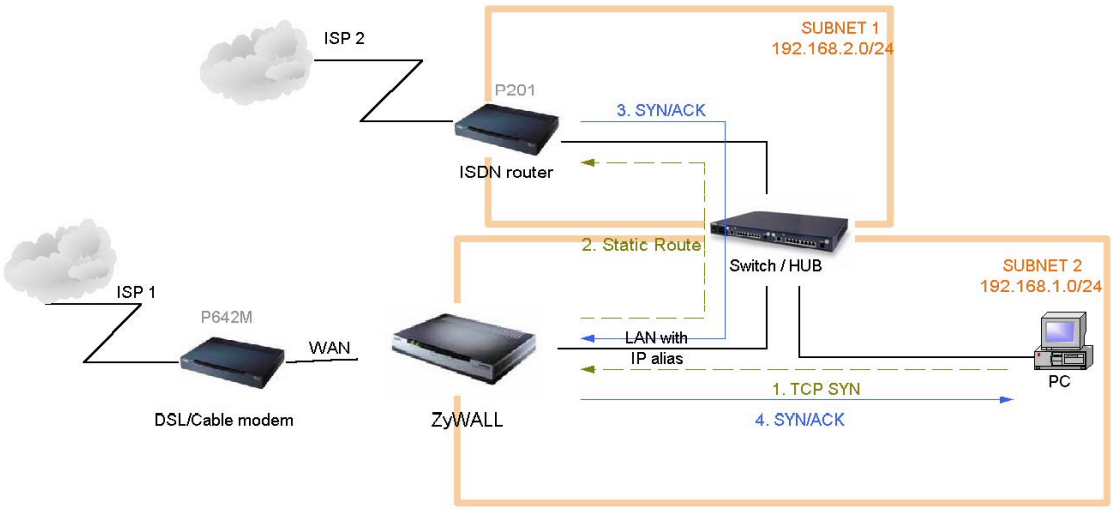


Figure 5-2 Gateway on alias IP network

(2) Gateway on WAN side

A working topology is suggested as below.

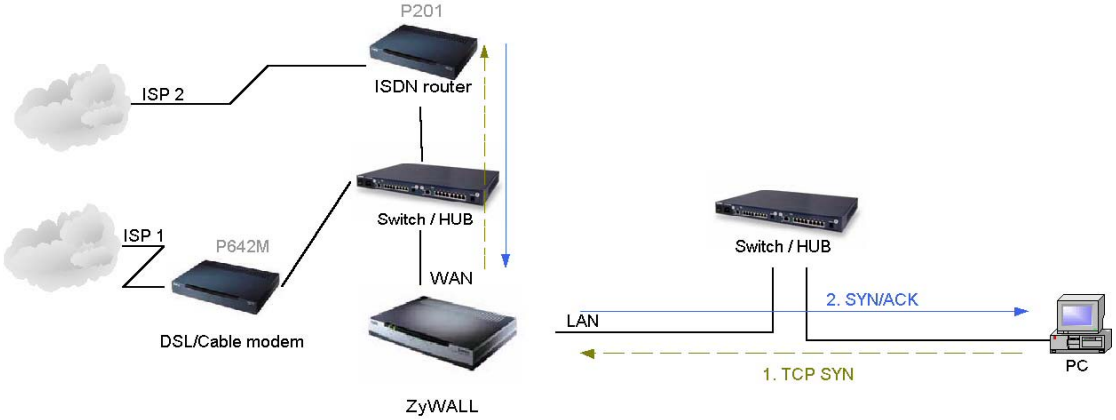


Figure 5-3 Gateway on WAN side

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.

Appendix 9 IPSec IP Overlap Support

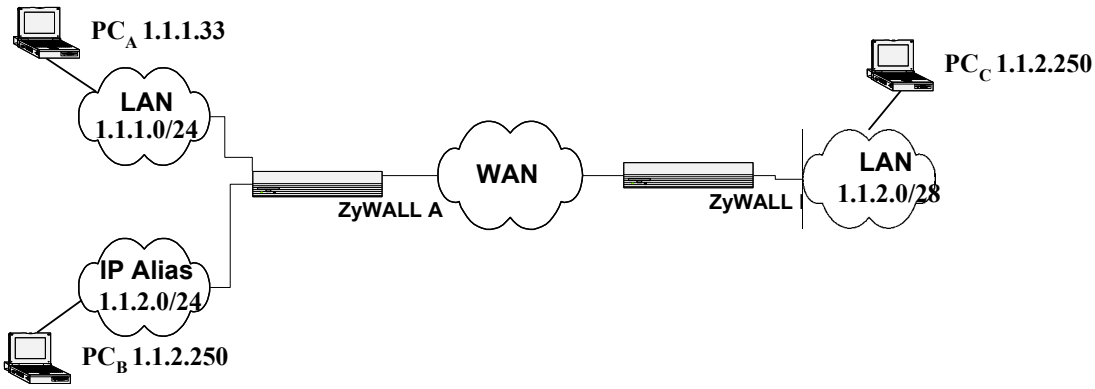


Figure 1

The ZyWALL uses the network policy to decide if the traffic matches a VPN rule. But if the ZyWALL finds that the traffic whose local address overlaps with the remote address range, it will be confused if it needs to trigger the VPN tunnel or just route this packet.

So we provide a CI command "ipsec swSkipOverlapIp" to trigger the VPN rule. For example, you configure a VPN rule on the ZyWALL A as below:

Local IP Address Start= 1.1.1.1 End= 1.1.2.254
Remote IP Address Start= 1.1.2.240 End = 1.1.2.254

You can see that the Local IP Address and the remote IP address overlap in the range from 1.1.2.240 to 1.1.2.254.

(1) Enter "ipsec swSkipOverlapIp off":
To trigger the tunnel for packets from 1.1.1.33 to 1.1.2.250. If there is traffic from LAN to IP Alias (Like the traffic from PC_A to PC_B in Figure 1), the traffic still will be encrypted as VPN traffic and routed to WAN, you will find their traffic disappears on LAN.
(2) Enter "ipsec swSkipOverlapIp on":
Not to trigger the tunnel for packets from 1.1.1.33 to 1.1.2.250. Even the tunnel has been built up, the traffic in this overlapped range still cannot be passed.

[Note]
If you configure a rule on the ZyWALL A whose
Local IP Address Start= 0.0.0.0
Remote IP Address Start= 1.1.2.240 End = 1.1.2.254
No matter swSkipOverlapIp is on or off, any traffic from any interfaces on the ZyWALL A will match the tunnel. Thus swSkipOverlapIp is not applicable in this case.

Appendix 10 VPN Local IP Address Limitation

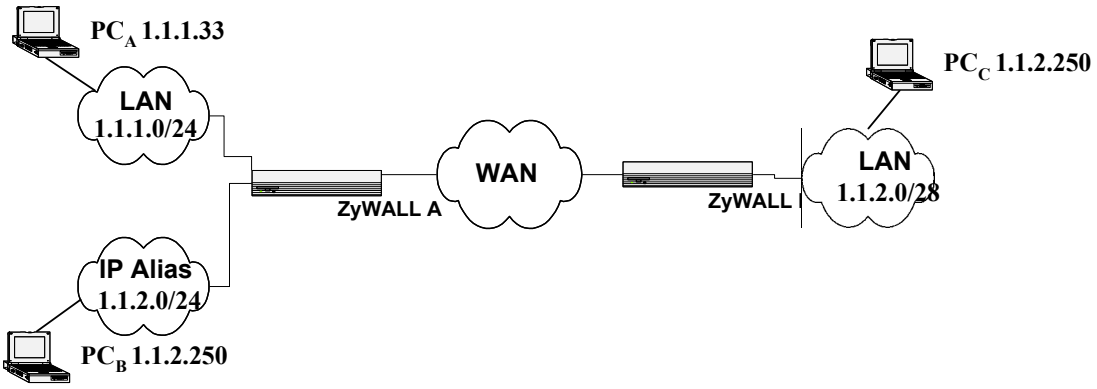


Figure 1

There is a limitation when you configure the VPN network policy to use any Local IP address. When you set the Local address to 0.0.0.0 and the Remote address to include any interface IP of the ZyWALL at the same time, it may cause the traffic related to remote management or DHCP between PCs and the ZyWALL to work incorrectly. This is because the traffic will all be encrypted and sent to WAN.

For example, you configure a VPN rule on the ZyWALL A as below:

Local IP Address Start= 1.1.1.1 End= 1.1.2.254
Remote IP Address Start= 1.1.2.240 End = 1.1.2.254

ZyWALL LAN IP = 1.1.1.10

ZyWALL LAN IP falls into the Local Address of this rule, when you want to manage the ZyWALL A from $PC_{A,}$ you will find that you cannot get a DHCP Client IP from the ZyWALL anymore. Even if you set your IP on PC_A as static one, you cannot access the ZyWALL.

Appendix 11 VPN rule swap limitation with VPN Client on XAuth

Example 1:

ZyWALL (WAN)---------- VPN Client
(IP:1.1.1.1) (IP:1.1.1.2)

ZyWALL VPN Rule: Two IKE rule	
➢ Dynamic IKE rule: Security Gateway: 0.0.0.0 X-Auth: Server I. Policy one: - Name: "Rule_A" - Local: 192.168.2.0/24 - Remote: 0.0.0.0	➢ Static IKE rule: Security Gateway: 1.1.1.2 X-Auth: None I. Policy one: - Name: "Rule_B" - Local: 192.168.1.0/24 - Remote: 1.1.1.2/32

ZyXEL VPN Client
Security Gateway: 1.1.1.1 Phase one Authentication method: Preshare Key Remote: 192.168.1.0/24

In example 1, user may wonder why ZyWALL swap to dynamic rule even VPN client only set authentication method as “Preshare Key” not “Preshare Key+XAuth”. The root cause is that currently ZyXEL VPN Cient will send XAuth VID no matter what authentication mode that him set. Because of the XAuth VID, ZyWALL will swap to dynamic rule.

This unexpected rule swap result is a limitation of our design. For ZyWALL, when we got initiator’s XAuth VID in IKE Phase One period, we know initiator can support XAuth. To take account of security, we will judge that initiator want to do XAuth, and we will search one matched IKE Phase One rule with XAuth server mode as the top priority. To our rule swap scheme, we search static rule first then dynamic rule. In example 1, we will find the static rule, named “Rule_B”, to build phase one tunnel at first. After finished IKE phase one negotiation, we known initiator want to do XAuth. Since Rule_B has no XAuth server mode, we try to search another rule with correct IKE Phase One parameter and XAuth server mode. The search result will lead us to swap rule to dynamic rule, named “Rule_A”. Thus to build VPN tunnel will fail by Phase Two local ip mismatch.

To avoid this scenario, the short-term solution is that we recommend user to set two IKE rule with different Phase One parameter. The long-term solution is that VPN Client needs to modify the XAuth VID behavior. VPN Client should not send XAuth VID when authentication method is “Preshare key”, but send XAuth VID when authentication method is “Preshare key+XAuth”.

Annex A CI Command List

Last Updated: 2003/11/03

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	Bandwidth Management
Firewall Related Command	Certificate Management (PKI) Command	Load Sharing Command
Bridge Related 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	mail schedule policy

			[0:full/1:hourly/2:daily/3:weekly/4:none]	
			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.
		consolidate		
			switch <0:on|1:off>	active to enable log consolidation
			period	consolidation period (seconds)
			msglist	display the consolidated messages
		switch		
			bmlog <0:no|1:yes>	active to enable broadcast/multicast log
			display	display switch setting
			trilog <0:no|1:yes>	active to enable triangle route log
	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. State: process state. Pri: priority, a_usg: accumulated cpu usage, p_usg: profiling cpi usage.(take count after do clear command). Size: (lowest available stack size)/(total stack size).
		stack	[tag]	display process's stack by a give TAG

		pstatus		display process's status by a give TAG
		clear		Restart cpu usage measurement. (Result will be in p_usg column from display command.
	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
	support			not support in this product
	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
		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
	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
		mem	<addr> <data> [type]	write memory data in address
	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-timeo		Edit the wait time for the SYN TCP sessions

			ut <seconds>		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
	alg			
		disp		Show ALG enable disable status
		enable	<ALG_FTP|ALG_H323|ALG_SIP>	Enable ALG command
		disable	<ALG_FTP|ALG_H323|ALG_SIP>	Disable ALG command
		siptimeout	<timeout in second> or 0 for no timeout	Configure SIP timeout command
	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 defined(private)> <isp group idx|dns server ip>	insert dns NS record
			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
	Httpd			
		debug	[on|off]	set http debug flag
	icmp			
		echo	[on|off]	set icmp echo response flag

		data	<option>	select general data type
		check		
			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
	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
		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
	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

	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/keywordBl ock/fullPath/caseInsensitive/fileNa me][enable/disable]	set action flags
			logFlags [type(1-3)][enable/disable]	set log flags
			add [string] [trust/untrust/keyword]	add url string
			delete [string] [trust/untrust/keyword]	delete url string
			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			
		active	[0:lan|1:dmz][1:yes|0:no]	active report
		start	[0:lan|1:dmz]	start report
		stop	[0:lan|1:dmz]	stop report
		url	[0:lan|1:dmz] [num]	top url hit list
		ip	[0:lan|1:dmz] [num]	top ip addr list
		srv	[0:lan|1:dmz] [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
			display	display all the timeout values
		update		create nat system information from spSysParam
		iamt	<iface>	display nat iamt information
		lookup	<rule set>	display 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
			sip debug	enable/disable sip debug flag
			sip display	display the sip call buffer

		resetport		reset all nat server table entries
		incikeport	[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
		natTable	[enifX, X=0, 1, 2, …]	show the NAT global information
		simulation	<enifX, X=0, 1, 2, …>	for engineer debug only
		acl		
			display	display all NAT acl set and rule information
			load <set number>	load a specific acl of set number
			save <set number>	save a specific acl of set number
		routing	[0:LAN|1:DMZ] [0:no|1:yes]	set NAT routing attributes
	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
		exUseMode	[enable|disable]	Set exclusive use mode for client tunnel flag
		exUseMac	[MAC address]	Set exclusive use mode for client tunnel MAC address
	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

Firewall Related Command Home

Command					Description
sys	Firewall				
		acl			
			disp		Display specific ACL set # rule #, or all ACLs.
			delete		Delete specific ACL set # rule #.
		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.
		debug			Set firewall debug level.
		disp			Display firewall log
		init			### nothing. ###
		mailsubject			
			disp		Display mail setting which is used to mail alert.
			edit		Edit mail setting.
		online			Set firewall log online.
		pktdump			Dump the 64 bytes of dropped packet by firewall
		tos			
			delete		Delete specific TOS session.
			display		Display TOS sessions.
			status		Display TOS sessions' status.
			dump		Dump TOS.
		tosctrl			
			destination		Display TOS destination hash
			incomplete		Display TOS incomplete List.
		dynamicrule			
			display		Display firewall dynamic rules
		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.

Bandwidth management Related Command

Home

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

						100Mbps.
				<wrr|prr>		Select fairness-based(WRR) or priority-based(PRR) mechanism. the default value is fairness-based.
				<efficient>		Enable work-conserving feature.
			disable			Disable bandwidth management in DMZ
		wlan	enable	<bandwidth xxx>		Enable bandwidth management in WLAN with bandwidth xxx bps. If the user doesn't set the bandwidth, the default value is 100Mbps.
				<wrr|prr>		Select fairness-based(WRR) or priority-based(PRR) mechanism. the default value is fairness-based.
				<efficient>		Enable work-conserving feature.
			disable			Disable bandwidth management in WLAN
	class	lan	add #	bandwidth xxx	<name xxx>	Add a class with bandwidth xxx bps in LAN. The name is for users' information.
					<priority x>	Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The default value is 3.
					<borrow on|off>	The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The default value is off.
			mod #	<bandwidth xxx>		Modify the parameters of the class in LAN. The bandwidth is unchanged if the user doesn't set a new value.
				<name xxx>		Set the class' name.
				<priority x>		Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The priority is unchanged if the user doesn't set a new value.
				<borrow on|off>		The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The borrow is unchanged if the user doesn't set a new value.
			del #			Delete the class # and its filter and all its children class and their filters in LAN.
		wan	add #	bandwidth xxx	<name xxx>	Add a class with bandwidth xxx bps in WAN. The name is for users' information.
					<priority x>	Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The default value is 3.
					<borrow on|off>	The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The default value is off.
			mod #	<bandwidth xxx>		Modify the parameters of the class in WAN. The bandwidth is unchanged if the user doesn't set a new value.
				<name xxx>		Set the class' name.
				<priority x>		Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The priority is unchanged if the user doesn't set a new value.
				<borrow on|off>		The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The borrow is unchanged if the user doesn't set a new value.
			del #			Delete the class # and its filter and all its children class and their filters in WAN.
		dmz	add #	bandwidth xxx	<name xxx>	Add a class with bandwidth xxx bps in DMZ. The name is for users' information.
					<priority x>	Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The default value is 3.
					<borrow on|off>	The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The default value is off.
			mod #	<bandwidth xxx>		Modify the parameters of the class in DMZ. The bandwidth is unchanged if the user doesn't set a new value.
				<name xxx>		Set the class' name.

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

			dmz			Show the filters settings of DMZ
			wlan			Show the filters settings of WLAN
		statistics	lan			Show the statistics of the classes in LAN
			wan			Show the statistics of the classes in WAN
			dmz			Show the statistics of the classes in DMZ
			wlan			Show the statistics of the classes in WLAN
	monitor	lan	<#>			Monitor the bandwidth of class # in LAN. If the class is not specific, all the classes in LAN will be monitored. The first time you key the command will set it on; the second time you will set it off, and so on.
		wan	<#>			Monitor the bandwidth of class # in WAN. If the class is not specific, all the classes in WAN will be monitored. The first time you key the command will set it on; the second time you will set it off, and so on.
		dmz	<#>			Monitor the bandwidth of class # in DMZ. If the class is not specific, all the classes in DMZ will be monitored. The first time you key the command will set it on; the second time you will set it off, and so on.
		wlan	<#>			Monitor the bandwidth of class # in WLAN. If the class is not specific, all the classes in WLAN will be monitored. The first time you key the command will set it on; the second time you will set it off, and so on.
	moveFilter	<channName>	<from>	<to>		User can move BWM filter order via this command.<channName>: lan, wan/wan1, dmz, wan2, wlan<from>: filter index<to>: filter index
	config	save				Save the configuration.
		load				Load the configuration.
		clear				Clear the configuration.

Load Sharing Command Home

Command				Description
ls				
	band	<up|down>	<WAN1 bandwidth+WAN2 bandwidth>	It is used to configure the bandwidth parameters. The CI format is ls band <method(up, down)|WAN1 loading bandwidth |WAN2 bandwidth. Ex: "ls band up 100 200" will configure the Load Sharing function dispatch the loading between WAN1 and WAN2 with 100K and 200K upstream loading.
	wrr		<Weight of WAN1> + <Weight of WAN2>	It is used to configure the weight parameters. The CI format is ls wrr <Weight of WAN1> + <Weight of WAN2>. The valid numver of weight is 0~10 Ex: "ls wrr 10 5" will configure the weight of the WAN1 to be 10, weight of the WAN2 to be 5.
	spillover		< upper bandwidth of primary WAN >	It is used to configure the spillover upper bandwidth of primary WAN. Ex: "ls spillover 100", the router will send the

				traffic to secondary WAN when the primary WAN bandwidth exceeds 100Kbps.
	mode		<1:Least Load First|2:WRR|3:Spillover|255:None>	Change the dispatch mode. 1 is for dispatch packets by Dynamic Load Balancing, 2 is for dispatch packets by WRR, 3 is dispatch packets by Spillover. And 255 is for disable the Load Sharing function.
	timeframe		<10~600>	Change the Time Frame number. The valid number of it is 10~600
	disp			Display the Load Sharing configuration data
	debug			Debug CI commands
		online	<on|off>	To toggle the debug message on or off. This command is useful for debugging.

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