ZyXEL

Firmware Release Note

ZyWALL 5

Release 4.01(XD.1)C0

Date:	**September 04, 2006**
Author:	**Summer Tseng**
Project Leader:	**Steven Chen**

ZyXEL ZyWALL 5 Standard Version release 4.01(XD.1)C0 Release Note

Date: September 04, 2006

Supported Platforms:

ZyXEL ZyWALL 5

Versions:

ZyNOS Version: V4.01(XD.1) | 09/04/2006
Bootbase Version: V1.08 | 01/28/2005
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. When firewall turns from "off" to "on", the firewall initialization procedure will disconnect all connections running through the ZyWALL.
5. SUA/NAT address loopback feature was enabled on ZyWALL by default, however, if users do not need it, a C/I command "ip nat loopback off" could turn it off.
6. 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.
7. When UPnP is on, and then reboot the device, Windows XP will not detect UPnP and refresh “My Network Places→Local Network”. Plug in network wire again can solve this problem.
8. The default port roles for LAN/DMZ setting is: port 1 to port 4 are all LAN ports.
9. In bridge mode, If LAN side DHCP clients want to get DHCP address from WAN side DHCP server, you may need to turn on the firewall rule for BOOT_CLIENT service type in WAN→LAN direction.
10. Under Bridge Mode, all LAN ports will behave as a hub, and all DMZ ports will also

behave as another hub.

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”. (Upgrade from 3.62)
12. 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.
13. In SMT menu 24.1, "WCRD" only represents the WLAN card status when you insert WLAN card into the ZyWALL. If you insert TRUBO card, you will see " WCRD" is always down.
14. If you do not want a mail to be scanned by Anti-Spam feature, you can add this mail into whitelist in eWC->Anti-Spam->Lists
15. If you want traffic redirect feature to work, you should turn on WAN ping check by "sys rn pingcheck 1".
16. The first entry for static route is reserved for creating WAN default route and is READ-ONLY.
17. If you had activated content filtering service but the registration service state is "Inactive"after upgrading to 4.00, please click "Service License Refresh" in "eWC->REGISTRATION->Registration" or wait until device synchronize with the myzyxel.com.

Known Issues:

[UPnP]

1. Sometimes on screen the “Local Area Connection” icon for UPnP disappears. The icon shows again when restarting PC.
2. 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.

[Bandwidth Management]

1. Bandwidth Management doesn’t work on wireless LAN.
2. Bandwidth management H.323 service does not support Netmeeting H.323 application.
3. Using BWM in PPPoE/PPTP mode, there are two filters for FTP and H323 ALG
   (1) If we execute FTP first then H323 cannot pass through ZyWALL.
   (2) If we execute H323 before FTP, all functions work properly.
4. In some cases, BWM (Fairness-Based mode) cannot manage bandwidth accurately. Ex. In WAN interface, there are two subclasses for FTP service, their speed are 100Kbps and 500Kbps, the traffic match the filter which speed is 500Kbps may only use half of it’s bandwidth.

[Content Filter]

1. Can’t block ActiveX in some case. (Sometime the ActiveX block fails. This is because the ActiveX is cached in C:\WINNT\Downloaded Program Files\ If you want to test the ActiveX block functionality. Please clear the cache in windows.)
2. CF Denied Access Message and Redirect URL have not limit sepcial character, it will caused DUT crash.
3. CF Denied Access Message can run script.

[Bridge Mode]
1. 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.
2. Don't use CI command "bridge rstp bridge enable" to enable RSTP, it will change the initial Path Cost value to an incorrect value.

[Wireless]
1. The fragmentation threshold size support between 800~2432.
2. Wireless client still can scan device network after disabling wireless card.

[ALG]
1. Symptom: P2002 can not connect with each other in Peer-to-Peer mode.
   Condition:
   Topology: P2002--(LAN)ZyWALL_A(WAN, IP=172.21.2.151)--(WAN, IP=172.21.1.134)ZyWALL_B(LAN)--P2002
   (1) In ZyWALL_A and ZyWALL_B, add a "WAN to LAN" firewall rule to pass traffic with port "5060".
   (2) In ZyWALL_A and ZyWALL_B, add a port forwarding rule "5060" to P2002.
   (3) In ZyWALL_A and ZyWALL_B, enable SIP ALG.
   (4) Setup both P2002 to Peer-to-Peer mode.
   (5) Making the SIP connection by P2002 will be failed.
   (6) Turn off firewall in ZyWALL_A and ZyWALL_B, sometimes the connnection can be built up if we dial from P2002 which is behind ZyWALL_A.

[Anti-Virus]
1. The log description is not clear if packet if forwarded when exceeding maximun session number.

[Anti-Spam]
1. Symptom: Mail cannot be delivered successfully.
   Condition:
   Topology: Mail Client ----- ZyWALL_A---- ZyWALL_B--- Mail Server
   (1) Turn on Anti-Spam at ZyWALL A and B.
   (2) Mail Client sent mail to Mail Server.
   (3) Sometimes mail cannot be sent or received successfully.
   (4) The situation also happens when mail client receive mail.
2. Mail cannot be passed through in below conditions:
   (1) Through 2 devices with Anti-Spam enabled.
   (2) NAT loopback with Anti-Spam enabled.

[VPN]
1. Symptom: PC can't ping remote gateway through VPN tunnel under this special topology.
   Condition:
   PC------LAN ZyWALL_A WAN----------LAN ZyWALL_B
   WAN-------Internet
   (192.168.1.33）　（192.168.100.33）(192.168.100.1)　　（172.202.77.145)

   (1) VPN configuration in ZyWALL_A:

WAN IP Address=192.168.100.33，WAN IP Subnet Mask=255.255.255.0， Gateway IP Address=192.168.100.1.
Gateway policy，Name=IKE1，Remote Gateway Address=192.168.100.1，Pre-Shared Key=12345678.
Network policy for IKE1，Active=enable，Name=IPSec1，Local Network/Starting IP Address=192.168.1.33，Remote Network/Starting IP Address=0.0.0.0
(2) VPN configuration in ZyWALL_B
WAN IP Address=172.202.77.145，WAN IP Subnet Mask=255.255.0.0，Gateway IP Address=172.202.77.1.
Gateway policy，Name=IKE1，Remote Gateway Address=192.168.100.33，Pre-Shared Key=12345678.
Network policy for IKE1，Active=enable，Name=IPSec1，Local Network/Starting IP Address=0.0.0.0，Remote Network/Starting IP Address=192.168.1.33.
(3) When we established the VPN tunnel between ZyWALL_A and ZyWALL_B, we can access ZyWALL_B (192.168.100.1) with the remote management,
such as Telnet, FTP…, this traffic will go through VPN tunnel. However, we can not ping ZyWALL_B (192.168.100.1) successfully because this ICMP traffic did not go through VPN tunnel to ZyWALL_B.

2. SNMP tools get ZYWALL VPN MIB data, the index of received data are wrong if rules are larger than 1.
3. VPN rule swap does not support NAT Traversal.

[MISC]

1. The DMZ TxPkts counter increment at about 1 pkt/min even without any Ethernet cables ever connected.
4. At SMT24.1, the collisions for WAN, LAN and DMZ port are not really counted.
5. Under PPTP encapsulation mode, we can not access some website like http://www.kimo.com.tw/
6. In eWC->Statistics, Tx data for Dial Backup is not correct.
7. Symptom: LAN host can ping Internet while LAN host change cable from LAN port to DMZ port.
   Condition:
   (1) Host connects to LAN port and gets 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.
7. Symptom: Dial Backup can’t work when Traffic Redirect is enabled.
   Condition:
   (1)Enable Traffic Redirect and Dial Backup
   (2)When disconnect WAN line, the traffic will go through Backup Gateway
   (3)At now, disconnect the Backup Gateway, the Dial Backup modem should be triggered. But it doesn’t.
8. Symptom : After system password hash, downgrade F/W, user can't use GUI
   Condition:
   (1) In patch 6 support password encrypted, CLI "sys pwdEncryption on". "sys md5 1234" will display a string "xxxxxxx"

(2) Downgrade F/W to patch2 (not support password encrypted), SMT can use password "xxxxxxx" login but GUI can't

Features:

Modifications in V4.01(XD.1) | 09/04/2006
Modify for formal release

Modifications in V4.01(XD.1)b1 | 08/29/2006

1. [ENHANCEMENT]
   Support 60 categories in content filtering.
   New categories: ""Hacking", Phishing", "Spyware/Malware Sources", "Spyware Effects/Privacy Concerns", "Open Image/Media Search", "Social Networking", "Online Storage", "Remote Access Tools", "Peer-to-Peer", "Streaming Media/MP3s" and "Proxy Avoidance".

2. [ENHANCEMENT]
   Add second time schedule setting in content filtering

3. [ENHANCEMENT]
   Enhance the CI command "ip ifconfig".
   (1) Add a new argument "mss" to configure the MSS value.
   (2) After finishing the configuration, the interface information will be displayed.
   Usage: ip ifconfig [iface] [ipaddr</mask bits>] <broadcast [addr]> <mtu [value]> <mss [value]> <dynamic> <showoff>
   Ex: ip ifconfig enif1 192.168.70.222/24 broadcast 192.168.70.250 mtu 1500 mss 1460

4. [ENHANCEMENT]
   Add CI command "av zipUnsupport". Processing ZIP file will destroy encrypted file if flag is on, otherwise pass it.

5. [ENHANCEMENT]
   Add a CI command to turn on or off the LDAP packet parsing in NAT module.
   Usage: "ip nat service ldap [on|off]"

6. [BUG FIX]
   Symptom: zywall 5 WAN fixed 100/full negotiation fail against cisco 3550/2900.
   Condition:
   (1) Configure cisco 3550/2900 port to fixed 100/full.
   (2) Configure zywall 5 WAN to fixed 100/full.
   (3) Zywall 5 WAN can not sync up; remain down.

7. [BUG FIX]
   Symptom: The DHCP table shows incorrect information.
   Condition:
   (1) Set the ZyWALL's DHCP IP Pool Starting Address is 192.168.102.146.
   (2) Add a DHCP static IP 192.168.102.22 for a PC on the LAN.

(3) Add another PC on the LAN but this PC doesn't have a corresponding DHCP static IP rule, and then it gets 192.168.102.146 from the ZyWALL.
(4)Go to eWC>Home>DHCP Table, the ZyWALL doesn't show 192.168.102.146, but show 192.168.103.157.

8. [BUG FIX]
   Symptom: The packet will be dropped if the device does not have the ARP entry of the receiver of this packet.
   Condition:
   (1) Clear ARP table by "CI>ip arp flush".
   (2) Send a ping to 168.95.1.1, but the PC will not get a response in the first ICMP Echo Request.
   (3) After the first ping, the rest of pings can get responses.

9. [BUG FIX]
   Symptom: ZyWALL serial cannot connect one CDMA terminal RWT FCT CDMA.24.
   Condition:
   Russia raised this issue that our ZyWALL cannot connect one kind of CDMA terminal RWT FCT CDMA.24, but it is okay when this Terminal connect to P662 and D-Link route. After check, they found when short-circuit the CTR and DTS can make it work (ZyWALL connect to the CDMA)

10. [BUG FIX]
    Symptom: Device crashes because of memory double free in Content Filter.
    Condition:
    (1) Enable Content Filter and Web site customization.
    (2) After a while, the device will crash sometimes.

11. [BUG FIX]
    Symptom: Device crashes when enable CNM agent.
    Condition:
    (1)Enable AV/IDP/CNM.
    (2)Disable AS.
    (3)Block LAN to LAN packet from Firewall.
    (4)Make LAN to LAN heavy traffic.

12. [BUG FIX]
    Symptom: Trace route fails to get response from our device.
    Condition:
    Topology:
    PC-----(LAN)ZW70(WAN)
    (1) On PC, try trace route a host(www.yahoo.com).
    (2) Trace route cannot get response from our device.

13. [BUG FIX]
    Symptom: Device crashes (software watchdog wakes up by NAT).

Condition:
(1) Restore default romfile.
(2) After a while, the device will crash sometimes.

14. [BUG FIX]
Symptom: Backuping the configuration of AntiVirus is too slow.
Condition:
(1) In eWC->SECURITY->ANTI-VIRUS->Backup & Restore, click "Backup" button to backup the AntiVirus configuration.
(2) Sometimes we need to wait for the popup window for a prolonged period of time.

Modifications in V4.01(XD.0) | 08/08/2006
Modify for formal release

Modifications in V4.01(XD.0)b5 | 07/31/2006
1. [BUG FIX]
Symptom: Device crashes when upload F/W.
Condition:
Topology : PC_A == ZyWALL == P1 == PC_B
(1) Build tunnel between PC_A and PC_B and sent TFGEN traffic(1M) between PC_A and PC_B.
(2) Use eWC to upload F/W from ZyWALL's WAN and device crashes.

Modifications in V4.01(XD.0)b4 | 07/11/2006
2. [BUG FIX]
Symptom: Anti-Spam cannot work in NAT loopback situation.
Condition:
(1) Put PC1 and PC2 on LAN side of ZyWALL.
(2) ZyWALL enables Anti-Spam and disables External Database.
(3) PC2 installs the Merak Mail Server.
(4) PC1 uses the outlook express to send mail to itself by the mail server of PC2.
(5) When the PC1 is sending mails will cause mail stuck until timeout.
3. [BUG FIX]
Symptom: Upload firmware by eWC will cause CPU load 100%.
Condition:
(1) Use GUI to upload firmware will cause CPU 100%.
(2) It will be successful, but need more than 1 minute.
4. [BUG FIX]
Symptom: There should be a progress page when upload F/W by eWC.
Condition:
(1) Goto eWC>Maintenance to upload F/W.
(2) ZyWALL should show a progress page, but it is not.
(3) ZyWALL should display login page after reboot, but it is not.

Modifications in V4.01(XD.0)b3 | 06/25/2006
1. [FEATURE CHANGE]

Change log format of Spam mail.
Was: Mail score is higher than threshold - Spam Score:<Score><Title>!<Direction>
Is: Mail score is higher or equal than threshold - Spam Score:<Score><Title>!<Direction>

2. [FEATURE CHANGE]
   Change some wordings which contain "fail back" in GUI and log.
   Was: "Fail back ****".
   Is: "Fall back ****".
3. [FEATURE CHANGE]
   WAS: In eWC>HOME page, the memory bar will become red when the percentage of memory usage is over 90%.
   IS: In eWC>HOME page, the memory bar will become red when the percentage of memory usage is over 95%.
4. [FEATURE CHANGE]
   In eWC>BW MGMT>Class Setup page, change wording:
   WAS: "filter, to filter, (filter number)", "Filter class Search Order"
   IS: "class, to class, (class number)", "Enabled classes Search Order"
5. [ENHANCEMENT]
   Enlarge Anti-Spam session number from 5 to 20
6. [ENHANCEMENT]
   Microsoft cryptographic library supports only odd-sized keys for generating the RSA-modulus. Let the key number of creator primes be odd-size.
   Note: Without this enhancement, importing self-signed certificate with PKCS#12 format into MS IE sometimes will fail.
7. [ENHANCEMENT]
   (1) In eWC>HOME page, show MAC address in Network Status Table.
   (2) Change ZyWALL eWC refresh pages to consistent with HOME page.
8. [BUG FIX]
   Symptom: Device will crash in bridge mode AV testing.
   Condition: PC(mail client)----(LAN)DUT(WAN)----Mail Server
   (3) In bridge mode, enable AV and activate SMTP from LAN to WAN direction.
   (4) Disable Outlook SMTP authentication in PC.
   (5) PC on LAN and sent out Microsoft Outlook testing mail.
   (6) Device will crash immediately.
9. [BUG FIX]
   Symptom: ZyWALL WLAN & DMZ ports cannot work in dynamic VLAN ports.
   Condition:
   (1) Restore default romfile.
   (2) Set Port Roles as 1>LAN, 2>LAN, 3>DMZ, 4>WLAN.
   (3) Set DMZ IP as 10.10.2.1/24, DHCP as None.
   (4) Set Wireless Card bridge to WLAN.
   (5) Unplug wireless card and reboot device.
   (6) PC connects to DMZ port, IP is 10.10.2.100/24 and gateway is 10.10.2.1, and the PC ping 10.10.2.1 will fail.
10. [BUG FIX]
    Symptom: The eWC>Firewall>Default Rule page will popup JavaScript error in router

mode.
Condition:
(1) Go to eWC>FIREWALL>Default Rule page.
(2) Click Reset button, ZyWALL pop-ups a JavaScript error.

11. [BUG FIX]
Symptom: Unknown crash.
Condition:
(1) Restore default romfile.
(2) Switch device to Active/Active mode, and confirm WAN1 and WAN2 can work fine.
(3) Set WAN2 ping check point to User-defined.
(4) After a while, the device sometimes will crash.
12. [BUG FIX]
Symptom: IDP Total Sessions Scanned is wrong.
Condition:
(1) Enable AV, SMTP service and enable all directions.
(2) Enable IDP, but disable all traffic direction.
(3) Attacker sends the mail containing virus to victim via ZyWALL to check if Anti-Virus can detect viruses.
(4) In eWC>REPORTS>THREAT REPORTS, Total Sessions Scanned of IDP will count number. But it should not.
13. [BUG FIX]
Symptom: ZyWALL crashes if you try to backup Configuration AV or IDP.
Condition:
(1) Go to eWC>Security>ANTI-VIRUS(or IDP)>Backup & Restore page.
(2) Click Backup or Restore button.
(3) System will crash sometimes.
14. [BUG FIX]
Symptom: The ZyWALL should use user configured time server to do daily time adjustment.
Condition:
(1) Reboot the ZyWALL, set 'abc.abc.edu' as user defined 'Time Server Address'.
(2) The time synchronization will fail at start-up and use the default built-in time server list.
(3) The ZyWALL will always use one of built-in time servers to adjust time daily, but the ZyWALL should use user configured time server to do daily time adjustment.
15. [BUG FIX]
Symptom: The IDP should work when the traffic is "from VPN to LAN".
Condition:
Topology
PCB-------ZYWALL----tunnel-----ZYWALL--------PCA
(1) Build a tunnel between PCA and PCB.
(2) Enable IDP and check the direction of "From VPN to LAN" and download a file "eicar.com" by HTTP.
(3) The IDP doesn’t detect the virus.
(4) But IDP works when you choose ’From LAN to VPN’.

16. [BUG FIX]
    Symptom: The device will crash when using VPN manual mode.
    Condition: PC1--ZWA--ZWB--PC2
    (1) Add a VPN manual mode rule in both ZWA and ZWB and make sure PC1 can ping PC2 through the VPN tunnel.
    (2) PC1 ping PC2 continuously.
    (3) Unplug the physical link in WAN, the VPN traffic will pass through (ZWA).
    (4) ZWA will crash.
17. [BUG FIX]
    Symptom: The incorrect data shows on the eWC>THREAT REPORTS>AV.
    Condition:
    (1) Enable AV and use Edonkey behind the ZyWALL.
    (2) The incorrect data shows on the eWC>THREAT REPORTS>AV.
    The detect virus name shows 'Unknown Signature' and the Occurrence is very big, even is a negative number.
18. [BUG FIX]
    Symptom: Sometimes we cannot login ZyWALL by HTTP or HTTPS after enabling the password hash function.
    Condition:
    (1) Enable password hash function in SMT 24.8, "sys pwdHash on".
    (2) After the convert of password, we can never login by HTTP or HTTPS.
19. [BUG FIX]
    Symptom: In ZyWALL 5 bridge mode, the Port statistics of eWC>HOME page shows "Dial Backup" port information.
    Condition:
    (1) ZW5 switches to bridge mode.
    (2) Go to eWC＞HOME>Port statistics.
    (3) The redirected page will show "Dial Backup" port information.

Modifications in V4.01(XD.0)b2 | 05/22/2006

1. [FEATURE CHANGE]
   The multicast AH or ESP packet will not pass to the VPN module in ZyWALL.
2. [FEATURE CHANGE]
   Change wording of one category name in external content filtering.
   Was: Streaming Media/MP3
   Is: Streaming Media/MP3/P2P
3. [FEATURE CHANGE]
   WAS: In SMT 24.8, "ipsec adjTcpMss auto" will let the "IPSec adjust TCP MSS" switch to auto mode.
   IS: "ipsec adjTcpMss 0" will change to auto mode.
4. [ENHANCEMENT]
   (1) System Resources:
   1. Some memory, which is used by running features and system process, has gone in system resource bar. Add back this part of memory in the bar.
   2. Give a space between number and MB.
      WAS: 19/64MB; IS: 19/64 MB

(2) Time representation: Modify eWC>home page>Up Time as a running clock.
(3) Firmware Version: Give eWC>Homepage>Firmware Version a hyperlink to eWC>Maintenance> F/W Upload.
(4) Security Services:
1. Give eWC>Homepage>IDP/Anti-Virus Definitions a hyperlink to eWC>IDP> Update.
2. Add eWC>Homepage>IDP/Anti-Virus Expiration Date a hyperlink to eWC>Registration> Service.
3. Give eWC>Homepage>Anti-Spam Expiration Date a hyperlink to eWC>Registration> Service.
4. Give eWC>Homepage>Content Filter Expiration Date a hyperlink to WC>Registration> Service.
(5) Interfaces
1. Give each eWC>interface a hyperlink to link to the corresponding configuration page.
WAN1/WAN2 link to eWC>Network>WAN page
Dial Backup link to eWC>Network>WAN>Dial Backup page
LAN link to eWC>Network>LAN>LAN page
IP alias1/2 link to eWC>LAN>IP alias 1/2 page
WLAN link to eWC>Network>WLAN>WLAN page
IP alias1/2 link to eWC>WLAN>IP alias 1/2 page
DMZ link to eWC>Network>DMZ>DMZ page
IP alias1/2 link to eWC>DMZ>IP alias 1/2 page
(6) Remove underlines from the links in eWC>Homepage.
(7) Put eWC>Homepage a warning message for Turbo card is not installed.
(8) If there is no Turbo Card installed, the Security Services should be presented accordingly:
WAS: Intrusion Detected 0
Virus Detected 0
IS: Intrusion Detected N/A
Virus Detected N/A

5. [ENHANCEMENT]
Support dual multiple WAN devices for IPSec HA scenario.
6. [ENHANCEMENT]
Change the Anti-Spam wording in log.
WAS: "Mail Parser buffer is overflow!"
IS: "AS checking bypassed as a mail header line exceeds 1024 characters!"
7. [ENHANCEMENT]
(1) Remove the eWC check box: Enable Firewall for VPN traffic.
(2) Remove CI command "ipsec swFwScan on|off".
8. [BUG FIX]
Symptom: Device crashes when sends large number of mails.
Condition:
(1) Enable Anti-SPAM and external database.
(2) Enable Bandwidth management in WAN and DMZ.
(3) Send and receive large number of mails between DMZ and WAN interface.

(4) Device will crash.

9. [BUG FIX]
   Symptom: Traffic can't pass VPN tunnel after a long while.
   Condition:
   Topology:
   PC1 (192.168.1.33) --- ZW_A (192.168.70.100) ==== VPN tunnel ====
   (192.168.70.200)ZW_B --- (192.168.2.33)PC2
   (1) VPN configuration on ZW_A:
   IKE 1: Secure gateway: 192.168.70.200
   Enable XAUTH client
   SA lifetime = 180 seconds
   Policy 1: Local network: 1.1.1.1/24
   Remote network: 2.2.2.2/24
   Enable Nail up
   SA lifetime = 28800 seconds
   Policy 2: Local network: 192.168.1.33/24
   Remote network: 192.168.2.33/24
   SA lifetime = 180 seconds
   (2) VPN configuration on ZW_B:
   IKE 1: Secure gateway: 192.168.70.100
   Enable XAUTH server
   SA lifetime = 180 seconds
   Policy 1: Local network: 2.2.2.2/24
   Remote network: 1.1.1.1/24
   SA lifetime = 28800 seconds
   Policy 2: Local network: 192.168.2.33/24
   Remote network: 192.168.1.33/24
   SA lifetime = 180 seconds
   (3) PC1 ping PC2
   (4) After a while the Policy 2 can't be established anymore.
10. [BUG FIX]
    Symptom: Some wordings in "eWC->ANTI-VURUS" are not correct.
    Condition:
    (1) Go to "eWC->ANTI-VIRUS->General".
    (2) The wording "POP3 (TCP/UDP 110)" should be "POP3 (TCP 110)"
    (3) The wording "SMTP (TCP/UDP 25)" should be "POP3 (TCP 25)"
11. [BUG FIX]
    Symptom: The device can't enable multiple proposal in IKE rule.
    Condition:
    (1) Add an IKE rule using "Preshare key" as authentication type.
    (2) Add another IKE rule using "Certificate" as authentication type, different preshare key and enable the multiple proposals.
    (3) This IKE rule cannot save.
12. [BUG FIX]
    Symptom: In eWC>HOME>Network Status>more page, wireless cannot get correct port status.

Condition:
(1) Insert G-110 wireless card.
(2) Switch device to bridge mode.
(3) Go to eWC>HOME>Network Status>more page.
(4) The "Port Status" of Wireless Card is 100M/Full, but SMT is 54M.
(5) The "Port Status" of WLAN Interface has no any information.

13. [BUG FIX]
Symptom: In PPTP encapsulation, enable VPN, AV and AS, PC can not receive the mail via VPN tunnel.
Condition:
PC1(mail-server:argosoft1.8)--(DMZ)ZW70(WAN:PPPoE)---(WAN:PPTP)ZW5(LAN) ------PC2(Outlook Express)
(1) Establish a VPN tunnel between ZW70 and ZW5.
(2) In ZW70, enable AV, disable AS.
(3) In ZW5, enable AS.
(4) PC2 can't receive the mail from PC1.
14. [BUG FIX]
Symptom: Bridge mode Network Status Bridge Port loss DMZ port.
Condition:
Bridge mode in GUI Home> Network Status>More> Bridge Port loss DMZ port.
15. [BUG FIX]
Symptom: VPN rule swap fails on phase one ID check.
Condition:
Topology:
(LAN) Bridge_A (WAN)=======(WAN) Bridge_B(LAN)
(1) On Bridge_A, add a VPN rule:
IKE: Static rule, enable XAUTH and set as client mode.
Local ID: Type=DNS Content = d.c.b.a
Peer ID: Type=DNS Content = a.b.c.d
IPSEC Policy: Local=Single 1.1.1.1, Peer=Single 2.2.2.2
(2) On Bridge_B, add two VPN rules:
1. Rule one:
IKE: Static rule, XAUTH is disabled.
Local ID: Type=DNS Content = a.a.a.a
Peer ID: Type=DNS Content = b.b.b.b
IPSEC: Local=Single 3.3.3.3, Remote=Single 4.4.4.4
2. Rule two:
IKE: Dynamic rule, enable XATUH and set as server mode.
Local ID: Type=DNS Content = d.c.b.a
Peer ID: Type=DNS Content = a.b.c.d
IPSEC Policy: Local=Single 1.1.1.1, Remote=Single 2.2.2.2
(3) Dial VPN tunnel from Bridge_A to Bridge_B, the VPN tunnel will fail to build up by phase one ID mismatch.
16. [BUG FIX]
Symptom: User can't receive mail through VPN tunnel when WAN is in PPTP encapsulation.

Condition:
Topology:
PC1 (mail client) --- ZW5 (PPTP) === VPN tunnel === ZW70 ---- PC2 (mail server)
(1) Establish VPN tunnel between ZW5 and ZW70.
(2) ZW5's WAN is PPTP, enable AS.
(3) ZW70's WAN can be any encapsulation type, disable AS.
(4) PC1 receives mail from PC2 but it fails.

17. [BUG FIX]
Symptom: Asymmetrical route cannot work.
Condition:
Topology as follows:
PC (A) ---- [L]DUT(B)[W] ------- Internet --- HTTP server(D)(66.102.7.104)
| |
-- [L]Router(C)[W] --- Internet
(1) DUT configures a static route that forwarding packets of destination IP 66.102.7.104 through internal link to Router(C).
PC (A)’s default route entry is DUT (B).
Router (c) is NAT enabled.
(2) PC (A) establishes HTTP connection to HTTP server (D).
a. SYN Packet: A -> B (LAN) -> C (LAN) -> C (WAN) -> D.
b. SYN ACK Packet: D -> C (WAN) -> C (LAN) -> A.
c. ACK Packet: A -> B (LAN), and DUT drop it.

18. [BUG FIX]
Symptom: Trigger port can’t be reconnected.
Condition:
Topology:
PC1(192.168.1.33)------(LAN)ZyWALL(WAN:192.168.70.175)-----PC2(192.168.70.176)
(1) Reset to default romfile.
(2) Go to eWC>WAN>WAN1, set WAN IP Address=192.168.70.175.
(3) Go to eWC>NAT>Port Triggering>WAN1 Interface>Index 1, set Name=ftp, Incoming Start Port=21, incoming End Port=110, Trigger Start Port=21,Trigger End Port=21.
(4) Disable Firewall.
(5) PC1 ftp to PC2, and then PC2 ftp to PC1.
(6) PC2 disconnects ftp session and then reconnects to PC1 will be fail, while PC1 ftp session still connected.

19. [BUG FIX]
Symptom: GUI popup java script error in eWC>NAT>NAT Overview
Condition:
(1) Go to eWC>NAT>NAT, change Max concurrent session per host to 500 and press key "Enter".
(2) ZyWALL popup java script error.
(3) The status bar shows "spSave () fail with Error -6103".

20. [BUG FIX]
Symptom: Redundant gateway sometimes can’t be saved if it's in domain name

format.
Condition:
(1) Create an IKE rule with IPSEC HA is enabled.
(2) Configure a non-exist domain name as redundant gateway.
(3) Let Domain Name Update Timer query this non-exist domain name. It will fail.
(4) Try to modify the domain name with a correct one and save it.
(5) Several minutes later, users will find the domain name has not been changed; it's still the old one.

21. [BUG FIX]
Symptom: In eWC>VPN, VPN Rules page shows incorrect domain name.
Condition:
(1) Go to eWC>DNS>DDNS, set a WAN domain name as "123456789.123456789.123456789.123456789.123456789.123456789.123".
(2) Go to eWC>VPN, create a VPN rule using My domain as 123456789.123456789.123456789.123456789.123456789.123456789.123".
(3) While applying the setting, VPN Rules page shows incorrect domain name.
22. [BUG FIX]
Symptom: Wireless client still can scan wireless network after disabled wireless card.
Condition:
(1) Plug in G100/G110 wireless card.
(2) Go to eWC/Network/Wireless Card/Wireless Card, enable wireless card and set ESSID as "testWlan".
(3) Wireless Client can scan the "testWlan" network by Odyssey tool.
(4) Disable wireless card.
(5) Wireless Client still can scan the "testWlan" network by Odyssey tool.
23. [BUG FIX]
Symptom: ZyWALL crashes when setting NAT address mapping rules.
Condition:
(1) Go to eWC＞NAT＞Address Mapping page.
(2) Add a new rule, configure
Type= Many-to-Many-Overload,
Local Start IP= 1.1.1.1
Local End IP= 3.3.3.3
Global Start IP= 4.4.4.4
Global End IP= 5.5.5.5
(3) Click "Apply" button, then ZyWALL crashes.
24. [BUG FIX]
Symptom: Change WAN IP in GUI, the "Private" option in SMT11.1->Edit IP will be set as "NO".
Condition:
(1) Go to SMT11.1, configure Encapsulation as "PPPoE" or "PPTP".
(2) Go to SMT11.1->Edit IP, change "Private" to "Yes".
(3) Go to eWC->WAN->WAN1, set IP as static IP address.
(4) Go to SMT11.1->Edit IP, the value of "Private" will become "No".
25. [BUG FIX]
Symptom: NAT Many-to-Many Overload rule cannot be set in eWC.

Condition:
(1) Go to eWC>NAT>Address Mapping page, click "Insert" button.
(2) In NAT - ADDRESS MAPPING page, select Type= Many-to-Many Overload.
(3) Click the "Apply" button, and the status shows "Extra characters were detected in the item".

26. [BUG FIX]
Symptom: NAT historical high NAT session per host will over one session than Max concurrent session per host.
Condition:
(1) Go to eWC>NAT>NAT overview, change Max concurrent sessions per host to 500.
(2) Use BluePortScan to do port scan.
(3) Historical high session per host is 501.
27. [BUG FIX]
Symptom: Anti-Spam cannot work in NAT loop back situation.
Condition:
(1) Put PC1 and PC2 on LAN side of ZyWALL.
(2) ZyWALL enables Anti-Spam and disables External Database.
(3) PC2 installs the Merak Mail Server.
(4) PC1 uses the outlook express to send mail to itself by the mail server of PC2.
(5) When the PC1 is sending mails will cause mail stuck until timeout.
28. [BUG FIX]
Symptom: Device responds an invalid sysObjectID value while SNMP browsing.
Condition:
(1) Restore default romfile.
(2) MIB browser connects to device and will get invalid value enterprises.890.1.2 (prestige).
29. [BUG FIX]
Symptom: VPN can be successfully built up with wrong IPSec rule.
Condition:
Topology:
(LAN) ZyWALL_A (WAN)=======(WAN) Bridge_B (LAN)
(1) On ZyWALL A, add a VPN rule:
IKE: Static rule, enable XAUTH and set as client mode.
IPSEC Policy: Local=Single 1.1.1.1, Remote=Single 2.2.2.2
(2) On Bridge_B, add two VPN rules:
1. Rule one:
IKE: Static rule, enable XAUTH and set as server mode.
IPSEC: Local=Single 3.3.3.3, Remote=Single 4.4.4.4
2. Rule two:
IKE: Dynamic rule. XATUTH is disabled.
IPSEC Policy: Local=Single 1.1.1.1, Remote=Single 2.2.2.2
(3)Dial VPN tunnel from ZyWALL_A to Bridge_B, the VPN tunnel will be successfully built up with Bridge_B's rule two.
30. [BUG FIX]
Symptom: The eWC>Firewall>Default Rule page will pup up JavaScript error in

bridge mode.
Condition:
(1) Go to eWC>FIREWALL>Default Rule page.
(2) Click Reset button, ZyWALL pup up JavaScript error.

31. [BUG FIX]
    Symptom: Device crash (Soft watchdog starts up.)
    Condition:
    (1) Firewall+NAT+AV+IDP+AS+AS black list+LB
    (2) LAN has a mail client、mail server；DMZ has a mail client、2 mail server；
    WLAN has a mail client. All of them are on IxLoad
    (3) Run IxLoad 10 minutes，device crash
32. [BUG FIX]
    Symptom: Traffic can't go out after use the tfgen tool.
    Condition:
    (1) Restore default rom file.
    (2) In LAN, use the TfGen with following setting.
    Utilization: 40000; Destination: 168.95.1.1; Port: 777;
    After using the tfgen, all the traffic from LAN can't go outside.

Modifications in V4.01(XD.0)b1 | 04/24/2006

1. [ENHANCEMENT]
   (1) Add UTM reports for IDP/AV/AS.
   (2) Change linkage from GUI>Logs>Reports to GUI>UTM Reports>System Reports.
   (3) Re-layout UTM Home GUI for ZyWALL 4.01.
2. [ENHANCEMENT]
   Add redundant IPSec gateway (IPSec HA).
3. [ENHANCEMENT]
   IPSec traffic can be managed by security rule (IDP/AV/AS/FW/CF/BM)
4. [FEATURE CHANGE]
   Was: IPSec auto-build tunnel command can only build tunnels with same secure gateway IP.
   Is: Users can automatically build VPN tunnels with incremental secure gateway IP addesses.
   Usage of CLI command: ipsec build<secure gateway> <local IP address> <remote IP address> <Nailed-Up> <num> <Control ping> in which
5. [ENHANCEMENT]
   Add direction matrix setting in Firewall/AV/AS/IDP.
6. [ENHANCEMENT]
   Chage weighting of Anti SPAM servers based on average time and fail rate.
7. [ENHANCEMENT]
   (1) Add CI command to see the runtime data for AntiSpam.
   "as display runtimedata <all|black|white> [all|ip|mime|email|subject]"
   (2) Wildcard support for subject and email fields in black list and white list.
   1. Support "*" to indicate match any character 0 or more times.
   2. It is case-insensitive.

3. The maximum length of the email and subject fields is 63 characters.

8. [ENHANCEMENT]
   Add PKCS12 for ZyNOS.
9. [ENHANCEMENT]
   WLAN Zone enhancement.
   (1) ZyWALL has an independent WLAN Zone interface, no matter WLAN card.
   (2) WLAN card is not the independent WLAN interface.
   (3) WLAN card can be bridged to LAN, DMZ and WLAN Zone interface.
10. [ENHANCEMENT]
    support WLAN in "ip nat routing" CI command. Turn on this option for LAN/DMZ/WLAN, packets will be routed when it cannot match any NAT rule.
11. [ENHANCEMENT].
    Add a CI command "ip alg ftpPortNum [port number]" to support a different port number on FTP ALG. This port is an additional FTP ALG port, the original FTP port(21) still works. Note: This CI command will not save to SPT, so user will need to put into autoexec.net if they want to keep the setting.
12. [ENHANCEMENT]
    Consolidate "Router reply ICMP packet" log.
    (1) Router reply ICMP packet: ICMP(Port Unreachable).
    (2) Router reply ICMP packet: ICMP(Host Unreachable).
13. [ENHANCEMENT]
    Add a CI command "sys arp ackGratuitous", let ZyWALL to support gratuitous ARP request and update MAC mapping on ARP table for the sender of this ARP request. There are two subcommands under "ackGratuitous":
    (1) "active [yes|no]": Let ZyWALL accept gratuitous ARP request.
    (2) "forceUpdate [on|off]" If zywall ARP table already had target IP address ARP entry, forceUpdate option will update the exist MAC mapping to new one.
14. [FEATURE CHANGE]
    WAS: The ZyWALL uses a fixed NTP server list with 10 NTP servers to adjust the system time.
    IS: Use 0.pool.ntp.org, 1.pool.ntp.org, 2.pool.ntp.org instead of specific NTP servers to adjust the system time.
    The pool.ntp.org is a virtual cluster of timeservers, it uses a round robin way to provide different NTP server to clients.
15. [ENHANCEMENT]
    Device will detect if Turbo Card is instered or not to determine the NAT and TOS session number. Without Turbo Card inserted, device will recover NAT and TOS session number to 6000.

Modifications in V4.00(XD.8) | 03/16/2006
Modify for formal release.

Modifications in V 4.00(XD.8)b1 | 03/10/2006

16. [ENHANCEMENT]
    Support Green Product Turbo Card
17. [FEATURE CHANGE]

Change the command usage for saving password with hashed by MD5 in the ROM file.
WAS: sys pwdEncryption <on | off> [newPassword] [oldPassword]
IS: sys pwdHash <on | off> [newPassword] [oldPassword]

Modifications in V4.00(XD.7) | 02/24/2006
Modify for formal release.

Modifications in V4.00(XD.7)b1 | 02/17/2006
1. [BUG FIX]
   Symptom: Device crashes after about 5 minutes with default romfile.
   Condition:
   (1) Restore default romfile.
   (2) Only connect WAN port to internet.
   (3) Do NOT access eWC.
   (4) After about 5 minutes, device crashes with Prefetch Abort message.
2. [FEATURE CHANGE]
   WAS: Device accepts any ARP reply information if has its ARP entry.
   IS: Device does not accept ARP reply information which does not have corresponding ARP request by device itself.
3. Symptom: GUI and SMT behavior is not consistent.
   Condition:
   (1) In eWC>VPN>Global Setting page, "Adjust TCP MSS" can be configured as uint16 but as an integer in SMT.
4. [BUG FIX]
   Symptom: ZyWALL crashs when receiving unsupported IKE packet.
   Condition:
   ZW5A-------(tunnel)------ZW5B
   |------PC(send IKE unsupported packetl)
   (1) Edit an IKE rule and an IPSEC rule.
   (2) PC sends unsupported IKE exchange type packet.
   (3) ZyWALL will crash.
5. [ENHANCEMENT]
   Add a CI command "ip arp ackGratuitous", let ZyWALL to support gratuitous ARP request and update MAC mapping on ARP table for the sender of this ARP request. There are two subcommands under "ackGratuitous":
   (1) "active [yes|no]":
   Let ZyWALL accept gratuitous ARP request.
   (2) "forceUpdate [on|off]"
   If zywall ARP table already had target IP address ARP entry, forceUpdate option will update the exist MAC mapping to new one.
6. [ENHANCEMENT]
   Add a CI command, "ipsec initContactMode gateway|tunnel", to support multiple VPN clients which located behind the same NAT router can build VPN tunnel to ZyWALL.
7. [BUG FIX]

Symptom: IKE last packet send out after ESP packet.
Condition:
(1) A PC continuously generates traffic from LAN and it matches a VPN tunnel.
(2) ZyWALL should intiate the VPN tunnel.
(3) After receiving the second packet of quick mode from the peer, ZyWALL send some ESP packets before sending the last quick mode packet.
(4) It should send out the last quick mode packet first, and then send those ESP packet.

8. [ENHANCEMENT].
   Add a CI command "ip alg ftpPortNum [port number]" to support a different port number on FTP ALG.
   Note: This port is an additional FTP ALG port, the original FTP port (21) still works.

Modifications in V4.00(XD.6) | 02/06/2006
Modify for formal release.

Modifications in V4.00(XD.6)b1 | 01/23/2006
1. [ENHANCEMENT]
   Add CLI command "as scoreTimeout" to change AS rating server query timeout value.
2. [ENAHNCEMENT]
   CLI command "as display serverlist" shows information about rating server query round trip time.
3. [ENHANCEMENT]
   The password saved in ROM file can be encrypted by MD5.
   (1) "sys pwdEncryption <on | off> [newPassword] [oldPassword]"
   (a)Use this CI command to turn on or off this feature. Once the feature is on in a ROM file, the F/W without this feature support can not deal the ROM file well. Ex. login problem.
   (b) To turn off the feature, you must provide two password, "newPassword" is the new password that will be saved in the ROM file in plaintext. "oldPassword" is the original administration password that is for security issue.
   (2) "sys md5 <string>" Input a string, it will output the md5 code.
4. [ENHANCEMENT]
   Add CI command, "ipsc swSkipPPTP [on/off]", to let all traffic pass through VPN tunnel setting not to apply on PPTP traffics.
5. [ENHANCEMENT]
   ZyNOS adds device local port conflict protection. ZyWALL will avoid port 1029 as local port.
6. [FEATURE CHANGE]
   WAS: The DDNS of ZyWALL will not update IP when the ZyWALL's WAN IP is static.
   IS: The DDNS of ZyWALL will update IP when WAN IP changes, no matter the ZyWALL's WAN IP is static or dynamic.
7. [FEATURE CHANGE]

WAS: If the zip session is over the maximum zip sessions, this session is bypassed.
IS: Add CI command to decide this session is bypassed or blocked.

8. [FEATURE CHANGE]
   Expend dial bacokup initial string length from 31 characters to 63 characters.
9. [BUG FIX]
   Symptom: The registered username is wrong in
   eWC->REGISTRATION->Registration page.
   Condition:
   (1) A registered device with username abcdefgh.
   (2) In 24.8, type "sys myZyxelCom load".
   (3) Type "sys myZyxelCom config username 1234567890".
   (4) Type "sys myZyxelCom save".
   (5) Type "sys myZyxelCom serviceRefresh".
   After the refresh is finished.
   (6) Type "sys myZyxelCom load".
   (7) Type "sys myZyxelCom display".
   (8) You can see the username field is wrong "abcdefgh90", it should be "abcdefgh".
10. [BUG FIX]
    Symptom: Can not change gateway IP address to "0.0.0.0".
    Condition:
    (1) In eWC->NETWORK->WAN->WAN1(WAN2), set WAN interface as static IP address and gateway = "10.0.0.1".
    (2) Change gateway IP address to 0.0.0.0 and click "Apply".
    (3) Goto eWC->NETWORK->WAN->WAN1(WAN2), the gateway IP address is still "10.0.0.1".
11. [BUG FIX]
    After we rebooted ZyWALL, ZyWALL fails to transmit data through VPN.
    Condition:
    Topology: PC1------(LAN)ZW A(WAN)=====+======(WAN)ZW B(LAN)
    192.168.167.1 | 192.168.1.1
    DHCP Server
    (1) On ZW A, WAN uses dynamic IP address and set a static VPN rule with policy as below:
    IKE: Nail-up is ON
    Local: Subnet Type 192.168.167.0/24
    Peer: Subnet Type 192.168.1.0/24
    (2) On ZW70, set a Dynamic VPN rule with policy as below:
    Local: Subnet Type 192.168.1.0/24
    Peer: Any
    (3) PC1 ping ZW B's LAN IP. Ping result is OK.
    (4) Reboot ZW A.
    (5) Check ZW A eWC SA monitor page, we can see a new VPN tunnel was successfully built up.
    (6) PC1 ping ZW B's LAN IP again. Ping result is fail.
12. [BUG FIX]
    Symptom: Anti Spam cannot work in NAT loopback situation.

Condition:
(1) Put PC1 and PC2 on LAN side of ZW70W.
(2) ZW70W enables Anti Spam and disables External Database.
(3) PC2 installs the ArgoSoft Mail Server.
(4) PC1 uses the outlook express to send mail to itself by the mail server of PC2.
(5) When the PC1 is receiving mails will cause mail stuck until timeout.

13. [BUG FIX]
    Symptom: VPN tunnel up time of ZyWALL private MIB has some problems.
    Condition:
    (1) Successfully build a VPN tunnel.
    (2) Use MIB browser to get the up time value from ZyWALL. The returned result is correct.
    (3) Add a new ipsec policy.
    (4) Get the up time value again. The returned result of the built VPN tunnel is "0(days) 00:00:00".
14. [BUG FIX]
    Symptom: AS log is not correct.
    Condition: The source/destination IP address in log "Exceed maximum mail session" are the same.

Modifications in V4.00(XD.5) | 01/06/2006
Modify for formal release.

Modifications in V4.00(XD.5)b1 | 01/05/2006
1. [BUG FIX]
   Symptom: The incremental rules may not work after updating signature.
   Condition:
   (1). Register myzyxel.com and update the signature.
   (2). Enable the IDP feature.
   (3). For some time, update the signature.
   (4). The incremental rules may not work.

Modifications in V4.00(XD.4) | 12/15/2005
Modify for formal release.

Modifications in V4.00(XD.4)b1| 12/13/2005
1. [BUG FIX] 051202307
   Symptom: DUT can not block infected zip file.
   Condition:
   (1) Use I.E. browser to get http://www.vx.netlux.org.
   (2). DUT can not block the infected zip file, which extended file name is not “zip”.
2. [BUG FIX] 051208573
   Symptom: User updated some version signature, IDP/AV configuration may be lost.
   Condition:
   (1) If user updated 1.092 version signature, IDP/AV configuration will be lost.

Modifications in V4.00(XD.3) | 12/09/2005
Modify for formal release.

Modifications in V4.00(XD.3)b1| 12/06/2005
1. [ENHANCEMENT]
   In eWC->LAN (DMZ, WLAN)->LAN (DMZ, WLAN) page, the DHCP WINS servers now can be configurable via GUI.
2. [ENHANCEMENT]
   In eWC->VPN-> Global Setting page, add two fields "Adjust TCP Maximum Segment Size" and "VPN rules skip applying to the overlap range of local and remote IP addresses."
3. [ENHANCEMENT]
   VPN configuration by CI commands "ipsec adjTcpMss" and "ipsec swSkipOverlapIp" will be reflected in the two fields of GUI -- "Adjust TCP Maximum Segment Size" and "VPN rules skip applying to the overlap range of local and remote IP addresses.", and vice versa.
4. [FEATURE CHANGE]
   Login-Name for PPPOE, PPTP need support 63 characters, Password need support 31 characters in GUI.
5. [BUG FIX]
   Symptom: VPN Relay does not work.
   Topology:Branch A[ZyWALL30W] === HQ[ZyWALL5] ==== Branch B[ZyWALL30W]
   Condition:
   Device Settings:
   Branch_A
   WAN:10.0.0.2
   LAN:192.168.167.0/24
   HQ
   WAN:10.0.0.1
   LAN:192.168.168.0/24
   Branch_B
   WAN:10.0.0.3
   LAN:192.168.169.0/24
   VPN settings:
   Branch_A
   Local IP address 192.168.167.0/24
   Remote IP address 192.168.168.0~192.168.169.255
   Headquarter
   (1)
   Local IP address 192.168.168.0~192.168.169.255
   Remote IP address 192.168.167.0/24
   (2)
   Local IP address 192.168.167.0~192.168.168.255
   Remote IP address 192.168.169.0/24

Branch_B

Local IP address 192.168.169.0/24

Remote IP address 192.168.167.0~192.168.168.255.

Action: Dial up VPN in from both Branch A and Branch B to HQ. Then you can pingBranch B from Branch A, but you can not login any FTP server in Branch A from Branch B. In packets trace, it seems that ZYWALL5 with 4.00(WZ.2)C0 can not relay TCP packets in VPN from wan-to-wan.

6. [BUG FIX]
   Symptom: Under bad network environment, transmit a lot of packets by a VPN tunel, there are a lot of "Replay Packet" log entries.
   Condition:
   (1) Network environment is bad (ex: heavy traffic).
   (2) Build up a VPN tunnel.
   (3) Transmit heavy traffic through the tunnel, after few days it shows a lot of "Replay Packet" log entries.
7. [BUG FIX]
   Symptom: Change Log Mail server, mail will send to old mail server.
   Condition:
   (1). Fill Log mail server ”mail.zyxel.com.tw” and fill other fields by correct data (Enable SMTP Authentication)
   (2). Click ”E-mail Log Now” and receive this log will successful
   (3). Modify Mail server to ”mail.aaa.com.tw” click ”E-mail Log Now", user also can receive this log mail.
8. [BUG FIX]
   Symptom: VPN rule with subnet mask 0.0.0.0 should allow all traffic to pass through VPN, but it doesn’t.
   Condition:
   1. Restore default ROM file.
   2. Set up a VPN policy with remote address type = subnet, remote starting IP address = 0.0.0.0, remote subnet mask = 0.0.0.0.
   3. Trigger tunnel by local PC, and it wil never trigger tunnel.
9. [BUG FIX] 051014149
   Symptom: PC can't send the mail (L to W: SMTP) when the device's bridge and IP is different subnet with the mail client.
   Condition:
   Topology: Mail Server(192.168.12.123/24)---Internet----Device(192.168.11.9/23)----PC(192.168.12.163/24)
   (1) Change the device to Bridge Mode, IP = 192.168.11.9, Mask = 255.255.254.0, Gateway = 192.168.10.11, DNS = 168.95.1.1.
   (2) Edit web eWC/Anti Spam, Enable Anti Spam = Enable.
   (3) Edit web eWC/Anti Spam/External DB Enable, threshold = 0.
   (4) PC can't send the mail to MailServer.
   (5) if we disable Anti-Spam or change the device's IP subnet to 192.168.12.x/24, it works.
10. [BUG FIX]

Symptom: Mail stuck when enable Anti-Spam, because of checksum error.
Condition:
Topology: Client ------(W) ZYWALL (L) ------ Mail Server
(1) Enable AS.
(2) Set port forwarder default server to Mail server.
(3) Client receive mails, sometimes mail stuck.

11. [BUG FIX]
Symptom: Mail get stuck.
Condition:
Mail receive/send stuck when AS is on and mail is going through VPN tunnel.
12. [BUG FIX]
Symptom:In eWC->VPN>Global Setting page, warning messages is not correct.
Condition:
WAS: (Warning: When this checkbox is checked, you may not access device because of triggering VPN tunnels)
Warning messages should be :
(Warning: When this checkbox is not checked, you may not access device because of triggering VPN tunnels).
13. [BUG FIX]
Symptom: Using Outlook Express to receive mails with ZyWALL Anti-Spam enabled, it will stuck until timeout.
Condition:
(1) PC1 -- [LAN]ZW35_A[WAN] -- [WAN]ZW35_B[LAN] -- PC2.
(2) ZW35_A enables NAT + Firewall + Anti-Spam, and Anti-Spam enables external database, Spam Tag = "[**SPAM**]", Tag for No Spam Score = "".
(3) ZW35_B enables NAT + Firewall.
(4) PC2 installs the ArgoSoft Mail Server.
(5) PC1 uses the outlook express to send mail to itself by the mail server of PC2.
(6) When the PC1 is receiving mails will cause mail stuck until timeout.
14. [BUG FIX]
Symptom: All traffic goes through VPN does not work.
Condition:
Topology:
PC1----------(LAN)ZW35A(WAN)===Internet===(WAN)ZW35B(LAN)--------PC2
192.168.1.1/24 | 192.168.2.1/24
(1) On ZW35A, set a Static VPN rule with policy as below:
Local: Subnet Type
192.168.1.0/24
Peer: Single Type
0.0.0.0
(2) On ZW35B, set a Dynamic VPN rule with policy as below:
Local: Single Type
0.0.0.0
Peer: Any
(3) Under the setting, we expect all PC1's traffic to PC2 will go through VPN tunnel to ZW35B first then to PC2.

(4) But it doesn't work.

Modifications in V4.00(XD.2) | 10/26/2005
Modify for formal release.

Modifications in V4.00(XD.2)b2| 10/19/2005
1. [BUG FIX] 051013130
   Symptom: Convert rom file from 3.64 to 4.00, Max. Concurrent session Per Host has some problem.
   Condition:
   (1) Upgrade firmware from 3.64 to 4.00.
   (2) In eWC->ADVANCE->NAT, Max. Concurrent Sessions Per Host is 6000, it should be 4000.
2. [BUG FIX] 051014221, 051014222, 051014223
   Symptom: Spelling error in eWC->Registration page.
   Condition:
   (1) In eWC->REGISTRATION-> Registration page, set two different passwords.
   (2) Press "Apply" button, the status shows "Password and Confirm password are differencet".
   (3) A word "differencet" spells error. It should be "different".
3. [BUG FIX]
   AS fail count will not be increased even the real timeout occurs
4. [BUG FIX] 050928542, 051012075, 051012076, 051012077
   Symptom: The added source IPs of Firewall rule will be lost.
   Condition:
   (1) Go to GUI->FIREWALL->RULE EDIT page.
   (2) Edit a firewall rule.
   (3) Add a source IP(or destination IP) that exceeds its maximum size(20 for ZW5).
   (4) The added item will be lost.
5. [FEATURE CHANGE] 051018364 , 051018365, 051018366
   In eWC->Registration page, change Username field behavior.
   WAS: "-" character is not allowed to key in.
   IS: "-" character is allowed to key in.
6. [BUG FIX] 051018403
   Symptom: PPTP (GRE) cannot pass through NAT.
   Condition:
   PPTP
   Server(192.168.1.33)--(LAN:192.168.1.1)DUT(WAN:192.168.11.100)--PC(192.168.1 1.200)
   (1) Add PPTP Server(192.168.1.33) as Default Server in Port Forwarding
   (2) Firewall is disabled.
   (3) PC(192.168.11.200) can not dial in PPTP on 192.168.11.100
7. [BUG FIX] 051014198, 051014199, 051014200
   Symptom: Use registration wizard to enable service, and last page wording error.
   Condition:
   (1) In eWC->HOME->Internet Access button, go to the last page.

(2) Registration status wording was wrong.

Modifications in V4.00(XD.2)b1| 10/08/2005

1. [BUG FIX] 050906259
   Symptom: Disable bridge mode Firewall "Log Broadcast Frame". Broadcast logs always appear.
   Condition:
   (1) In bridge mode, disable all Firewall -> Default Rule -> "Log Broadcast Frame".
   (2) Broadcast logs always appear.
2. [BUG FIX] 050825052
   Symptom: Tfgen tool causes router crash.
   Condition:
   (1) Use tfgen to send 40000 to 172.21.0.254 and turn it off.
   (2) Use "dev chan disp enet3" to make sure the sending bit is 1.
   (3) Unplug and plug wan2 and router will crash.
3. [BUG FIX]050912438
   Symptom: Device will hang and reboot after "Email Log Now" in bridge mode.
   Condition:
   (1) Topology(Public IP): PC(211.72.158.115) --- [LAN]ZW70_BridgeMode(211.72.158.116)[WAN] --- Internet/MailServer/MailRecipient.
   (2) Set the device as Bridge mode.
   (3) Configure eWC->LOGS: "E-mail Log Settings".
   (4) Click eWC->"Email Log Now" to send log mail.
   (5) System will hang and then reboot by software watchdog.
4. [BUG FIX]050905192
   Symptom: Anti-Spam causes memory leak in bridge mode.
   Condition:
   (1) Topology: Mail Client --- ZyWALL --- Mail Server
   (2) Turn on Anti-Spam at ZyWALL (Bridge Mode).
   (3) Mail Client sents mail to Mail Server. (You can try 500 mails with 2 attachments, total size is about 30k).
   (4) ZyWALL memory leaks.
5. [BUG FIX] 050922955
   Symptom: After updating signature, sometimes the server IP address is incorrect in centralized log.
   Condition:
   (1) In SMT 24.8, type "sys update signatureUpdate".
   (2) After updating signature, type "sys log dis".
   (3) Sometimes you can see a signature update log with incorrect server IP "127.0.0.1".
6. [ENHANCEMENT]
   In eWC->FIREWALL->EDIT RULE page, we added the limitation on the number of source ip address and destination ip address. The limitation is 20.
7. [ENHANCEMENT]
   The device will not retry to update the signature if the update is triggered by user. Ex. CI

command "sys update signatureUpdate", "idp update start", "av update start" or "Update Now" button in eWC.

8. [ENHANCEMENT]
   In eWC>Anti-Spam>General>Action taken when mail sessions threshold is reached, the wording of "Discard" will mislead user to think the system will "drop the mail" when mail session reach the system's limit. In fact, the system doesn't drop the mail, it just drop the mail connection until system have an available mail session to process incoming connection. We replaced "Discard" with "Block" and the wording of "Block" will be explained in web help and User's Guide by "System will Block this mail until a mail session is available".
9. [BUG FIX]
   Symptom: Sometimes device will crash when receiving special mails.
   Condition:
   Topology: Mail_Client --- ZyWALL --- Mail_Server
   (1) ZyWALL turn on Anti-Spam, turn on external DB, threshold = 0.
   (2) Mail_Client receive mail from Mail Server
   (3) Sometimes ZyWALL will crash due to ”Data Abort”, ”not mbuf cookie”, ”mbuf double free”, or mail did not tagged with spam string.
10. [BUG FIX] SPR ID: 050926383,050926384,050926385
    Symptom: AS+AV Enable, it can’t send or receive mail if attached virus files.
    Condition:
    (1) AS and AV enable.
    (2) AV General Setup select all.
    (3) Send or receive a mail with attached virus files.
    (4) It will can’t send or receive mail.
11. [BUG FIX] 051003282
    Symptom: PC cannot transfer file from server (172.20.0.38)
    Condition:
    Topology: PC ---- ZyWALL(WAN:172.x.x.x)(Bridge/Router) --- trunk (172.20.0.38)
    (1) Restore default romfile.
    (2) PC get file from trunk, but it always fails after several seconds.
12. [BUG FIX] SPR ID: 050930643
    Symptom: Edit NAT port forwarding default server = 192.168.1.33, then ping from DUT2 to DUT1, it should show W to L logs, but it show W to W logs.
    Condition: PC1-------LAN DUT1 WAN-------PQA LAB----------WAN DUT2 LAN
    (1) Set with CI commend ”sys romr|y”
    (2) Edit web eWC/WAN/WAN1,My WAN IP Address =172.202.77.121,My WAN IP Subnet Mask=255.255.0.0 ,Gateway IP Address=172.202.77.1
    (3) Edit NAT port forwarding default server = 192.168.1.33, then ping from DUT2 to DUT1, it should show W to L logs, but it show W to W logs.
        -> If we telnet from DUT2 to DUT1, it shows W to L logs, and this right.
        -> If we ping from DUT2 to DUT1, it shows W to W logs, but it should show W to L logs.
13. [BUG FIX] 051003323
    Symptom: NAT many one to one cannot work.
    Condition:

(1) Edit web eWC/NAT/Address Mapping,WAN Interface =WAN2,Insert a Many One-to-One rule (Local Start IP=192.168.1.41,Local End IP=192.168.1.42,Global Start IP=192.168.12.100,Global End IP=192.168.12.101) on eWC/NAT/Address Mapping page
(2) Set with CI command ”ip nat reset enif1”
(3) 192.168.12.110 do port scan 192.168.12.100(port 1-100) and 192.168.12.101(port 1-100)
(4) 192.168.1.41 and 192.168.1.42 cannot capture all port scan packets.

14. [BUG FIX] 050930647
Symptom: Some mails should have SPAM tag or NoScore tag but they didn't have any tag
Condition:
(1) Enable AS
(2) eWC->AS->ExternalDB-: Enable external DB, set the threshold=0, fill the tag for no spam score
(3) MS Outlook Express received a lot of mails from the mail server
(4) Some mails did not have any Spam/No Score tag.

15. [FEATURE CHANGE]
WAS: Allow timeouted ConeNAT session to recreate NAT session from WAN to LAN.
IS: Do not allow timeouted ConeNAT session traffic to recreate NAT session from WAN to LAN.

Modifications in V4.00(XD.1) | 09/26/2005

Modify for formal release.

Modifications in V4.00(XD.1)b2| 09/21/2005

1. [BUG FIX]
Symptom: Content filter was registered in router mode and changed to bridge mode without configure DNS server. One PC open a web site can make DUT crash.
Condition:
(1) In router mode, register content filter and enable it. Edit eWC/Content Filter/Categories/Select Categories, and enable some items (Pornography, Business, Gambling, etc.)
(2) Change DUT to bridge mode without configure DNS server.
(3) PC1 on LAN open a website, and IE would show “block (DNS resolving failed)”
(4) DUT crashed.

Modifications in V4.00(XD.1)b1| 09/12/2005

1. [ENHANCEMENT]
Add CI command "ip urlfiler bypass [LAN/DMZ/WAN] [ON/OFF]" to let traffic matches LAN->LAN, DMZ->DMZ or WAN->WAN directions can be bypassed content filtering.
NOTE: (1) This is a runtime CI command, user can add it into autoexec.net.
(2) This command only support in router mode.
2. [ENHANCEMENT]
Periodically sending the keep-alive zero window TCP ACK when the AS engine

handles the mail. The default value is 5 seconds.

3. [BUG FIX] 050830189
   Symptom: Enable AS ”Discard SMTP mail” and send a mail with attached file will cause the device hangs up
   Condition:
   (1) Enable AS ”Discard SMTP mail”
   (2) Send a over 20k sized mail
   (3) The device hangs up
4. [BUG FIX] 050831205
   Symptom: Device will crash if users turn on myZyxelCom debug message then process device registration and trial service activation.
   Condition:
   (1) Turn on myzyxel.com debug message by "sys myZyxelCom debug type 3"
   (2) Go to eWC>REGISTRATION, register device and activate trial service for Content Filter.
   (3) Device will crash.
5. [BUG FIX] 050701018
   Symptom: DHCP client gets IP failed
   Condition:
   (1) Topology: PC---(192.168.1.1) Router switch to: PC---(192.168.70.250) DUT
   (2) PC connects to the router LAN port with DHCP, and get an IP.
   (3) DUT set a static DHCP rule for the PC.
   (4) PC switch to DUT, and gets an IP failed. The user must release IP manually, then PC will get IP successfully.
6. [BUG FIX]
   Symptom: ZyWALL sends [HASH][DELETE] to delete VPN tunnel after output timed-out even they keeps traffic via the tunnel.
   Condition: PC1 -----ZyWALL----------PC2(Zywall VPN client)
   (L) (W) |----------PC3(Zywall VPN client)
   (1) Configure a dynamic VPN-rule in the ZyWALL.
   (2) Establish first VPN tunnel by PC2 using ZyWALL VPN client.
   (3) Establish Second VPN tunnel by PC3 using ZyWALL VPN client.
   (4) Both PC2 and PC3s’ PCs keep ping to PC1.
   (5) ZyWALL sends [HASH][DEL] to 2nd VPN peer only every 2 minutes which is output Idle time-out timer.
7. [BUG FIX] 050907311
   Symptom: Bridge mode VPN can’t work if configure by Wizard.
   Condition:
   (1) Configure bridge mode VPN with wizard.
   (2) Dial VPN rule and it always fail.
8. [BUG FIX] 050907308
   Symptom: Device will hang forever when editing firewall custom service
   Condition:
   (1) Enable firewll and add custom service, service name=test1, IP protocol=TCP/UDP , port range=2222-2223.
   (2) Edit eWC/firewall/rule summary, packet direction=WAN to WAN/ZyWALL,

insert service "test1", Action for matched packet=permit.
(3) Edit eWC/firewall/service and add another custom service, service name=test2, IP protocol=TCP , port range=100-200.
(4) Edit eWC/firewall/rule summary, packet direction=LAN to WAN, insert service "test2", Action for matched packet=Drop.
(5) Edit eWC/firewall/service and modify custom service "test2", change IP protocol to UDP then click apply.
(6) Device will hang.

Modifications in V4.00(XD.0) | 09/02/2005
Modify for formal release.

Modifications in V4.00(XD.0)b5| 09/02/2005
1. [BUG FIX]
   Device crashed sometimes when doing FTP stress test.

Modifications in V4.00(XD.0)b4| 08/27/2005
1. [BUG FIX] 050819823
   Symptom: Device will crash.
   Condition:
   (1) Enable Anti Spam.
   (2) Enable "Discard SMTP mail. Forward POP3 mail with tag in mail subject".
   (3) Send a spam mail.
   (4) Device will crash.
2. [BUG FIX] 050822932
   Symptom: CPU loading will be very heavy.
   Condition:
   (1) Set two IKE rules which secure gateways are both domain name.
   (2) Go to CI command "sys cpu display", CPU loading is 100%.
3. [BUG FIX] 050824993, 050824994, 050824995
   Symptom: Sometimes system DNS cannot resolve domain name to IP address.
   Condition:
   (1) In CLI, enter "ip dns query name myupdate.zywall.zyxel.com"
   (2) Try (1) more times and sometimes cannot be resolved.
4. [BUG FIX] 050819842
   Symptom: ZyWALL 5 will crash when upload firmware via GUI.
   Condition
   (1) Upload a very large file via GUI.
   (2) Device will crash.
5. [BUG FIX] 050823954
   Symptom: The IPSec rule swap without configuring ID Content will fail (XAUTH case).
   Condition:
   (1) Add one static IPSec rule with XAuth (Rule one).
   (2) Add one dynamic IPSec rule with XAuth. Keep the "Peer ID Content" and "Local ID Content" unchanged "0.0.0.0" (Rule two).

(3) Dial the VPN tunnel from peer gateway, the device won't swap to rule two, and the connection can not be built up.

6. [BUG FIX] 050822915
   Symptom: VPN can not be established if reponder has multiple rules and the correct rule's phase 2 ID type is subnet.
   Condition:
   Topology: ZyWALL_A(WAN)----(Internet)----(WAN) ZyWALL_B
   (1) IPSec policy in ZyWALL_A:
   Policy 1:
   Local: 192.168.3.10/255.255.255.0
   Remote: 192.168.2.7/255.255.255.0
   Policy 2:
   Local: 192.168.1.10/255.255.255.0
   Remote: 192.168.2.6/255.255.255.0
   (2) IPSec policy in ZyWALL_B:
   Policy 1:
   Local: 192.168.2.0/255.255.255.0
   Remote: 192.168.1.0/255.255.255.0
   (3) The other phase 1 and phase 2 parameters for ZyWALL_A and ZyWALL_B are the same.
   (4) Establish policy 1 tunnel from ZyWALL_B.
   (5) ZyWALL_A should establish VPN tunnel by using policy 2, but it fails.
7. [ENHANCEMENT]
   Add CI command "aux usrmdn [1/0]" to switch USR modem flag. If this flag is on, user can dial USR modem successfully.
   Note:
   (1) For USR modem, user should disable hardware flow control(initial string is "at&f1"); or the modem speed should be 38400 BPS.
   (2) This is a runtime CI command, and this flag is not saved into flash. User can add this command into autoexec.net.
8. [BUG FIX] 050517977
   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.
9. [BUG FIX] 050823946, 050819858, 050820885
   Symptom: The UPnP discovery mechanism cannot work normally.
   Condition:
   (1) Disable the UPnP function.
   (2) Reboot device.
   (3) Enable the UPnP function.
   (4) The XP network place cannot show the UPnP icon.
10. [BUG FIX] 050822912

Symptom: Device crashes when doing VPN stress test.
Condition:
(1) Create several VPN tunnls and do stress test.
(2) Device will crash and output the following message on console.
- Prefetch abort exception
Fault Status = 0xXXXXXXXX
Fault Addr = 0xXXXXXXXX

Modifications in V4.00(XD.0)b3| 08/17/2005

1. [BUG FIX] 050727190
Symptom: Spelling invalid in IDP eWC.
Condition:
(1) In eWC>IDP>Signature, click the "Switch to query view".
(2) The wording of the type selection item "Trojan Hourse" is not right. The word "Hourse" should be "Horse".
2. [BUG FIX] 050721992
Symptom: Inactivate Wireless without wireless card will cause device hang.
Condition:
(1) Insert wireless card, and enable wireless function.
(2) After taking out B-100 card, upgrade firmware and disable wireless function.
(3) Reboot the device, the device will hang and cannot finish the system booting.
3. [BUG FIX] 050715808
Symptom: The wireless clients with 802.1x + dynamic WEP cannot ping each other.
Condition:
(1) Setup 802.1x+dynamic WEP environment.
(2) We find that these wireless clients cannot ping each other after rebooting the device.
4. [ENHANCEMENT]
Make AntiVirus LOG be consistent with IDP LOG in signature Release Date format.
5. [ENHANCEMENT]
Change the strategy of the search by name to be case-insensitive in eWC->IDP->Signature->Query page.
6. [FEATURE CHANGE]
Change the wording "WLAN ZONE" to be "WLAN" in the SMT menu 7.1.
7. [BUG FIX] 050727161
Symptom: Output idle timer should not be disabled.
Condition: In eWC->VPN->Global Setting page and SMT 24.8, we should not allow users to set output idle timer = 0.
8. [FEATURE CHANGE]
In SMT 24.1, Wording change: CARD -> WCRD.
9. [BUG FIX] 050728301, 050728302, 050728303
Symptom: Execute SMT 24.1->Press Command->”9-Reset Counters”, device will crash.
Condition:
(1) Insert turbo card.
(2) Execute SMT 24.1->Press Command->”9-Reset Counters” many times, device will crash.

10. [ENHANCEMENT] 050708441, 050708442 and 050712620
    (1) In eWC>AV/IDP>Update, avoid a blank web page be displayed.
    (2) In eWC>WIRELESS CARD>Wireless Card, remove "Your device must have a wireless card installed…" if the wireless card is installed.
    (3) In eWC>AV>General/IDP>General, remove "Your device must have a turbo card installed…" if the turbo card is installed.
11. [BUG FIX] 050616759, 050708438, 050712618
    Symptom: System crashes sometimes while signature update or service license refresh.
    Condition:
    (1) Disconnect WAN interface when you update signature. Hence, the update will fail.
    (2) Re-connect the device WAN interface to Internet.
    (3) After the update fail, the device will crash sometimes.
12. [ENHANCEMENT] 050808225
    Include "WLAN to WLAN" for FireWall hint message.
    WAS :In eWC>FireWall>Default Rule page, update message is "Warning:When this box is checked, all LAN to LAN, WAN to WAN, DMZ to DMZ and packets will bypass the Firewall check."
    IS : In eWC>FireWall>Default Rule page, change message to "Warning: When this box is checked, all LAN to LAN, WAN to WAN, DMZ to DMZ and WLAN to WLAN packets will bypass the Firewall check."
13. [ENHANCEMENT] 050808256
    Message in signatue update needs to be update.
    WAS :In eWC>IDP>signatue update>waiting page, update message is "This may take up a few seconds. Please wait..."
    IS :In eWC>IDP>signatue update>waiting page, change message to "This may take up to minutes. Please wait..."
14. [ENHANCEMENT]
    WAS: In eWC>REGISTRATION>Service page, when service is expired, the Expiration Day field and Registration Type is empty.
    IS : In eWC>REGISTRATION>Service page, when service is expired, the Expiration Day field shows expired date, and Registration Type shows type of expired service.
15. [BUG FIX] 050803125
    Symptom: Create two VPN rules which Remote Gateway IP are domain name,the second security gateway can't update automatically.
    Condition: PC1 ---- ZW5_1 (wan)----Internet ---- (wan) ZW5_2 ---- PC2
    (1) ZW5_1 configuration:
        - Set WAN Encapsulation = PPPoE mode.
        - Set DDNS & active it.
        - Create 2 IKE & 2 ipsec, both security gateway are IP address.
    (2) ZW5_2 configuration:
        - Set WAN Encapsulation = Ethernet/ Static IP.
        - Set DNS server= 168.95.1.1.
        - Create 2 IKE & 2 ipsec, both security gateway are domain.
        - eWC/ VPN/ Global Setting, Set " Gateway Domain Name
    (3) Dial up 2 VPN tunnels.
    (4) Drop ZW5_1's PPPoE line then dial up again.

(5) After 2 minutes into ZW5_2's menu 24.8, issue " ipsec ikeL" to check the security gateway IP --> The Second security gateway not update new IP .

16. [ENHANCEMENT]
Add a centralized LOG "Error: download signature file failed." for signature update fail due to not receive complete signature file. This situation most happens when the network connection is not stable so that device can not receive complete signature.

17. [BUG FIX]
Symptom: Mail can not be sent or received when device turn on Anti-Spam.
Condition:
(1) Device turn on Anti-Spam
(2) Generate a lot of mail sessions with a lot of mails from LAN side hosts at the same time.
(3) Mail can not be sent or received in the following conditions:
(3.1) If queued 20k mail can not be sent successfully after query succeed, then that mail will send fail.
(3.2) ACK packets generated by ZyWALL will cause the TCP connection between client and server abnormal.
(3.3) Re-trasmit packets from mail client or server may be dropped by ZyWALL.

18. [ENHANCEMENT]
Imporve Anti-Spam external database query timeout rate by adjusting internal system parameters.

19. [BUG FIX] 050814513
Symptom: System timer will be exhausted when using TfGen to send heavy traffic to LAN interface.
Condition:
(1) Enable AV/IDP feature.
(2) In LAN side PC, Use TfGen to generate heavy traffic to LAN interface. (Heavy traffic : 40000 kbps/sec up.)
(3) In SMT 24.8, type "sys updateServer signatureUpdate", the router will crash.

20. [BUG FIX]
Symptom: Device crashes in Bridge Mode when enable IDP and Content filter
Condition:
(1) Insert Turbo card and restart device to Bridge Mode.
(2) Download signature to device and restart.
(3) In ”eWC->IDP->General”, enable IDP and activate all interface.
(4) In CI command, type
(4.1) idp tune load
(4.2) idp tune con l7Httpasm on
(4.3) idp tune save
(5) In ”eWC->Content Filter->General”, enable content filter.
(6) In ”eWC->Content Filter->Customization”, enable customization and add a forbidden web site ”www.zyxel.com”.
(7) Access http://www.zyxel.com from a LAN PC.
(8) Device crashes.

21. [FEATURE CHANGE]
Change log behavior when mail session threshold is reached.

WAS: Only generate log when action is DISCARD.
IS: Generate log when action is FORWARD and DISCARD.

Modifications in V4.00(XD.0)b2 | 07/25/2005

1. [FEATURE CHANGE]
   WAS: After deleting the white/black rule via CLI, user needs to type the save command.
   IS: After deleting the white/black rule via CLI, user needn't to type the save command.
2. [BUG FIX] 050614631
   Symptom: IP overlapping check function in eWC->ADVANCED->NAT->Address Mapping sometimes will malfunction in some case in NAT address mapping.
   Condition:
   (1) In eWC->ADVANCED->NAT->Address Mapping->Edit a rule.
   (2) Select Type ”Many-To-Many Overload”, set ”Local Start IP” as ”0.0.0.0”, ”Local End IP” as ”1.0.0.5” ”Global Start IP” as ”1.0.0.2”, ”Global End IP” as ”6.0.0.8”.
   (3) Click ”Apply”, this rule will be saved, it should not.
3. [ENHANCEMENT] AS GUI wordings change
   In eWC>IDP>Signature>Signature Groups Table, refine "select all", "select partial" and "select none" icons in Active / Log / Alert fields.
4. [BUG FIX] 050624163
   Symptom: Host traffic can't pass through VPN tunnel with dial backup
   Condition: PC1-------ZW5 A------Internet-----ZW5 B----------PC2 Dial backup
   (1) ZW5A add one IKE and one Ipsec rules ,Enable Dial backup
   (2) ZW5B add one IKE and one Ipsec rules
   (3) Dail from ZW5 A, and make sure VPN tunnel build up
   (4) PC1 ping PC2 and PC2 ping PC1 is successful
   (5) Pull out ZW5A WAN line ,Dial backup will dial up ,Dail from ZW5 A, and make sure VPN tunnel is rebuild
   (6) PC1 ping PC2 is successful, but PC2 ping PC1 is fail
5. [BUG FIX] 050628469
   Symptom: In bridge mode of the multiple-WAN devices, the LAN web site hits of eWC->LOGS->Reports on WAN2 have not any data.
   Condition:
   (1) In Bridge mode, the WAN 1 is disconnected and WAN 2 is connected.
   (2) Enable LOGS->Reports "Collect Statistics" and "Send Raw Traffic Statistics to Syslog Server for Analysis".
   (3) A LAN PC uses IE to connect to "www.google.com".
   (4) Set "Statistics Report"->"Report type" is Web Site hits, and we cannot find any data.
6. [BUG FIX] 050701007
   Symptom: After displaying the log by CI, you will see the logs related to Anti-spam are broken.
   Condition:
   (1) Enable Anti-Spam and send a Email(not spam mail) through the ZyWALL.
   (2) Use CI->sys logs display to display the logs.
   (3) You will see the logs related to Anti-spam are broken like "! er1@192.168.70.20 Subject:EmailBomb".

7. [BUG FIX] 050705232
   Symptom: In VPN rule name, when users key-in " ' ", GUI will corrupt.
   Condition:
   (1) In eWC>VPN>VPN Rules(IKE) Summary Table, click "+" to add a gateway policy.
   (2) Fill in "Name" field with " ' ".
   (3) Key in "Pre-Shared Key" with 12345678 and click "Apply".
   (4) The GUI will refresh to VPN Rule(IKE) Summary Table page, but is abnormal.
8. [BUG FIX] 050628421
   Symptom: Device will crash after testing dial backup a period time.
   Condition:
   (1) Set WAN 1 as PPTP and enable Dial backup and Set Allocated Budget=1 minute, period=1 hour.
   (2) Ping 168.95.1.1 with DOS command from LAN site host successfully.
   (3) Dial backup will hang up after 1 minute.
   (4) Device will crash after pull out WAN and LAN and Dial Backup line for 10 mins.
9. [BUG FIX] 050707366
   Symptom: Device cannot get DHCP IP after WAN IP is released.
   Condition:
   (1) Device WAN port connects to DHCP server (WAN get DHCP IP).
   (2) Use SMT 24.4.2, "WAN DHCP Release" but not use "WAN DHCP Renewal".
   (3) LAN side PC ping outside, device cannot renew DHCP automatically.
10. [BUG FIX]
    Symptom: Content filter cannot add keyword.
    Condition:
    (1) Goto GUI->Content Filter->Customization page.
    (2) Add Trusted website to its maximum number.
    (3) Add Forbidden website to its maximum number.
    (4) Keyword cannot be added any more.
11. [BUG FIX] 050707368, 050708419
    Symptom: In the eWC->Firewall Rule Summary page, insert a new rule and click "Back" button of IE. Then insert rule again, Firewall will have a null record rule.
    Condition:
    (1) In eWC>Firewall>Rule Summary page, click "Insert" button, then click IE "Back" button.
    (2) Click "Insert" button again, and set one rule then "Apply".
    (3) Rule Summary page have an additional null record rule.
12. [BUG FIX] 050708444, 050708443
    Symptom: When IDP/AV service expired, the expiration day displayed incorrect format in eWC/AV/Update page.
    Condition:
    (1) Device IDP/AV service expired.
    (2) The expiration day displayed incorrect format in eWC>IDP and AV>Update.
13. [ENHANCEMENT]
    Change AV>Update error message.
    WAS : In eWC>AV>Update, update message is "The signature search engine is not

ready".

IS : In eWC>AV>Update, change message to "Can not find the signature , please update the signature!"

14. [BUG FIX] 050706310

Symptom: Hardware watchdog wake up and sometimes device hand up.

Condition:

(1) In SMT24.8, input ”ip ping 168.95.1.1”

(2) Use Ctrl+C to break it.

(3) Repeat steps 1, 2 fast and you can see the watch dog wake up or device hang.

15. [ENHANCEMENT]

Add firewall predefined services: POP3S/IMAP/IMAPS

16. [BUG FIX] 050627328

Symptom: ZyWALL will log ”SMTP successfully” when SMTP authentication fail. Condition:

(1) In ”eWC->LOGS->Log Settings”, set ”E-mail Log Settings”.

(2) Enable ”SMTP Authentication” and set wrong ”Mail Sender”.

(3) In ”eWC->View Log”, click ”Email Log Now”.

(4) There will have a log ”SMTP successfully”.

(5) Actually, the mail was not sent because SMTP server return a error code (454).

17. [BUG FIX] 050725067

Symptom: Fail in receiving the specific mail when the AV works Condition:

(1) Enable POP3 AV , Enable POP3 Assembly mode

(2) Run the POP3 Based-64 AV test with a lot of mail samples

(3) Some mails couldn't be received

18. [FEATURE CHANGE]

WAS: When Turbo card is not inserted, and accessing IDP at the moment, it shows ”The turbo card is not ready , please insert the card and reboot! ”.

IS: When Turbo card is not inserted, and accessing IDP at the moment, it shows ”The turbo card is not ready. Please power down the appliance, insert the card and reboot!”.

19. [FEATURE CHANGE]

WAS: Wording "WLAN" in the network status field in SMT menu 24.1 indicates the wireless card status. Wording "ZONE" indicates the WLANZONE channel status.

IS: "WLAN" -> "CARD, "ZONE" -> "WLAN". So that Wording "CARD" in the network status field in SMT menu 24.1 indicates the wireless card status. Wording "WLAN" indicates the WLANZONE channel status.

20. [FEATURE CHANGE]

When the device sends registration information to MyZyXEL.com server, the router should send 3 digit country number.

21. [BUG FIX] 050713682

Symptom: The router should filter the country code when it is "0".

Condition:

(1) In SMT 24.8, type "sys myZyxelCom register 123456 123456 1234@1.2.3.4 0" (the country code is 0 which is invalid).

(2) It should not be accepted by the router.

22. [BUG FIX] 050712614

Symptom: In eWC>WIRELESS CARD>Wireless card page, the max length of "ESSID"

field is too short.

Condition:

In eWC>WIRELESS CARD>Wireless card page, the max length of "ESSID" field is 30 characters, but user can key in 32 characters via SMT.

23. [BUG FIX] 050715784, 050715785, 050715786

Symptom: In eWC->UPnP page, after saving the related items by Firefox will cause device crash sometimes.

Condition:

(1) Open the Firefox browser and goto the eWC->UPnP page.
(2) Disable the UPnP function, and enable some items.
(3) Click the "Apply" button, the device will crash sometimes.

24. [ENHANCEMENT]

Add help pages.

25. [FEATURE CHANGE]

(1) Modify "Update Server" and "myZyXEL.com" logs.
(2) Pop-up new browser in IDP security policy links.

26. [ENHANCEMENT]

Add hyper link to pop up a new window to display certificate error reasons for certificate log message.

27. [ENHANCEMENT]

Unify eWC>Logs datetime format to ISO 8601 (YYYY-MM-DD hh:mm:ss)

28. [ENHANCEMENT]

Update G100/G110 AP F/W version from 1.0.4.3 to 1.2.8.0.

29. [ENHANCEMENT]

Add the Anti-Virus decompress option in eWC>Anti-Virus->General.

30. [BUG FIX] 050715809

Symptom: The device will reboot in bridge mode when setting wireless authentication as 802.1x.

31. [ENHANCEMENT]

In eWC>REGISTRATION>Registration page and eWC>HOME>wizard page, add username field format check for the myzyxel.com registration.

32. [ENHANCEMENT]

(1) Add the available free memory to the eWC->Home->memory
(2) GUI Memory bar will become red when the memory usage percentage is larger than 90%

33. [ENHANCEMENT]

(1) Change signature version format from 001.001 to 1.001 in the eWC->IDP/AV->Update page
(2) After signature updated, GUI shows "Get signature success". It should be "Get signature successfully."
(3) We should provide users hidden CI commands for clearing signature files.
These CI commands are "idp/av clearAllSig".
(4) When the Turbo card is not inserted, in the console: "Current IDP Signatures: N/A" may confuse users. Change to phrase "Turbo card is not installed" when Turbo card is not installed.
(5) The severity sorting function should perform according to the severity ,not the string

case in the eWC->IDP->Signature/Query page

(6) There should be one space after the SID in the IDP log. Was: IDP:10578,Windows Ping Is: IDP:10578, Windows Ping

(7) In LOG "Update the signature file successfully", it should be modified as "Signature updat OK - New pattern version: V1.001 Release Date: 2005-06-24".

(8) The "idp/av update display" should be consistent to the eWC->IDP->Update page

34. [BUG FIX] 050714719 ,050714720, 050714735

Symptom: If VPN policy enable NAT Traversal, VPN tunnel can't be built up.

Condition:

PC1(192.168.33.33)------VPN1(192.168.1.33)--(L)DUT(W)(192.168.12.100)----(192.168.12.101)VPN2--(192.168.2.33)PC2

(1) Edit DUT web eWC/NAT/Port Forwarding, index1/Incoming Port(s)=500-500, index1/Server IP Address=192.168.1.33

(2) Edit VPN1 web eWC/VPN:

- IKE: NAT-T=Enable, Name=IKE1, Remote Gateway Address=192.168.12.101, Pre-Shared Key=12345678, Local ID Content=192.168.1.33, Peer ID Content=192.168.12.101
- IPSec: Active=Yes, Name=IPSec1, Gateway Policy=IKE1, Local Network Starting IP Address=192.168.33.33 Remote Network Starting IP Address=192.168.2.33

(3) Edit VPN2 web eWC/VPN:

- IKE: NAT-T=Enable, Name=IKE1, Remote Gateway Address=192.168.12.100, Pre-Shared Key=12345678, Local ID Content=192.168.12.101, Peer ID Content=192.168.1.33
- IPSec: Active=Yes, Name=IPSec1, Gateway Policy=IKE1, Local Network Starting IP Address=192.168.2.33, Remote Network Starting IP Address=192.168.33.33

(4) To dial up VPN policy, and it will fail.

35. [ENHANCEMENT]

(1) In eWC>AV/IDP>General, add some warning messages if turbo card is not inserted but AV/IDP is activated. The behavior is similar with WLAN.

(2) When Turbo card is not inserted, in eWC>IDP/AV>Update>Current IDP Signatures will display "Turbo card is not installed".

(3) eWC> MAINTENANCE> Backup&Restore changes to eWC> MAINTENANCE> Backup & Restore.

36. [ENHANCEMENT]

Add centralized logs for signature updating events and errors.

37. [ENHANCEMENT]

Add a centralized log when WAN ping check fails.

38. [FEATURE CHANGE]

Change signature numbers displayed in "eWC->IDP->Signature" page.

39. [ENHANCEMENT]

Display IDP action in centralized log.

40. [BUG FIX] 050715787, 050715788, 050715789.

Symptom: In eWC "HOME" page , "System Time" display error.

Condition:

(1) Go to eWC>HOME Page.

(2) "System Time" display error, the field length is too short.

41. [BUG FIX] 050719921
 Symptom: Mail can't be received via POP3.
 Condition: Topology:
  PC ----- ZyWALL ----- Mail Server
  1. Enable Anti-Spam.
  2. PC receives mails from Mail Server.
  3. PC sometimes can't receive mail and mail client will timeout.
42. [ENHANCEMENT] 050708486, 050712606, 050719906, 050707395, 050712605
 Add protection to avoid setting unsupported security in "eWC->Wireless Card" when inserted wireless card is B100. Note: B100 does not support WPA, WPA-PSK, 802.1x + Dynamic WEP.
43. [ENHANCEMENT] Wording
 WAS: The device will now reboot. As there will be no indication of when the process is complete, please wait for one minute before attempting to access the router again
 IS: The system will now reboot. As there will be no indication of when the process is complete, please wait for one minute before attempting to access the system again.
44. [FEATURE CHANGE] Update registration message
 WAS:
 (1) When user upgrade IDP/AV/AS services, the LOGS shows "service upgrade successfully" but users can not know which service is upgraded"
 (2) When user activate trial service(s), the LOGS shows "trial service activation successfully" but users can not know which service is activated. IS:
 (1) When user upgrade services, the LOGS will show
 "Content Filter service upgrade successfully" or
 "IDP/Anti-Virus service upgrade successfully" or
 "Anti-Spam service upgrade successfully" depends on which service license key is used.
 (2) When user activate trial service(s), the LOGS shows which trial service is activated. Ex. "Content Filter, IDP/Anti-Virus trial service(s) activation successfully"

Modifications in V4.00(XD.0)b1 | 07/01/2005

1. [ENHANCEMENT]
 Change the input format of trap destination in eWC->Remote Management->SNMP rom text to IP format.
2. [ENHANCEMENT]
 Support small font size on ZyWALL GUI.
3. [ENHANCEMENT]
 Replace the Cerberian logo by Blue Coat in Content Filter blocked page.
4. [ENHANCEMENT]
 Support Turbo Card (external IDP/AV signature search accelerator)
5. [ENHANCEMENT]
 Add ARP probe for DHCP server.
 (1) Change probe type by CI command "sys probeType [icmp | arp]".
 (2) Default type is "ICMP".
 (3) ARP probe only works when you use arp probe type and dhcp mode should be "Server".
 (4) This value will be saved in ROM.

6. [FEATURE CHANGE]
   Add ALG configuration in navigation panel.
7. [ENHANCEMENT]
   Re-layout ZyWALL navigation panel on GUI.
8. [ENHANCEMENT]
   Add "Service Status" and "Expiration Date" in Content Filter GUI. The modified GUIs are:
   eWC>CONTENT FILTER>Categories
9. [ENHANCEMENT]
   Add a sender email field in "E-mail Log Settings".
10. [ENHANCEMENT]
    When the daylight saving is activated, there should be a "DST" string trailed behind the time in eWC.
11. [ENHANCEMENT]
    WAS: DNS domain name is not case insensitive.
    IS: DNS domain name is case insensitive.
12. [ENHANCEMENT]
    Firewall ”Available Services” add some common services which are
    (1) Microsoft RDP (remote desktop protocol) - tcp:3389
    (2) VNC (virtual network computer) - tcp:5900
    (3) NTP - tcp/udp:123
13. [ENHANCEMENT]
    Consolidate log “Under SYN flood attack, sent TCP RST”
14. [ENHANCEMENT]
    (1) Users cannot enter characters into eWC>VPN>GATEWAY POLICY >EDIT>SA Life Time (Seconds)
    (2) User cannot enter characters in eWC>VPN>NETWORK POLICY >EDIT>Protocol
    (3) Users cannot enter characters into eWC>VPN>NETWORK POLICY >EDIT>SA Life Time (Seconds)
15. [ENCHANCEMENT]
    Add IDP,Anti-Virus and Anti-Spam features.
16. [ENHANCEMENT]
    Add the SMTP server to the log entry.
17. [ENHANCEMENT]
    Add sequence number and SPI in log for ESP / AH packets.
18. [ENHANCEMENT]
    DHCP log shows the hostname.
19. [ENHANCEMENT]
    Add VPN over Bridge feature.
20. [ENCHANCEMENT]
    Add MyZyxel.Com and Registration features.
21. [ENHANCEMENT]
    Add Firewall Custom Service enhancements.
    Modifications are listed below:
    (1) Allow user to configure ICMP type and code in Firewall ACL.
    (2) Allow user to configure IP protocol in Firewall ACL.

(3) Add "Any IP Protocol" in default service.(GUI only)
(4) Replace "PING" with "Any ICMP" in default service. (GUI only)
(5) Allow user to configure Firewall rule name.
(6) Firewall (defeault/rule) action supports "permit", "drop" and "reject".
(7) Centralized LOGS shows descriptions for matched ICMP packet instead of displaying type/code value only.

22. [ENHANCEMENT]
Enhance Firewall Custom Service
(1) In eWC>Firewall>add new page "Service", it displays the summary of custom services and predefined services.
(2) In eWC>Firewall>Service>Firewall Service Edit page, add two new options: IP protocol and ICMP.

23. [ENHANCEMENT]
On eWC>FIREWALL>Threshold, add a GUI option to enable/disable DoS Attack protection.

24. [ENHANCEMENT]
Each static route entry should have its own "Modify" and "Delete" icons.

25. [ENHANCEMENT]
Add dial backup support for CI command.
The following is the original SPR description.
Enhance SMT “sys rn accessblock 0 ” debug message.
(1) CI “sys rn load 3”
(2) CI “sys rn accessblock 0”
(3) CI “sys rn save”
(4) And SMT will occur message “[-6103] Bad entry number”

26. [ENHANCEMENT]
Enhance Firewall Edit GUI to make it more user-friendly.
Before: When users click Add/Modify/Delete button to configure an address or select a service from Available Service to Selected Service, the page will be submitted to the ZyWALL immediately to have a rule check and then refresh. It consumed too much time on editing a firewall rule for a user.
Now: When users click Add/Modify/Delete or select a service, the page will not be submitted to the ZyWALL immediately. The page will be submitted to the ZyWALL to have a rule check after users click "Apply" button. It reduces the refresh time and it is more convenient for the users.

27. [ENCHANCEMENT]
(1) Enhance WLAN to be an independent interface so that traffic passes through WLAN can be handled by firewall.
(2) WLAN can be bound to LAN or DMZ for user’s chosen.
(3) DHCP sever can be applied on LAN, DMZ and WLAN.

28. [ENHANCEMENT]
In order to solve ZW5 available memory is not enough for 4.00, allocate a share memory for signature download and firmware upload.

29. [ENHANCEMENT]
Add DDNS as My Address in VPN IKE rule. (GUI)

30. [ENHANCEMENT]

Add ping check switch for single WAN products.
CI command: sys rn pingcheck [0:disable|1:enable]
Note: This will not be saved in romfile.

Modifications in V3.64(XD.3) | 06/21/2005
Modify for formal release.

Modifications in V3.64(XD.3)b1 | 06/16/2005
1. [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()".
2. [ENHANCEMENT] 050418857
DNS domain name should be case insensitive.
3. [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.
4. [BUG FIX] 050526694
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.
5. [BUG FIX]
Symptom: Output idle timer doesn't work correctly.
Condition:
PC1--(L)ZW5(W)--Intranet--(W)Router(L)--PC2
(1) ZW5 and Router had established VPN tunnel.
(2) Output idle timer=120 secs, input idle timer=30 secs.

(3) Unplug the WAN link of Router, make a ICMP echo request to PC2 from PC1.
(4) ZW5 doesn't send out "are u there" packets to peer gateway after 120 seconds.

6. [BUG FIX] 050613568
   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.
7. [BUG FIX] 050615688
   Symptom: The Log Consolidation Period can not configure properly.
   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 V3.64(XD.2) | 06/10/2005
Modify for formal release.

Modifications in V 3.64(XD.2)b3 | 05/31/2005
1. [BUG FIX] 050527748
   Symptom: DNS of Dail backup had some problem if WAN's Encapsulation = PPTP mode.
   Condition:
   1. Restore default Rom.
   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. eWC/DNS/System, DNS server keep old DNS IP (Assigned from PPTP server) .

Modifications in V 3.64(XD.2)b2 | 05/25/2005
1. [BUG FIX] 050414592
   Symptom: Dynamic rule with more than two initiators has problem.
   Condition:
   1. ZyWALL 5 as responder has one dynamic rule and use XAUTH.
   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]
   Symptom: Trigger dial fail in dial backup.
   Condition:
   1. Restore default rom file.
   2. Setup dial backup account and phone number, 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]
   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] 050502014
   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 settigs are correct.
5. [BUG FIX] 050502014
   Symptom: Modification to exisiting 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. It doesn’t work
   5) Now add the standard SSH (or any other predefined TCP rule) service to the same firewall rule. It works.
6. [BUG FIX] 050311653
   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.
7. [BUG FIX] 050502038
   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.

8. [BUG FIX]
Symptom: Router crash.
Condition:
(1) Turn on firewall.
(2) Sometimes router will crash when suffer attack.

9. [BUG FIX]
Symptom: Dial backup will be triggered abnormally.
Condition:
(1) Configure a Dial Backup.
(2) Close ping check flag by “sys rn pingcheck 0”.
(3) WAN is ethernet, gets an IP, and cannot access Gateway.
(4) Dial backup will be triggered, it is not right.

10. [BUG FIX]
Symptom: Dial backup will be triggered abnormally.
Condition:
(1) Configure a Dial Backup.
(2) WAN is ethernet.
(3) Reset the router, Wan gets an IP but dial back-up still will be triggered.

11. [FEATURE CHANGE]
When edit a firewall rule, the source IP and destination IP rule numbers are limited to 20.

12. [FEATURE CHANGE]
At the beginning of router restart, the pingcheck is disabled.

Modifications in V 3.64(XD.2)b1 | 05/18/2005

1. [BUG FIX] 050414592
Symptom: Dynamic rule with more than two initiators has problem.
Condition:
1. ZyWALL 5 as responder has one dynamic rule and use XAUTH.
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]
Symptom: Trigger dial fail in dial backup.
Condition:
1. Restore default rom file.
2. Setup dial backup account and phone number, 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]
   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] 050502014
   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 settigs are correct.
5. [BUG FIX] 050502014
   Symptom: Modification to exisiting 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. It doesn’t work
   5) Now add the standard SSH (or any other predefined TCP rule) service to the same firewall rule. It works.
6. [BUG FIX] 050311653
   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.
7. [BUG FIX] 050502038
   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.

8. [BUG FIX]
   Symptom: Router crash.
   Condition:
   (1) Turn on firewall.
   (2) Sometimes router will crash when suffer attack.
9. [FEATURE CHANGE]
   When edit a firewall rule, the source IP and destination IP rule numbers are limited to 20.
10. [FEATURE CHANGE]
    At the beginning of router restart, the pingcheck is disabled.

Modifications in V3.64(XD.1) | 05/03/2005
Modify for formal release.

Modifications in V 3.64(XD.1)b2 | 04/27/2005
1. [BUG FIX] 050201039
   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.
2. [BUG FIX]
   Symptom: LAN & WAN deathed 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: “DUT’s WAN IP”, Port: 500.
   (4) After a period time, DUT’s LAN & WAN both deathed that all traffic can’t go out.
3. [BUG FIX] 050203206
   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.

Modifications in V 3.64(XD.1)b1 | 04/22/2005

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] 050420986
   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] 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.

9. [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"
10. [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.
11. [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.
12. [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.
13. [BUG FIX] 050407161
    Symptom: PC cannot ping remote secure gateway's LAN IP via VPN tunnel
    Condition:
    PC A (1.33) – (1.1)ZW5 --- LAB ---- ZW70 (2.1) ----(2.33) PC B
    (1) Add a VPN rule(ZW5), 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) ZW70 had opposite setting.
    (3) Build up this tunnel, PC A can ping PC B, but PC A can't ping 192.168.2.1(ZW70 gateway LAN IP)
14. [BUG FIX] 050302166

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.

15. [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.
16. [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.
17. [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"
18. [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.
19. [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.
20. [BUG FIX] 050201041
    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.

21. [BUG FIX] 050415693
    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.
22. [BUG FIX] 050406055
    Symptom: ZyWALL VPN traffic will lose from time to time
    Condition:
    (1) To create tunnel from zw5 to peer.
    (2) To ping the LAN PC of peer VPN gateway fom the LAN PC of zw5 via the tunnel.
    (3) About 1 min, it will re-key again.
    (4) The tunnel loses packet.
23. [BUG FIX] 041201001
    Symptom: Router will crash when receive an unrecognizable DNS response
    Condition:
    Environment:
    PC(192.168.1.33)-----(192.168.1.1)ZW5---Internet
    (1) Set ZW5's system DNS server as "164.67.128.1"
    (2) From PC, send a DNS query to ZW5. 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) ZW5 will relay the DNS query to "164.67.128.1".
    (4) ZW5 will crash after receive DNS response from "164.67.128.1"
24. [BUG FIX] 050311685
    Symptom: Firewall WAN to DMZ Reject can’t work.
    Condition: PC A ---- (W)ZW5 (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 ZW5 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 [ZW5]Firewall W2D item 3->1
25. [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".
26. [BUG FIX] 050201045
    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.

27. [BUG FIX] 050301081
Symptom: Subclass(FTP service) can not borrow all rest of parent bandwidth in priority-base.
Condition:
1.Root bandwidth is 1000kbps
2.Add a FTP service subclass which bandwidth is 100kbps and can borrow from parent.
3.Add a Custom service subclass which bandwidth is 100kbps and can borrow from parent
4.Execute FTP，but FTP service bandwidth can not borrow all rest of parent bandwidth
5.Send lots of UDP packet，but Custom service bandwidth can not borrow all rest of parent bandwidth. Sometimes all traffic can not pass through DUT.

28. [BUG FIX] 050128718
Symptom: The VT6105 Ethernet port may fail to receive any packet.
Condition:
1. Connect ZyWALL5's LAN port (using VT6105 Ethernet chip) to an SMC hub and operate it in 100M/HALF mode.
2. Generate heavy traffic to go through the ZyWALL 5's LAN port.
3. After an indefinite period of time, the ZyWALL 5's LAN port may fail to receive any packet. When this hang condition happens, the console will show "enet0 stop NIC Rx never completed!"

29. [BUG FIX]
Symptom: DDNS failed to update when PPPoE redial.
Condition:
1. Configure the DDNS host and enable it.
2. Configure WAN as PPPoE mode and idle timeout, and connected OK.
3. When the connection is doown, and connected again, IP is change, it failed to update DDNS server.

Modifications in V3.64(XD.0) | 03/04/2005
Modify for formal release.

Modifications in V3.64(XD.0)b4 | 02/23/2005
1. [BUG FIX]
Symptom: In PPPoE/PPTP mode, BWM can not classify the traffic of FTP, H323, SIP.
2. [BUG FIX]
Symptom: Bandwidth Management, Priority based, FTP transfer speed slow down until to disconnect .

Condition:
(1) Edit web eWC/BW MGMT，WAN/Active=enable, WAN1/Speed (kbps)=1000, Scheduler=Priority-Based
(2) Edit web eWC/BW MGMT/Class Setup, Interface=WAN1, Add Sub-Class, Class Name=FTP, Bandwidth Budget=200, Priority=3, Borrow bandwidth from parent class=enable，Enable Bandwidth Filter=enable, Service=FTP, Destination IP Address =192.168.10.0, Destination Subnet Mask=255.255.255.0
(3) FTP upload file from LAN to WAN

3. [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.

4. [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

5. [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"
   (2) When selecting "WPA+PSK", "Authentication Databases" should be hidden.

Modifications in V3.64(XD.0)b3 | 02/03/2005

1. [BUG FIX]
   Symptom: OpenPhone H.323 traffic will be blocked by Firewall if connection is initiated from WAN side to LAN side.
   Condition:
   PC1(OpenPhone)--------(LAN) ZyWALL (WAN) --------- PC2(OpenPhone) 192.168.1.33
   (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) Enable H.323 ALG by "ip alg enable ALG_H323"
   (4) PC1 and PC2 use OpenPhone, PC2 call PC1.
   (5) OpenPhone application traffic will be blocked by Firewall, you will see a lot of Firewall blocked log in Centralized LOG.
2. [BUG FIX]
   Symptom: DPD vendor ID is not correct.
   Condition: VID value of DPD is not compatible with RFC3706.
3. [FEATURE CHANGE]
   WAS: The second datagram will use the last 8 octets of the first datagram as IV. This may cause IV "predictable".
   IS: All datagrams will use random IV to make IV unpredictable.

Modifications in V3.64(XD.0)b2 | 01/31/2005

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 Addrsss" 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 wordings in "Budget" is "Always On".
   (2) In SMT, the wording is "Nailed-Up Connection".
5. [BUG FIX]
   Symptom: While performing “Chariot 128 application 48 hours stress testing”, ZyWALL crashed several .
   Condition: Chariot Server<-----DUT----->Chariot end point
   (1) DUT reset default romfile, and only configured WAN and LAN IP address.
   (2) Traffic direction: Server to end point.
   (3) Execute Chariot (automation.exe) after load stress file (stress-all.txt)
   (4) After a while, DUT crashed
6. [BUG FIX]
   Symptom: The traffic redirect should have higher priority than dial backup.
   Condition:
   (1) In eWC>WAN>Route, set Traffic Redirect priority smaller than Dial Backup, then click Apply.
   (2) It can be saved.
7. [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.
8. [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”.
9. [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, and 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.

10. [ENHANCEMENT] Add SIP protocol in service list in firewall rule edit page.
11. [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 overloads(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.

12 [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.

13 [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.

14 [ENHANCEMENT] NAT address mapping need prevent user configure local IP range and global IP range overlap.

15 [BUG FIX]
Symptom: SIP WiFi-Phone's voice communication failed.
Condition:
(1) Use following topology to test.
WiFi A–(L)ZW35(W)----Internet(SIP server)---(W)ZW5(L)----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.

16 [BUG FIX]
Symptom: The deivce 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.

17 [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.

18 [BUG FIX]
Symptom: BWM linear search can not find first match filter.
Condition:
PC1 ------------ (LAN) Router (WAN) ----- PC2
(1) In router, enable BWM on WAN, setup two classes for WAN Root class: 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.

19. [BUG FIX]
Symptom: When manual mode encapsulation is Tunnel, responder can’t build up tunnel.
Condition:
(1) PC A – ZW70 ---- ZW5 – PC B
(2) On eWC/VPN/Manual add two manual rules in ZW70 and ZW5. 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.

20. [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.

21. [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"
22. [BUG FIX]
    Symptom: VPN tunnel cannot be disconnected.
    Condition:
    (1) PC1—ZW5-----HUB-----ZW10W(V362WH7)--PC2
    (2) ZW5 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 ZW5 VPN tunnels can not be disconnected
23. [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.
24. [ENHANCEMENT] Add "Session Table is Full!" log message, when tos session is full.
25. [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.
26. [BUG FIX]
    Symptom: The centralized log shows the strange DHCP entry with hex IP address.

Condition:
(1) The device enables LAN DHCP server.
(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)

27. [ENHANCEMENT] When router reset, console will display the reset date and time. For example, .\sys_cmd.c:869 sysreset() ZyWALL 5 system reset at 01/18/2005 15:07:48
28. [BUG FIX]
    Symptom: VPN page cannot be configured.
    Condition:
    (1) Go to eWC>VPN>GATEWAY POLICY>EDIT to add a GATEWAY POLICY rule.
    (2) Go to eWC>VPN>NETWORK POLICY>EDIT to add 10 NETWORK POLICY rules and bind them with the GATEWAY POLICY rule which was added in Step1.
    (3) Delete the GATEWAY POLICY rule which was added in Step1 and 10 NETWORK POLICY rules will be put into the Recycle Bin
    (4) VPN page can't be configured anymore.
29. [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 an 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.
30. [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 cycle. 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.
31. [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.

32. [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.
33. [ENHANCEMENT] Add port information in centralized log message when a netbios packet was blocked.
34. [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. If NTP server is on LAN/DMZ subnet, DUT still won't sync when WAN interface is down.
35. [BUG FIX]
Symptom: VPN tunnel can be established but traffic cannot go through tunnel.
Condition: PC1 -- ZyWALL -- Any Router/Internet -- ZyWALL -- PC2
(1) Configure corresponding VPN setting in both ZyWALLs.
(2) Dial VPN tunnel
(3) After tunnel established, PC1 cannot ping PC2 vice versa.
36. [BUG FIX]
Symptom: The router cannot 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.
37. [BUG FIX]
Symptom: In bridge mode, SIP traffic cannot be managed by BWM.
Condition: SIP Phone1 ----- (LAN)ZyWALL(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.
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 cannot 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 borrows 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 cannot be deleted via CI command.
Condition:
(1) On eWC->BW MGMT->Class Setup, create 3 classes on LAN interface. all classes have filter 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: Device will crash.
Condition: Use IXIA to simulate 1012 ip address to access web site (every ip has 10

sessions), device will crash.

43. [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.
44. [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.
45. [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 (FTP server in 192.168.70.8)
    (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. (This is right)
    Then logout the ftp.
    (5) Repeat step 3 but change the 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.
46. [FEATURE CHANGE] Extend "devID" field to six hexadecimal numbers(12 characters) in syslog format.
47. [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.
48. [BUG FIX]
    Symptom: After VPN tunnel is established, user will see DPD packet while traffic still can be transferred through tunnel.
    Condition:
    PC1-------- ZyWALL-A ========== ZyWALL-B ------- PC2 IPSec tunnel
    (1) Configure VPN tunnel between ZyWALL-A and ZyWALL-B.
    (2) In ZyWALL-A eWC->VPN->Global Setting, set Output Idle Timer = 120.
    (3) Reboot ZyWALL-A.

(4) PC1 ping PC2 to trigger tunnel.
(5) after tunnel is established, users will see ZyWALL-A's LOG show DPD packets.

49. [ENHANCEMENT] BWM children's bandwidth's sum will not exceed parent's. For example, the bandwidth of WAN interface is 50000 kbps. The sum of all children's bandwidth can not exceed 50000 kbps

Modifications in V3.64(XD.0)b1 | 12/17/2004

1. [ENHANCEMENT] Redesign IPSec mechanism to comply with ICSA Labs 1.1D IPSec Certification Testing.
   New feature added :
   (1) Multiple Proposal.
   (2) Support Nail Up, Dead Peer Detection, Control Ping.
   (3) Separate IPSec SA (Phase 2) from IKE SA (Phase 1), multiple IPSec SAs can bind to one the same IKE SA. (Multiple policy)
   (4) Add a "Global Setting" tab in eWC->VPN which contains some timer settings.
   (5) IKE and manual key rules have their setting pages respectively in eWC->VPN.
   (6) Remove the VPN setup page (SMT 27)
   (7) Redesign lots of IPSec CI command.
2. [ENHANCEMENT] Support Port Restricted Cone NAT.
3. [ENHANCEMENT] Redesign eWC->BW MGMT->Class Setup page.
4. [ENHANCEMENT] Enable "ip alg" command in bridge mode.
5. [ENHANCEMENT] Add the eWC>CONTENT FILTER>Cache and eWC>DNS>Cache GUI.
   (1) Add total cache entry number info.
   (2) Remove the "Port" info in URL Cache Entry table.
   (3) The "Action" in URL Cache Entry table shows "Blocked" first by default.
   (4) The URL entry in URL Cache Entry table aligns to the left.
   (5) On the URL Cache Entry table, if the length of a URL entry is over 50, it will be truncated to 50 characters, with three trailing dots (...) appended.
   (6) To adjust the note font size in eWC>DNS>Cache GUI.
6. [ENHANCEMENT] Popup message improvement: "Delete this rule?" => "Delete entry #[number] ?"
7. [ENHANCEMENT] DNS adds CI command "ip dns system cache flush".
8. [ENHANCEMENT] eWC>LOGS>Reports>Report Type>"LAN IP Address" renamed as "Host IP Address"
9. [ENHANCEMENT] In eWC>DNS>System>Address Record, add Wildcard.
10. [ENHANCEMENT] Add length checking of DNS(Peer ID Type) content in VPN.
11. [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)
12. [ENHANCEMENT] Add FQDN support in my IP address in IKE.
13. [ENHANCEMENT] IPSec GUI enhancements

(1) On eWC>VPN>Global Settings, add IPSec timers configuration.
(2) On eWC>VPN>Network Policy Edit page, add Netbios passthrough field.
(3) On eWC>VPN>Gateway Policy Edit page, add FQDN field for My ZyWALL.

14. [ENHANCEMENT] Enhance ZyWALL GUI.
    (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.
15. [ENHANCEMENT]
    (1) In eWC>Home>System 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] Auth Server/Local User Database needs long time to save all entries, enhance the saving policy to speed up this action.
18. [ENHANCEMENT] In SMT 24.6, the menu adds the reminding message "You can enter ctrl-x to terminate operation any time."
19. [ENHANCEMENT] Add a API function to move rules for NAT address mapping table. CI command: ip nat acl move <set#> <rule# from> <rule# to>
20. [ENHANCEMENT] For Manual IPSec rule, the "My ZyWALL" and "Remote Gateway Address" should not have FQDN fields. (Remove My Domain Name and change Secure Gateway Address into IP field)
21. [ENHANCEMENT]
    (1) In eWC>MAINTENANCE>General, change the type of the "Administrator Inactivity Timer" field from ASCII to integer.
    (2) Add a JavaScript Global function to avoid filling any character in the specific fields on both IE and Netscape. (allow number only)
22. [ENHANCEMENT] Add a "Log" check box for "VPN connectivity check". in eWC>VPN>NETWORK POLICY>EDIT.
23. [FEATURE CHANGE] Modify CI command "ip arp add" from hidden to visible.
24. [ENHANCEMENT] For single WAN, the WAN cannot receive an IP from DHCP server with the same subnet with other interfaces.
25. [ENCHANCEMENT] The new DST feature allows user to know the start/end date. It will be nice if the ZyWALL shows what date ’1st Sun in April’ is ----. And there is some spare space on the screen on that line.
26. [ENHANCEMENT] User can use telnet/ping/ via VPN in SMT menu 24.8.
    (1) If you telnet/ping/... from your ZyWALL to an IP on the VPN "remote network" and the ZyWALL’s LAN IP (including alias IP) is on the VPN "local network", the

ZyWALL uses LAN IP as source.
(2) If you telnet/ping/... from your ZyWALL to an IP on the VPN "remote network" and the ZyWALL's DMZ IP (including alias IP) is on the VPN "local network", the ZyWALL uses DMZ IP as source.
(3) (For future wireless enhancement) If you telnet/ping/... from your ZyWALL to an IP on the VPN "remote network" and the ZyWALL's WLAN IP (including alias IP) is on the VPN "local network", the ZyWALL uses WLAN IP as source.
(4) Otherwise the ZyWALL uses any appropriate interface IP as source depending on the routing table.
Note: If there are more than one appropriate local interfaces, router will use the first matched local interface IP address as the source IP address.

27. [ENHANCEMENT] In GUI>NAT>Port Forwarding, router will now check if the translated end port is out of 65535.
28. [ENHANCEMENT] On eWC>HOME>VPN wizard, My ZyWALL address support Domain name.
29. [ENHANCEMENT]
    (1) In eWC>MAINTENANCE>F/W Upload, the warning message title should be red in order to be consistent with the style of other warning message.
    (2) In eWC>MAINTENANCE>Restore Configuration, the warning message title should be red in order to be consistent with the style of other warning message.
30. [ENHANCEMENT] On eWC>NAT>AddressMapping, add dynamic display for "Go To Page". If there are less than 10 address mapping rules, then hide "Go To Page", else display "Go To Page".
31. [ENHANCEMENT] When we receive a non-encrypt initial content payload in IKE, we will ignore it.
32. [ENHANCEMNET] Add payload information in IKE LOG. Besides reason, we also show which payload caused the IKE LOG.
33. [ENHANCEMENT] HOME>Internet Access, the "First DNS Server", "Second DNS Server" is inconsistent with DNS>Name Server Record.
    The specified "First DNS Server", "Second DNS Server" will be updated in eWC>DNS>Name Server Record.
34. [ENHANCEMENT] In GUI>WAN, add "Authentication Type" field.
35. [ENHANCEMENT] For DHCP server, if the requested client does not have a host name, the log will show MAC address instead of nothing.
36. [ENHANCEMENT]
    (1) In eWC>CONTENT FILTER>Cache, if users click Action/URL/Remaining Time to sort the cache entries, the page will not jump to the top of this page before it refreshes.
    (2) By using Firefox/Netscape in eWC>CONTENT FILTER>Cache, if useres click Action/URL/Remaing Time to sort the cache entries, the page will refresh immediately.
37. [ENHANCEMENT] In the past, we can delete a tunnel in SMT 27 and can only do this in eWC. Now, Add a CI command "ipsec drop <policy index>" to delete a tunnel and "ipsec show_runtime list" to list the active VPN tunnel.
38. [ENHANCEMENT] Consolidate "Receive IPSec packet, but no corresponding tunnel exists" logs.

Modifications in V3.62(XD.2) | 09/24/2004
Modify for formal release.

Modifications in V3.62(XD.2)b3 | 09/21/2004
1. [BUG FIX]
   Symptom: LAN host will get wrong DNS server.
   Condition:
   1. Set SMT 3.2 DNS first DNS server as user defined 1.1.1.1. Others are none.
   2. Unplug WAN port and reboot.
   3. LAN host get IP address and DNS server and the DNS server is LAN IP.

Modifications in V3.62(XD.2)b2 | 09/17/2004
1. [BUG FIX]
   Symptom: LAN host ping device LAN IP a period time, then PPPoE/PPTP will be triggered dial.
   Condition:
   1. Set WAN 1 are PPPoE.
   2. LAN host ping device LAN IP a period time, then WAN 1 will be triggered dial.
2. [BUG FIX]
   Symptom: Firewall sends TCP RST after it blocks traffic period of time.
   Condition:
   1. Configure Firewall LAN to WAN blocked and enable log
   2. Generate one TCP SYN packet from LAN to WAN
   3. Firewall will block this packet and generate block log
   4. After period of time (30 seconds), Firewall log shows it sent TCP RST to both client and server side
3. [BUG FIX]
   Symptom: System has a lot of long timeout UDP sessions.
   Condition:
   1. Enable firewall.
   2. Display TOS sessions.
   3. A lot of long timeout UDP sessions.
4. [BUG FIX]
   Symptom: ZyWALL crashes very often in bridge mode.
   Condition:
   1. Switch to bridge mode.
   2. Enable Firewall.
   3. ZyWALL crashes very often.
5. [ENHANCEMENT] Enhance "cnm keepalive" ci command. Add "cnm keepalive 0" command to stop sending of keepalive packet to Vantage.
6. [BUG FIX] Symptom: Symptom: FTP from WAN to LAN does not work.

Condition:
1. Set a FTP server on a host in the LAN side and configure a default server to this host.
2. Using FTP from WAN to the default server with port mode.
3. After typing username and password, "ls" command does not work.

7. [BUG FIX] Symptom: LAN host will get wrong DNS server.
   Condition:
   1. Set SMT 3.2 DNS first DNS server as user defined 1.1.1.1. Others are none.
   2. Unplug WAN port and reboot.
   3. LAN host get IP address and DNS server and the DNS server is LAN IP.
8. [BUG FIX] Symptom: System Crash when change encryption key in Vantage.
   Condition:
   1. Device register to Vantage in router mode under DES and PPPoE.
   2. configuration>>general>>system change the original encryption key and apply
   3. Device receives data but soon the system crash.
9. [BUG FIX] Symptom: WAN Gateway will be reset to 0.0.0.0.
   Condition:
   1. In Vantage CNM add a device (the device have a static IP),when it register to Vantage. Vantage set default value to device.
   2. After the device reset, WAN Gateway will be reset to 0.0.0.0.
10. [BUG FIX] Symptom: CNM agent accepts wrong CI command ”cnm keepalive -32312312222222222222222”.
    Condition:
    1. In SMT 24.8, type ”cnm keep -32312312222222222222222”.
    2. The system accepts it and saves with the value.
11. [BUG FIX] Symptom: CNM agent accepts wrong CI command ”cnm encrymode 1231223”.
    Condition:
    1. In SMT 24.8, type ”cnm encrymode 1231223”.
    2. The system accepts it and read it as ”65535”.
12. [BUG FIX] Symptom: [Vantage] Configuration>>VPN: When delete a active VPN tunnel successfully. Device sends VPN tunnel status "Destroy" to vantage.
    Condition:
    1. Create and dial up a VPN tunnel via Vantage.
    2. Delete this active rule in Vantage.
    3. Vantage server will have exception.
13. [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.

Modifications in V3.62(XD.2)b1 | 08/16/2004

1. [ENHANCEMENT]
   Add Unified ALG for SIP and H.323.
2. [ENHANCEMENT]
   Each unified ALG can be enabled/disabled. The default ALG setting for SIP and H.323 is disabled.
3. [ENHANCEMENT]
   Firewall can bypass AX.25 (protocol #93) & IPv6 (protocol #41) protocols.
4. [BUG FIX]
   Symptom: Bandwidth management with ALG_H.323 cause system crash.
   Condition:
   1. Create a class with a Service-H.323 filter in WAN1 interface.
   2. Unplug all WAN's cable
   3. Lanch the "Openphone" application that supports H.323 and make a call.
   4. Router crashes.
5. [BUG FIX]
   Symptom: Router block trusted web content.
   Condition:
   1). In "eWC->CONTENT FILTER->General", enable content filter.
   2). In "eWC->CONTENT FILTER->Customization", select check boxes of "Enable Web site customization" and "Disable all Web traffic except for trusted Web sites".
   3). In "eWC->CONTENT FILTER->Customization", set "www.hellowork.go.jp" as trusted web site.
   4). Open browser and access http://www.hellowork.go.jp/kensaku/servlet/kensaku?pageid=001
   5). In the new page, select third and fourth radio bottom and click "search" bottom.
   6). In the new page, click "next page" bottom.
   7). The new page will be blocked.
6. [BUG FIX]
   Symptom: External Content Filtering cannot block the URL belonging to restricted category.
   Condition:
   1). In "eWC->CONTENT FILTER->Customization", unselect "Enable Web site customization".
   2). Add a URL to "trusted web sites".
   3). In "eWC->CONTENT FILTER-Customization>, select "Block Web sites which contain these keywords".
   4). In "eWC->CONTENT FILTER->Categories", select the category which the URL belongs to.
   5). Access the trusted URL.
   6). The URL will not be blocked.
7. [BUG FIX]
   Symptom: System crash by memory leak.
   Condition:
   1). Enable bandwidth management.
   2). Into eWC->Bandwidth Management->Monitor and wait for a period time.
   3). System crash by memory leak.

8. [BUG FIX]
   Symptom: Remote node CI command crashes.
   Condition:
   1). Goto SMT 24.8
   2). Load dial backup remote node to working buffer.
   3). Type CI command "sys rn accessblock 0".
   4). Save this remote.
   5). System crashes.
9. [BUG FIX]
   Symptom: System crash when someone want to configure NAT mapping rules.
   Condition:
   1. Use the terminal program to login the console.
   2. Enter SMT 15, NAT Setup
   3. Select 1 to enter SMT 15.1, Address Mapping Sets.
   4. The system crash
10. [BUG FIX]
    Symptom: eWC>NAT>ADDRESS MAPPING edit page leaks memory.
    Condition:
    1. Log on to eWC.
    2. Go to eWC>NAT>ADDRESS MAPPING edit page, and then click Cancel.
    3. Repeat Step 2 for several times.
    4. Check system memory info by the CI command: system memu ms You will observe abnormal increases of memory sections, indicating memory leaks.
11. [BUG FIX]
    Symptom: Trigger port will disappear after system reboot.
    Condition:
    1. Configure Trigger port rule.
    2. System reboot.
    3. The configured Trigger port rule disappear.
12. [BUG FIX]
    Symptom: The system might crash when enabling IPSec.
    Condition: During IKE negotiation the system might crash.
13. [BUG FIX]
    Symptom: MSN Messenger's "Ask for Remote Assistance" function causes system crash.
    Condition:
    1. Enable UPnP.
    2. Set PC(A) and router(B) in intranet and PC(C) connects to LAN port of router(B).
    3. Test MSN Messenger's "Ask for Remote Assistance" function from PC(A) to PC(C).
    4. After PC(C) accepts the PC(A) request by "Ask for Remote Assistance" then the device will crash.
14. [BUG FIX]
    Symptom: System out of memory.
    Condition:
    1. Let the ZyWALL be a DNS proxy for LAN hosts.

2. Do a lot of DNS inverse queries by running IPScan tool continuously from LAN host.
3. After a long time, the ZyWALL will out of memory.

15. [FEATURE CHANGE]
    Change UPnP device name for ZyWALL35 and ZyWALL5
    WAS: "ZyXEL ZyWALL 35 Internet Security Gateway"
    IS: "ZyXEL ZyWALL 35 Internet Security Appliance"
16. [BUG FIX]
    Symptom: Packets cannot pass through NAT router to LAN hosts.
    Condition:
    1. NAT default server is on
    2. Procotol of the packet is not TCP, UDP, ICMP, ESP, GRE.
    3. Packets from WAN to router.
    4. Packets cannot pass through NAT router to LAN hosts (NAT default server)
17. Symptom: External Content filtering cannot register.
    Condition:
    1. In "eWC->content filter->categories", click "register" to connect to ZSSW.
    2. Do the registration on ZSSW.
    3. The registration will fail in the final step.
18. [ENHANCEMENT]
    External content filtering support full URL checking.
    Was: External content filtering only take domain name or IP address of URL into category checking.
    Is: External content filtering put entire URL into category checking.
19. [ENHANCEMENT]
    CI command to turn off triangle route log, multicast log and broadcast log.
    1. Add CI commands:
    a. "sys logs switch".
    b. "sys logs switch display".
    c. Triangle route log switch: "sys logs switch bmlog <0:no|1:yes>"
    d. Broadcast/Multicast log switch: "sys logs switch trilog <0:no|1:yes>".
20. [BUG FIX]
    Symptom: System time problem.
    Condition:
    1. enter SMT24.10, configure time server.
    2. open daylight saving, configure the start time and end time so that current time is within the daylight saving time.
    3. after writing to rom file, router ask you to calibrate the system clock, answer yes.
    4. If system failed to connect time server, system time will add one hour, every time you enter smt 24.1,system time add 1 hour automatically.
21. [FEATURE CHANGE]
    Change external content filtering message on centralized log and blocked page for some error events.
22. [BUG FIX]
    Symptom: Router will crash.
    Condition: When user continuously accesses eWC and press "Apply" button,

sometimes router will crash.

23. [BUG FIX]
    Symptom: The system crashes after it receives a url that contains more than three "/"s behind the ip address (or domain name).
24. [BUG FIX]
    Symptom: Sometimes when connect to router by TCP, FTP or HTTP will fail.
    Condition:
    1. One user connects to router by FTP, TELNET or HTTP.
    2. In TCP handshake, client doesn't receive SYN ACK. i.e., router is in SYN RECEIVE state.
    3. Client timeout and send RESET to router.
    4. Related socket in router is still alive and other users can't login router until this socket timeout.
25. [BUG FIX]
    Symptom: eWC spelling error: eWC->Firewall→Default Rule: Allow Asymetrical should be “Asymmetric”
26. [BUG FIX]
    Symptom: System out of memory and reboot when firewall enable.
    Condition:
    1. Enable firewall, then generate traffic.
    2. The memory will slowly leak until it uses up all the memory, then reboot.
27. [BUG FIX]
    Symptom: Generate a lot of TCP port 80 sessions to ZyWALL will cause device to hang and reboot by hardware watchdog.
    Condition:
    1. Use session.exe to generate a lot of TCP port 80 sessions to ZyWALL's LAN or WAN interface
    2. After several hundreds of sessions are established, the ZyWALL will hang and finally reboot.
28. [ENHANCEMENT]
    1. Support user config for SIP session timeout value.
    2. Support SIP SDP multiple RTP port.
    3. Delete unused ALG type.
    4. Command for ALG enable/disable and sip timeout.
29. [BUG FIX]
    Symptom: Sometimes the ZyWALL reboots by software watchdog.
    Condition:
    1.Put the ZyWALL on the network for a long time.
    2.Sometimes the ZyWALL will reboot by software watchdog.
30. [BUG FIX]
    Symptom: XAUTH with rule swap doesn’t work.
    Condition:
    1. In initiator, set up a VPN rule with XAUTH in client mode.
    2. In responder, there are three VPN rules:
    a. Rule 1 is XAUTH off.
    b. Rule 2 is XAUTH with client mode.

c. Rule 3 is XAUTH with server mode (this rule corresponds to client rule).
3. Dial from initiator, and the tunnel will never be up.

31. [BUG FIX]
Symptom: Content filter timeout problem.
Condition:
1. A router is register the content filter (CF) server.
2. Enable the CF feature.
3. Enable the external database content filtering.
4. The router log often record "Waiting content filter server (server name) timeout!".
5. A PC in lan fetch web from internet often hang for a while.

Modifications in V3.62(XD.1) | 06/25/2004

1. Formal release.

Modifications in V3.62(XD.1)b1 | 06/16/2004

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

Modifications in V3.62(XD.0) | 05/18/2004

1. Formal release.

Modifications in V3.62(XD.0)b5 | 05/14/2004

1. [BUG FIX] Symptom: The ZyWALL might crash or hang when users browse eWC→Firewall→Rule Summary.
Condition:
(1) Log on to eWC.
(2) Browse Ewc→Firewall→Rule Summary
(3) The ZyWALL might crash or hang.

Modifications in V3.62(XD.0)b4 | 04/27/2004

1. [FEATURE CHANGE]
Remove Policy Route feature from ZyWALL 5 because Policy Route is not defined in product specification.
2. [FEATURE CHANGE]
Maximum concurrent VPN tunnel number is changed from 5 to 10.
3. [FEATURE CHANGE]

The following default settings is changed:
(1) eWC→Firewall→Anti-Probing
WAS: Anti-Probing Respond Ping to LAN
IS: Anti-Probing Response Ping to LAN&WAN&DMZ
(2) eWC→Firewall→Threshold
WAS: TCP Maximum Incomplete Sessions = 10
IS: TCP Maximum Incomplete Sessions = 30
(3) eWC→WAN→Route
WAS: WAN Priority = 2
IS: WAN Priority = 1

4. [BUG FIX]
   Symptom: External Content Filtering cannot be registered.
   Condition:
   (1) In eWC→CONTENT FILTER→Categories", click "register" to connect to ZSSW.
   (2) Do the registration on ZSSW.
   (3) Browser display "Please wait....." and the page of "Register successfully" does not appear.
5. [BUG FIX]
   Symptom: Traffic Redirect does not work.
   Condition:

   Internet ------- Router A ------ ZyWALL ----- gateway B ----- Internet
   WAN LAN

   (1) Let ZyWALL WAN port connect to another router A and A is connected to Internet.
   (2) Setup Traffic Redirect to backup gateway B located at LAN side.
   (3) Disconnect the connection between router A and Internet.
   (4) The ZyWALL can not do Traffic Redirect to gateway B located at LAN side.
6. [BUG FIX]
   CI command “ip igmp” is lost.
7. [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 WAN1-2 has higher priority than WAN1-2.
8. [BUG FIX]
   Symptom: In eWC→MAINTENANCE→General, set a number which is bigger than 1000 for Administrator Inactivity Timer. The label string 'Administrator Inactivity

Timer' will disappear.
Condition:
(1) Go to eWC→MAINTENANCE→General, set a number which is bigger than 1000 for Administrator Inactivity Timer.
(2) Click 'Apply'.
(3) The label string 'Administrator Inactivity Timer' will disappear.

9. [BUG FIX]
   Symptom: ZyWALL ping sometimes fails.
   Condition:
   (1) Turn on Firewall.
   (2) Go to SMT 24.8
   (3) Ping to exist host, but it sometimes fails.
10. [BUG FIX]
    Symptom: In SMT 3.2, the subnet of ZyWALL LAN IP can be different from the subnet of DHCP client ip and ZyWALL LAN IP can be set within DHCP Client IP pool range.
    Condition:
    First case:
    (1) Go to SMT 3.2
    (2) Set DHCP client IP Starting address to be 192.168.2.3
    (3) Set LAN IP Address to be 192.168.1.1, then confirm to save.
    (4) These setting can be saved and no error message.
    Second case:
    (1) In SMT 3.2, set DHCP client ip Starting address to be 192.168.1.3
    (2) Set Size of Client IP Pool to be 10
    (3) Set LAN IP Address to be 192.168.1.3, then confirm to save.
    (4) These setting can be saved and no error message.
11. [BUG FIX]
    Symptom: Remote access control cannot work properly.
    Condition:
    (1) Turn on bridge mode
    (2) Configure telnet server access control from WAN only by SMT 24.11
    (3) Telnet to device via WAN side
    (4) The telnet connection fails.
12. [BUG FIX]
    Symptom: System crashes.
    Condition: Configure device by eWC sometimes cause crash.
13. [BUG FIX]
    Symptom: In bridge mode ZyWALL at eWC→Bridge, Bridge IP address settings can not be saved successfully.
    Condition:
    (1) Switch the ZyWALL to bridge mode.
    (2) Go to eWC→Bridge page.
    (3) Change "IP Address", "IP Subnet Mask", or "Gateway IP Address" then click "Apply"
    (4) Status shows "Configuration updated successfully" but the changes was not really

saved.

14. [BUG FIX]
    Symptom: In SMT 24.11, the setting of DNS Service is displayed under bridge mode
    Condition:
    (1) Go to SMT 1, change Device Mode to bridge mode.
    (2) After reboot, go to SMT 24.11, DNS Service incorrectly appear.

Modifications in V3.62(XD.0)b3 | 04/04/2004

1. [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".
2. [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.
3. [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.
4. [BUG FIX]
   Symptom: Router will crash when entering SMT menu 3.5
   Condition:
   (1) Insert WLAN card.
   (2) In CI command, enter "wlan active 11" instead of "wlan active 1" to activate WLAN on router.
   (3) Enter SMT 3.5, router will crash.

5. [ENHANCEMENT]
   Supports Vantage CNM 2.0(Vantage Centralized Network Management)
6. [BUG FIX]
   Symptom: The Content Filtering blocks cookies even if it is not in the blocked schedule.
   Condition:
   (1) In eWC→CONTENT FILTER→General, select "Block Cookies".
   (2) In eWC→CONTENT FILTER→General, set "Schedule to Block" with a time period NOT including the current time.
   (3) Access a web site which contains cookies.
   (4) The cookies will be blocked by the Content Filtering.
7. [BUG FIX]
   Symptom: WAN status in SMT 24.1 shows wrong information in bridge mode.
   Condition:
   (1) Configure Internet access as PPTP or PPPoE encapsulation in router mode.
   (2) Switch ZyWALL to bridge mode.
   (3) WAN status in SMT 24.1 shows idle and IP address is "0.0.0.0".
8. [BUG FIX]
   Symptom: Device cannot transfer Ethernet frame in bridge mode.
   Condition:
   (1) ZyWALL enables bridge mode.
   (2) The Internet connection is under DMZ port.
   (3) Plug Ethernet cable between one host and ZyWALL DMZ port.
   (4) This host starts to transfer packets to Internet.
   (5) Unplug the Ethernet cable from DMZ port and plug in LAN port.
   (6) This host cannot transfer packets to Internet anymore.
9. [BUG FIX]
   Symptom: PPPoE connection sometimes fails in France.
   Condition: Since France Telecom changes their core network setup to BRAS, ZyWALL PPPoE connection on authentication phase most of the time fails.
10. [ENHANCEMENT]
    Updates help pages for ZyWALL 5.
11. [BUG FIX]
    Symptom: On the eWC→WIZARD→Internet Access page, the System DNS Servers configuration is not available when the ZyWALL is not a DHCP server for its LAN hosts.
    Condition:
    (1) Log onto eWC, and go to eWC→LAN. Uncheck the "DHCP Server" option to stop ZyWALL from being a DHCP server to its LAN hosts.
    (2) Go to eWC→HOME→WIZARD→Internet Access. The System DNS Servers configuration is not available in the wizard.
12. [ENHANCEMENT]
    The ZyWALL 5 Firewall GUI are enhanced as follows.
    (1) On eWC→Firewall→Rule Summary→Edit Rule, a basic sanity check on the firewall rule is performed.
    (2) On eWC→Firewall→Rule Summary→Edit Rule, the selected service for a new rule is empty by default.

(3) On eWC→Firewall→Rule Summary→Edit Rule, the useless headers "####### Source IP Address #######" and "#### Destination IP Address #####" are removed.
(4). On eWC→Firewall→Rule Summary→Edit Rule, when a specific address is added to the Source/Destination Address list, the "Any" address will automatically be deleted.
(5) On eWC→Firewall→Rule Summary→Edit Rule, the firewall action radio buttons are replaced by a dropdown list.
(6) On eWC→Firewall→Threshold, the "Cancel" button is replaced by "Reset" button.
(7) On eWC→Firewall→Deafult Rule, the wording "Default Rule Settings" is replaced by "Deafult Rule Setup".
(8) On eWC→Firewall→Anti-Probing, the wording "Anti-Probing Settings" is replaced by "Anti-Probing Setup".
(9) "ACCESS POLICY" is renamed as "FIREWALL".
(10) "CUSTOM PORT" is renamed as "CUSTOM SERVICE".
(11) Users can expand or collapse "Source Address", "Destination Address" and "Service Type" drop down lists by clicking the [+]/[-] icon at the beginning of each rule in Firewall Rule Summary Table.

Modifications in V3.62(XD.0)b2 | 03/26/2004

1. [BUG FIX]
   Symptom: In eWC→FIREWALL→ACCESS POLICY→EDIT RULE, Action for Matched Packets can't be saved correctly.
   Condition:
   (1) Go to eWC→FIREWALL→ACCESS POLICY→EDIT RULE
   (2) Choose the type of Action for Matched Packets as Block, and then click Apply.
   (3) Leave this page and then re-enter this page again, Action for Matched Packets always shows Forward.
2. [ENHANCEMENT]
   Supports Intel TE28F640 J3C120 Flash ROM.

Modifications in V3.62(XD.0)b1 | 03/11/2004

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.

Note

(1) DNS Service is not available in Bridge Mode.

```
                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.

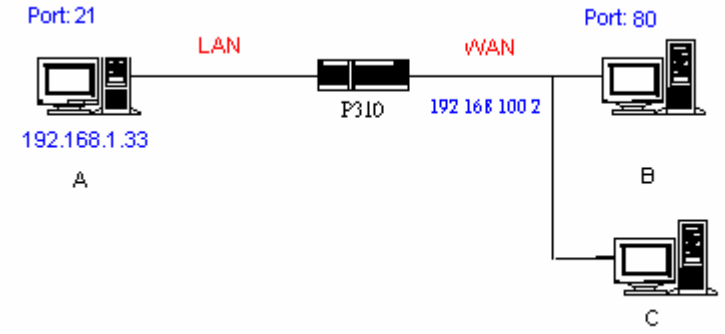
These triggered events can be timed so that they erase the port mapping as soon as they are done with the data transfer, so that the port mapping can be triggered by another Client computer. This gives the ***illusion*** that multiple computers can use the same port mapping at the same time, but the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

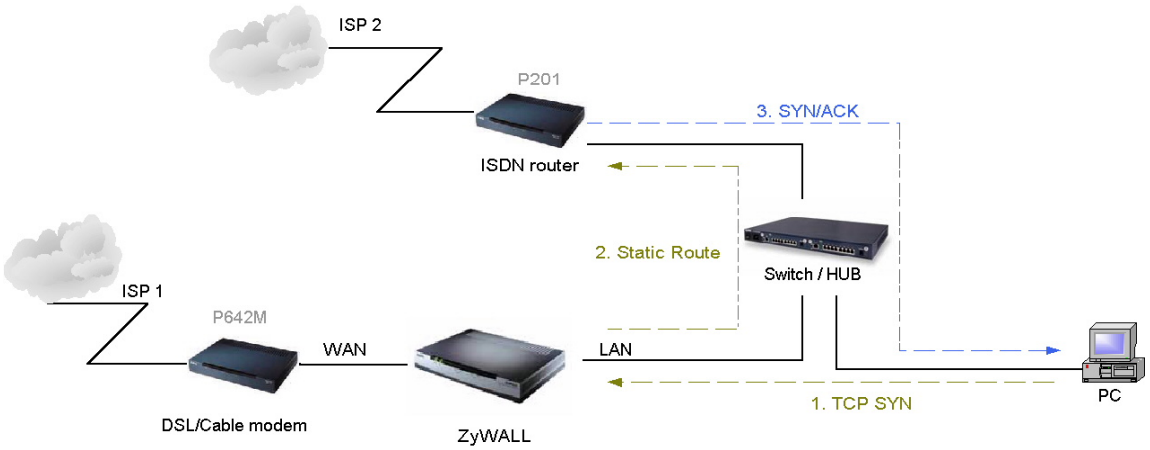


Figure 4-1 Triangle Route

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

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

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

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

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

That causes all of outgoing TCP traffics being reset!

How traffic redirect/static route works under protection - Solutions

(1) Gateway on alias IP network

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

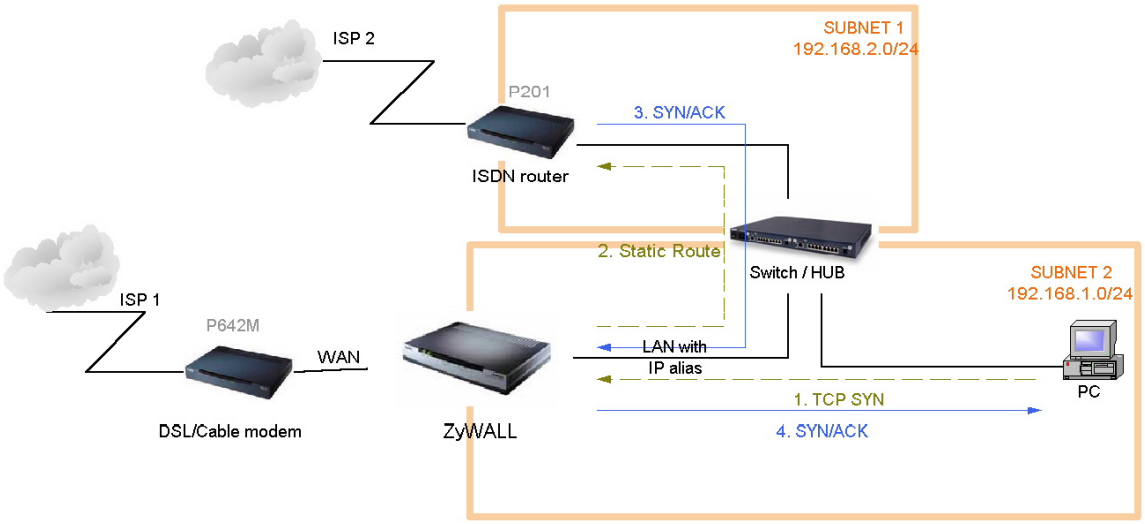


Figure 4-2 Gateway on alias IP network

(2) Gateway on WAN side

A working topology is suggested as below.

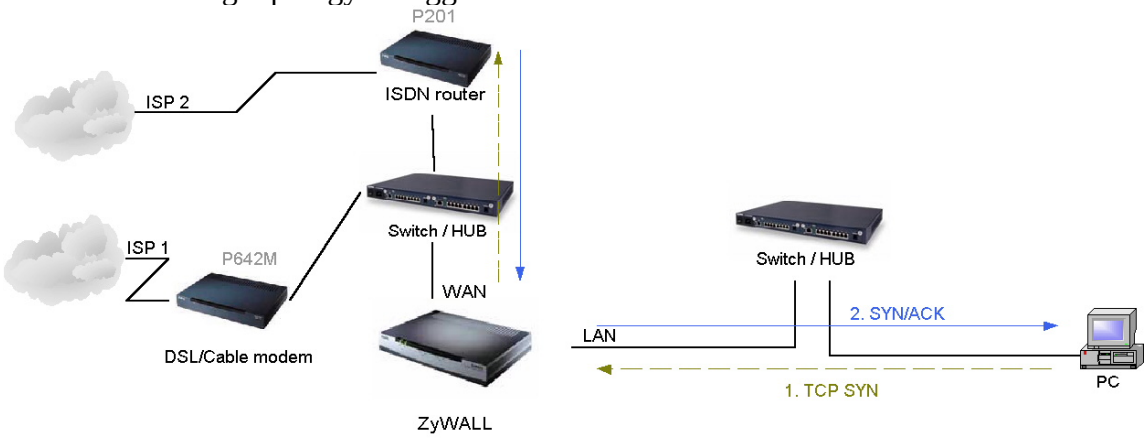


Figure 5-3 Gateway on WAN side

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 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 8 IPSec IP Overlap Support

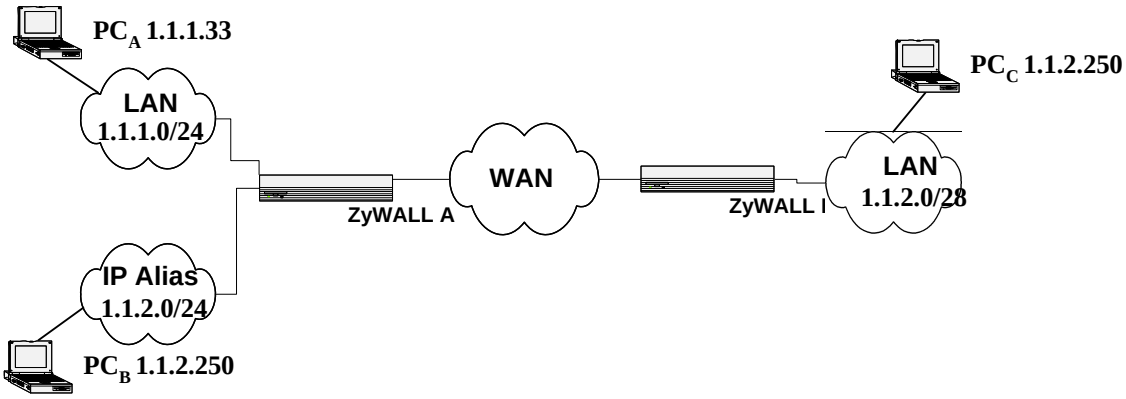


Figure 1

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 9 VPN Local IP Address Limitation

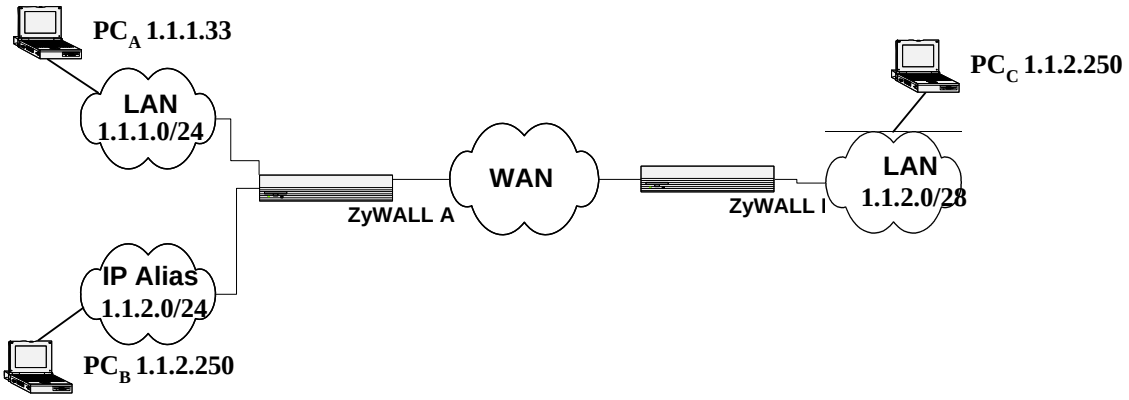


Figure 1

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 10 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

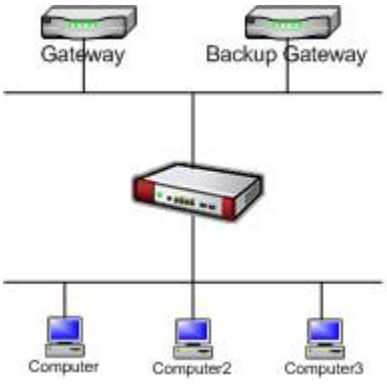
ZyXEL VPN Client
Security Gateway: 1.1.1.1 Phase one Authentication method: Preshare Key Remote: 192.168.1.0/24

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”.

Appendix 11 The mechanism of Gratuitous ARP in the ZyWALL



In the past, if the ZyWALL gets a gratuitous ARP it will not update the sender's MAC mapping into its ARP table. In current design, if you turn on 'ip arp ackGratuitous active yes', the ZyWALL will response such packet depends on two case: 'ip arp ackGratuitous forceUpdate on' or 'ip arp ackGratuitous forceUpdate off'. if you turn on forceUpdate, then the ZyWALL gets gratuitous ARP, it will force to update MAC mapping into the ARP table, otherwise if turn off forceUpdate, then the ZyWALL gets gratuitous

ARP, it will update MAC mapping into the ARP table only when there is no such MAC mapping in the ARP table.

Give an example for its purpose, there is a backup gateway on the network as the picture. One day, the gateway shuts down and the backup gateway is up, the backup gateway is set a static IP as original gateway's IP, it will broadcast a gratuitous ARP to ask who is using this IP. If ackGratuitous is on, the ZyWALL receive the gratuitous ARP from the backup gateway, it will also send an ARP request to ask who is using this IP. Once the ZyWALL gets a reply from backup gateway, it will update its ARP table so that the ZyWALL can keep a correct gateway ARP entry to forward packets. If ackGratuitous is off, the ZyWALL will not keep a correct gateway ARP entry to forward packets.

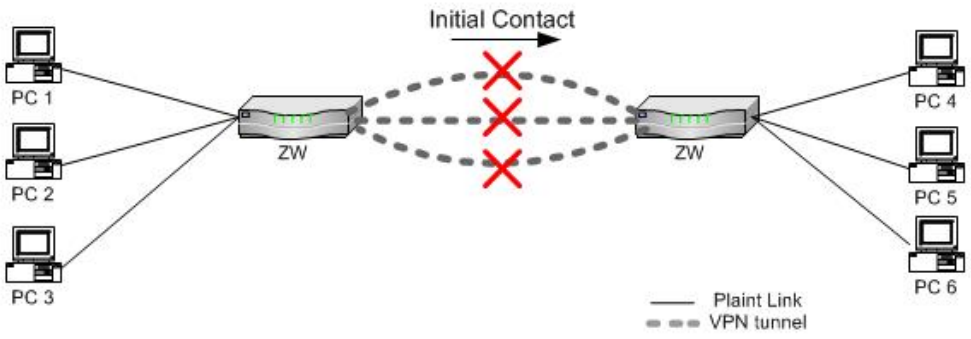
There is one thing need to be noticed: update the ARP entry might still have dangers more or less if there is a spoofing attack. So we suggest if you have no opportunity to meet the problem, you can turn off ackGratuitous. forceUpdate on will be more dangerous than forceUpdate off because it update ARP table even when ARP entry is existing.

Appendix 12 The mechanism when the ZyWALL receives a IKE packets with IC

[RFC 2407]The INITIAL-CONTACT(IC) status message may be used when one side wishes to inform the other that this is the first SA being established with the remote system. The receiver of this Notification Message might then elect to delete any existing SA's it has for the sending system under the assumption that the sending system has rebooted and no longer has access to the original SA's and their associated keying material.

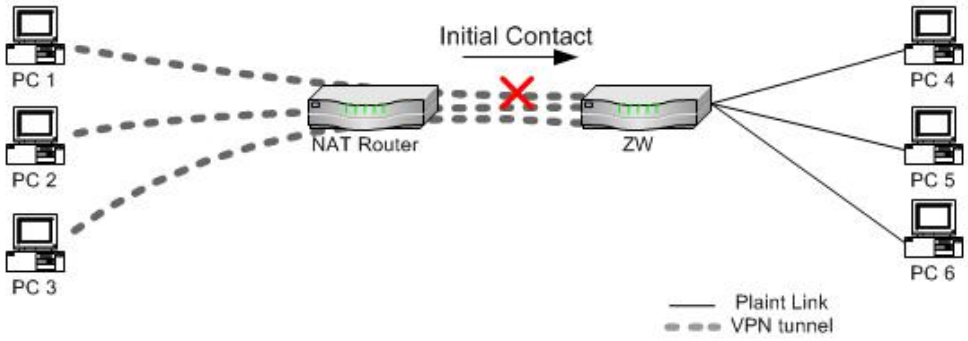
The ZyWALL has two ways to delete SA when it receives IC, it is switched by a global option 'ipsec initContactMode gateway/tunnel':

(1)ipsec initContactMode gateway
When the ZyWALL receives a IKE packets with IC, it deletes all tunnels with the same secure gateway IP. It is default option because the ZyWALL is site to site VPN device. Take the picture 1 as example, there are three VPN tunnels are created between ZWA and ZWB, but ZWA reboots for some reasons, and after rebooting, the ZWA will send a IKE with IC to the ZWB, then the ZWB will delete all existing tunnels whose security gateway IP is the same as this IKE's one and build a new VPN tunnel for the sender.



(2)ipsec initContactMode tunnel

When the ZyWALL receives a IKE packets with IC, it deletes only one existing tunnel, whose security gateway IP is not only the same as this IKE's one and also its phase 2 ID(network policy) should match. It is suitable when your tunnel is created from a VPN peer to ZyWALL and there are more than two this kind of VPN peers build tunnels behind the same NAT router. Take the picture 2 as example, PC 1, PC2 and PC3 has it's own VPN software to create tunnels with ZW. Suppose that the PC1, PC2 and PC3 separately create different tunnels with ZW for the traffic to PC4, PC5 and PC6, once the PC1 reboots for some reasons, and after rebooting, the PC1 sends a IKE with IC to the ZWB, then the ZWB will only delete the tunnel which is used by PC1 and PC4 and build a new VPN tunnel for it. So other tunnels will not be disconnected.



Annex A CI Command List

Last Updated: 2006/04/18

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	myZyXEL.com Command	Anti-Spam Command
IDP Command	Anti-Virus Command	

System Related Command Home

Command				Description
sys				
	atsh			Display system information
	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
	datetime		[year month date]	set/display date
	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	add extra phone numbers

			phone num]	
		display		display extra phone numbers
		node	<num>	set all extend phone number to remote node <num>
		remove	<set 1-3>	remove extra phone numbers
		reset		reset flag and mask
	feature			display feature bit
	fid			
		display		display function id list
	firmware			display ISDN firmware type
	hostname		[hostname]	display system hostname
	iface			
		disp	[#]	display iface list
	interrupt			display interrupt status
	logs			
		category		
			access [0:none/1:log/2:alert/3:both]	record the access control logs
			attack [0:none/1:log/2:alert/3:both]	record and alert the firewall attack logs
			display	display the category setting
			error [0:none/1:log/2:alert/3:both]	record and alert the system error logs
			ipsec [0:none/1:log/2:alert/3:both]	record the access control logs
			ike [0:none/1:log/2:alert/3:both]	record the access control logs
			javablocked [0:none/1:log]	record the java etc. blocked logs
			mten [0:none/1:log]	record the system maintenance logs
			packetfilter [0:none/1:log]	record the packet filter logs
			pki [0:none/1:log/2:alert/3:both]	record the pki logs
			tcpreset [0:none/1:log]	record the tcp reset logs
			upnp [0:none/1:log]	record upnp logs
			urlblocked [0:none/1:log/2:alert/3:both]	record and alert the web blocked logs
			urlforward [0:none/1:log]	record web forward logs
		clear		clear log
		display	[access|attack|error|ipsec|ike|javablocked|mten|packetfilter|pki|tcpreset|urlblocked|urlforward]	display all logs or specify category logs
		dispSvrIP		Display the IP address of email log server and syslog server
		errlog		
			clear	display log error
			disp	clear log error
			online	turn on/off error log online display
		load		load the log setting buffer

		mail		
			alertAddr [mail address]	send alerts to this mail address
			display	display mail setting
			logAddr [mail address]	send logs to this mail address
			schedule display	display mail schedule
			schedule hour [0-23]	hour time to send the logs
			schedule minute [0-59]	minute time to send the logs
			schedule policy [0:full/1:hourly/2:daily/3:weekly/4:none]	mail schedule policy
			schedule week [0:sun/1:mon/2:tue/3:wed/4:thu/5:fri/6:sat]	weekly time to send the logs
			server [domainName/IP]	mail server to send the logs
			subject [mail subject]	mail subject
		save		save the log setting buffer
		syslog		
			active [0:no/1:yes]	active to enable unix syslog
			display	display syslog setting
			facility [Local ID(1-7)]	log the messages to different files
			server [domainName/IP]	syslog server to send the logs
		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
		lastAlert	<index>	display the last #index alert in the centralized 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]	
	md5		<string>	This command will hash the string by MD5. Tha maximum length of the string is 64.
	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
	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
	ProbeType		[icmp | arp]	DHCP server probing type
	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
	pwdHash		<on | off> [newPassword] [oldPassword]	The password saved in ROM file can be hashed by MD5.
	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
		accessblock	[1|0]	Enable/disable block specific remote note packet.
		trigger	[on|off]	
		save	[entry no.]	save remote node information
	smt			not support in this product
	stdio		[second]	change terminal timeout value
	time		[hour [min [sec]]]	display/set system time
	timer			
		disp		display timer cell
	tos			
		display		display all runtime TOS
		listPerHost		display all host session count
		debug	[on|off]	turn on or off TOS debug message
		sessPerHost	<number>	configure session per host value
		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
		tempTOSDisplay		display temporal TOS records.
		tempTOSTimeout	[timeout value]	set/display temporal 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,sds100, 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
	pwderrtm		[minute]	Set or display the password error blocking timeout value.
	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
	threatReport				
		idp			
			active		Active/inactive threat report functionality for IDP
			dump		Dump all entry in memory
			flush		Flush all data and update time stamp
			summary		Show summary
			statistic	id	Show top N statistic records for id field
			statistic	src	Show top N statistic records for source IP field
			statistic	dst	Show top N statistic records for destination IP field
		av			
			active		Active/inactive URM report functionality for AV
			dump		Dump all entry in memory
			flush		Flush all data and update time stamp
			summary		Show summary
			statistic	id	Show top N statistic records for id field
			statistic	src	Show top N statistic records for source IP field
			statistic	dst	Show top N statistic records for destination IP field
		as			
			active		Active/inactive threat report functionality for AS
			dump		Dump all entry in memory
			flush		Flush all data and update time stamp
			summary		Show summary
			statistic	sender	Show top N statistic records for sender mail address field
			statistic	src	Show top N statistic records for source IP field
			statistic	score	Show score distribution for AS

	atmu			Show multiboot client version

Exit Command Home

Command				Description
exit				exit smt menu

Device Related Command
Home

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

Ethernet Related Command Home

Command				Description
ether				
	config			display LAN configuration information
	driver			
		cnt		
			disp <name>	display ether driver counters
			clear <name>	clear ether driver counters
		iface	<ch_name> <num>	send driver iface
		ioctl	<ch_name>	Useless in this stage.
		mac	<ch_name> <mac_addr>	Set LAN Mac address
		reg	<ch_name>	display LAN hardware related registers
		rxmod	<ch_name> <mode>	set LAN receive mode. mode: 1: turn off receiving 2: receive only packets of this interface 3: mode 2+ broadcast 5: mode 2 + multicast 6: all packets
		status	<ch_name>	see LAN status
		init	<ch_name>	initialize LAN
	version			see ethernet device type
	pkttest			
		disp		
			packet <level>	set ether test packet display level
			event <ch> [on|off]	turn on/off ether test event display
		sap	[ch_name]	send sap packet
		arp	<ch_name> <ip-addr>	send arp packet to ip-addr
	test		<ch_id> <test_id> [arg3] [arg4]	do LAN test
	ipmul		<num>	only receive ip multicast and broadcast

				packet
	pncconfig		<ch_name>	do pnc config
	mac		<src_ch> <dest_ch> <ipaddr>	fake mac address
	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
	enque		[size]	set pptp max en-queued size

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
	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
	usrmdn	flag	[1|0]	Enable/disable USR modem capability.

Configuration Related Command

Home

Command					Description
config					The parameters of config are listed below.
edit	firewall	active			Activate or deactivate the saved firewall

		<yes|no>			settings
	custom-service <entry#>	name <string>			Configure selected custom-service with name = <string>
		ip-protocol < icmp | tcp | udp | tcp/udp | user-defined>			Configure IP Protocol Type for selected custom-service
		port-range <start port> <end port>			When ip-protocol = "tcp | udp | tcp/udp ". configure port range for custom-service entry #. For single port configuration, start port equals to end port.
		user-defined-ip <1~65535>			When ip-protocol = "user-defined". Configure user defined IP protocol.
		icmp-type <0~255>			When ip-protocol = "icmp", configure ICMP type.
		icmp-code <0~255>			When ip-protocol = "icmp", configure ICMP code. This field is optional for ICMP.
retrieve	firewall				Retrieve current saved firewall settings
save	firewall				Save the current firewall settings
	custom-service <entry#>				Save the custom service entry specified by <entry#>
	anti-spam				Save current AntiSpam settings
	all				Save all working SPT buffer into flash.
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
	custom-service				Display all configured custom services.
	custom-service <entry #>				Display custom service <entry #>
	anti-spam				Display AntiSpam settings
edit		e-mail	mail-server <mail server IP>		Edit the mail server IP to send the alert
			return-addr <e-mail address>		Edit the mail address for returning an email alert

			e-mail-to <e-mail address>		Edit the mail address to send the alert
			policy <full | hourly |daily | weekly>		Edit email schedule when log is full or per hour, day, week.
			day <sunday | monday | tuesday | wednesday | thursday | friday | saturday>		Edit the day to send the log when the email policy is set to Weekly
			hour <0~23>		Edit the hour to send the log when the email policy is set to daily or weekly
			minute <0~59>		Edit the minute to send to log when the email policy is set to daily or weekly
			Subject <mail subject>		Edit the email subject
		attack	send-alert <yes|no>		Activate or deactivate the firewall DoS attacks notification emails
			block <yes|no>		Yes: Block the traffic when exceeds the tcp-max-incomplete threshold
					No: Delete the oldest half-open session when exceeds the tcp-max-incomplete threshold
			block-minute <0~255>		Only valid when sets 'Block' to yes. The unit is minute
			minute-high <0~255>		The threshold to start to delete the old half-opened sessions to minute-low
			minute-low <0~255>		The threshold to stop deleting the old half-opened session
			max-incomplete-high <0~255>		The threshold to start to delete the old half-opened sessions to max-incomplete-low
			max-incomplete-low <0~255>		The threshold to stop deleting the half-opened session
			tcp-max-incomplete <0~255>		The threshold to start executing the block field
		set <set#>	name <desired name>		Edit the name for a set
			default-permit <forward|block>		Edit whether a packet is dropped or allowed when it does not match the default set
			icmp-timeout <seconds>		Edit the timeout for an idle ICMP session before it is terminated
			udp-idle-timeout <seconds>		Edit the timeout for an idle UDP session before it is terminated
			connection-timeout <seconds>		Edit the wait time for the SYN TCP sessions before it is terminated
			fin-wait-timeout <seconds>		Edit the wait time for FIN in concluding a TCP session before it is terminated
			tcp-idle-timeout		Edit the timeout for an idle TCP session

			<seconds>		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>	Select and edit a destination address range of a packet which complies to this rule.

				<end ip address>	
				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
				custom-ip <desired custom service name>	Type in the desired User Defined IP Protocol custom service.
				custom-icmp <desired custom service name>	Type in the desired ICMP custom service
	anti-spam				
		action	<0|1>		Set the action for Spam Mail: add tag(0) or discard mail(1).
		markString	<spam tag>		Set the Spam tag string. This tag will add to the subject of spam mail.
		externDB	<0|1>		Enable(1)/Disable(0) External Database Query.
		query	<0|1>		Set the action for no spam score: add tag(0) ot discard mail(1).
		queryString	<no spam score tag>		Set the tag string for no spam score. This tag will add to the subject of spam mail.
		threshold	<threshold>		Set the spam score threshold. If the spam

					score is higher than this threshold, this mail will be judge as spam mail.
		switch	<0|1>		Enable(1)/Disable(0) AntiSpam function.
		whiteRule	<0|1>		Enable(1)/Disable(0) AntiSpam White Rule Filter.
		blackRule	<0|1>		Enable(1)/Disable(0) AntiSpam Black Rule Filter.
		phishingString	<Phishing tag>		Set the phishing tag string. This tag will add to the subject of spam mail.
		rule	<rule number>	ip <index> active <0|1> address <ip address> netmask <netmask>	Set the While(1)/Black(2) Rule IP Filter. The <index> is start from 0.
				email <index> active <0|1> data <email address>	Set the While(1)/Black(2) Rule Email Filter. The <index> is start from 0.
				mime <index> active <0|1> header <MIME Header> value <MIME Value>	Set the While(1)/Black(2) Rule MIME Filter. The <index> is start from 0.
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
	anti-spam	blackRule			Remove the AntiSpam Black Rule.
		whiteRule			Remove the AntiSpam White Rule.
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
		ftpPortNum	[port number]	Support a different port number on FTP ALG.
	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.
		gratuitous	<on|off>	Switch the duplicate IP address detection based on Gratuitous ARP
		ackGratuitous	active [yes|no]	Let DUT accept gratuitous ARP request.
			forceUpdate [on|off]	Update the exist MAC mapping to new one.
	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> <name> <0:FQDN|1:wildcard> <0:from ISP group|1:user defined> <isp group idx|ip address>	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> <name> <0:FQDN|1:wildcard> <0:from ISP group|1:user defined> <isp group idx|ip address>	insert dns A record
			insertns <before record idx|-1:new> <*|domain name> <0:from ISP|1:user	insert dns NS record

			defined(public)|2: user defined(private)> <isp group idx|dns server ip>	
			movea <record idx> <record idx>	move dns A record
			movens <record idx> <record idx>	move dns NS record
			dela <record idx>	delete DNS A record
			delns <record idx>	delete DNS NS record
		system cache		
			disp <0:none|1:name|2:type|3:IP|4:refCnt|5:ttl> [0:increase|1:decrease]	display DNS cache table
			flush	flush DNS cache
			negaperiod <second(60 ~ 3600)>	set negative cache period
			negative <0: disable|1: enable>	enable/disable dns negative cache
			positive <0: disable|1: enable>	enable/disable dns positive cache
			ttl <second(60 ~ 3600)>	set positive cache maximum ttl
	Httpd			
		debug	[on|off]	set http debug flag
	icmp			
		echo	[on|off]	set icmp echo response flag
		data	<option>	select general data type
		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
		max-incomplete	[number]	Set the maximum number of TCP incomplete connection.
		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			
		bypass	[LAN/DMZ/WAN] [ON/OFF]	Let lan to lan(for example) packet bypass content filter.
		enable		enable/disable url filter function
		reginfo		
			display	display urlfilter registration information
			name	set urlfilter registration name
			eMail <size>	set urlfilter registration email addr
			country <size>	set urlfilter registration country
			clearAll	clear urlfilter register information
		category		
			display	display urlfilter category
			webFeature [block/nonblock] [activex/java/cookei/webproxy]	block or unblock webfeature
			logAndBlock [log/logAndBlock]	set log only or log and block
			blockCategory [block/nonblock] [all/type(1-14)]	block or unblock type
			timeOfDay [always/hh:mm] [hh:mm]	set block time
			clearAll	clear all category information
		listUpdate		
			display	display listupdate status
			actionFlags [yes/no]	set listupdate or not
			scheduleFlag [pending]	set schedule flag
			dayFlag [pending]	set day flag
			time [pending]	set time
			clearAll	clear all listupdate information
		exemptZone		
			display	display exemptzone information
			actionFlags [type(1-3)][enable/disable]	set action flags
			add [ip1] [ip2]	add exempt range
			delete [ip1] [ip2]	delete exempt range
			reset	clear exemptzone information
		customize		
			display	display customize action flags
			actionFlags [filterList/disableAllExceptTrusted/unblockRWFToTrusted/keywordBlock/fullPath/caseInsensitive/fileName][enable/disab	set action flags

			le]	
			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 refresh	Check whether device had been registered and write the original license key to flash

			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
			aol [on|off]	Turn on/off aol flag
		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
			move <set#> <rule# from> <rule# to>	Move specific acl rule to specific position.
			save <set number>	save a specific acl of set number
		routing	[0:LAN|1:DMZ] [0:no|1:yes]	set NAT routing attributes
		historicalCHigh		Display the historical highest count of concurrent NAT sessions
		historicalHigh		Display the historical highest count of NAT sessions based on per host.
	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> vlcompat [on|off]	turn on/off vlcompat 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	type	<0:Disable | 1:Original on|off | 2:IKE on|off | 3:IPSec [SPI]|on|off | 4:XAUTH on|off | 5:CERT on|off | 6:All>	Turn on|off trace for IPsec debug information
		level	<0:None | 1:User | 2:Low | 3:High>	Set the debug level. Higher number means more detailed.
		display		Show debugging information, include type and level.
	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.
		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.
		wan2	<on|off>	After a packet is IPSec processed and will be sent to WAN2 side, this switch is to control if this packet can be applied IPSec again.
		wlan	<on|off>	After a packet is IPSec processed and will be sent to WLAN side, this switch is to

				control if this packet can be applied IPSec again.
	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.
		list		Display brief runtime phase 1 and phase 2 SA information
	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_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
	updatePeerIp			Force system to update IPSec rules which use domain name as the secure gateway IP right away.
	dial	<policy index>		Initiate IPSec rule <policy index> from ZyWALL box
	enable	<on|off>		Turn on/off IPSec feature
	ikeDisplay	<rule #>		Display IKE rule #, if no rule number assigned, this command will show current working buffer. NOTE: If working buffer is null, it will show error messages. Please ADD or EDIT an IKE rule before display.

	ikeAdd			Create a working buffer for IKE rule.
	ikeEdit	<rule #>		Edit an existing IKE rule #
	ikeSave			Save working buffer of IKE rule to romfile.
	ikeList			List all IKE rules
	ikeDelete	<rule #>		Delete IKE rule #
	ikeConfig	name	<string>	Set rule name (max length is 31)
		negotiationMode	<0:Main | 1:Aggressive>	Set negotiation mode
		natTraversal	<Yes| No>	Enable NAT traversal or not.
		multiPro	<Yes|No>	Enable multiple proposals in IKE 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
		authMethod	<0:PreSharedKey | 1:RSASignature | 2:preShare Key+XAUTH | 3:RSASignature+XAUTH>	Set authentication method in phase 1 in IKE
		preShareKey	<ASCII | 0xHEX>	Set pre shared key in phase 1 in IKE
		certificate	<certificate name>	Set certificate file if using RSA signature as authentication method.
		encryAlgo	<0:DES | 1:3DES | 2:AES>	Set encryption algorithm in phase 1 in IKE
		authAlgo	<0:MD5 | 1:SHA1>	Set authentication algorithm in phase 1 in IKE
		saLifeTime	<seconds>	Set sa life time in phase 1 in IKE
		keyGroup	<0:DH1 | 1:DH2>	Set key group in phase 1 in IKE
		xauth	type <0:Client Mode | 1:Server Mode>	Set client or server mode.
			username <name>	Set xauth user name
			password <password>	Set xauth password
			radius <username> <password>	Ser radius username and password
		ha	enable <on|off>	Enable / disable IPSec HA
			redunSecGwAddr <IP address | Domain name>	Configure redundant remote secure gateway address or domain name
			failback enable <on|off>	Enable or disable “Fail back to primary secure gateway when possible”
			failback interval <number>	Configure the check interval for fail back detection
			failover display	Display current fail over detection method
			failover dpd <on|off>	Enable / disable fail over by DPD
			failover outputIdleTime <on|off>	Enable / disable fail over by output idle timer
			failover pingCheck <on|off>	Enable / disable fail over by ping check

	ipsecDisplay	<rule #>		Display IPSec rule #, if no rule number assigned, this command will show current working buffer. NOTE: If working buffer is null, it will show error messages. Please ADD or EDIT an IPSec rule before display.
	ipsecAdd			Create a working buffer for IPSec rule.
	ipsecEdit	<rule #>		Edit IPSec rule #
	ipsecSave			Save working buffer of IPSec rule to romfile.
	ipsecList			List all IPSec rules
	ipsecDelete	<rule #>		Delete IPSec rule #
	ipsecConfig	name	<string>	Set rule name. (max length is 31)
		active	<Yes | No>	Set active or not
		saIndex	<index>	Bind to which IKE rule.
		multiPro	<Yes | No>	Enable multiple proposals in IPSec or not
		nailUp	<Yes | No>	Enable nailed-up or not
		activeProtocol	<0:AH | 1:ESP>	Set active protocol in IPSec
		encryAlgo	<0:Null | 1:DES | 2:3DES | 3:AES>	Set encryption algorithm in IPSec
		encryKeyLen	<0:128 | 1:192 | 2:256>	Set encryption key length in IPSec
		authAlgo	<0:MD5 | 1:SHA1>	Set authentication algorithm in IPSec
		saLifeTime	<seconds>	Set sa life time in IPSec
		encap	<0:Tunnel | 1:Transport>	set encapsulation in IPSec
		pfs	<0:None | 1:DH1 | 2:DH2>	set pfs in phase 2 in IPSec
		antiReplay	<Yes | No>	Set anitreplay or not
		controlPing	<Yes|No>	Enable control ping or not
		logControlPing	<Yes|No>	Enable logging control ping events or not
		controlPingAddr	<IP>	Set control ping address
		protocol	<1:ICMP | 6:TCP | 17:UDP>	Set protocol
		lcAddrType	<0:single | 1:range | 2:subnet>	Set local address type
		lcAddrStart	<IP>	Set local start address
		lcAddrEndMask	<IP>	Set local end address or mask
		lcPortStart	<port>	Set local start port
		lcPortEnd	<port>	Set local end port
		rmAddrType	<0:single | 1:range | 2:subnet>	Set remote address type
		rmAddrStart	<IP>	Set remote start address
		rmAddrEndMask	<IP>	Set remote end address or mask
		rmPortStart	<port>	Set remote start port
		rmPortEnd	<port>	Set remote end port
	policyList			List all IPSec policies
	manualDisplay	<rule #>		Display manual rule #

	manualAdd			Add manual rule
	manualEdit	<rule #>		Edit manual rule #
	manualSave			Save IPSec rules
	manualList			List all IPSec rule
	manualDelete	<rule #>		Delete IPSec rule #
	manualConfig	name	<string>	Set rule name
		active	<Yes | No>	Set active or not
		myIpAddr	<IP address>	Set my IP address
		secureGwAddr	<IP address>	Set secure gateway
		protocol	<1:ICMP | 6:TCP | 17:UDP>	Set protocol
		lcAddrType	<0:single | 1:range | 2:subnet>	Set local address type
		lcAddrStart	<IP>	Set local start address
		lcAddrEndMask	<IP>	Set local end address or mask
		lcPortStart	<port>	Set local start port
		lcPortEnd	<port>	Set local end port
		rmAddrType	<0:single | 1:range | 2:subnet>	Set remote address type
		rmAddrStart	<IP>	Set remote start address
		rmAddrEndMask	<IP>	Set remote end address or mask
		rmPortStart	<port>	Set remote start port
		rmPortEnd	<port>	Set remote end port
		activeProtocol	<0:AH | 1:ESP>	Set active protocol in 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
		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
	manualPolicyList			List all manual policy
	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”.
	swFwScan	<on|off>		Enable / disable to skip firewall packet inspection for IPSec packet.

	swIdpScan	<on|off>		Enable / disable the IDP for IPSec packet.
	swAvScan	<on|off>		Enable / disable the Anti Virus for IPSec packet.
	swAsScan	<on|off>		Enable / disable the Anti Spam for IPSec packet.
	swCfScan	<on|off>		Enable / disable the Content Filter for IPSec packet.
				-
				-
				-
				-
				-
				-
				-
				-
	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.
	ha	pingRetryCnt	<value> (1~10)	Ping retry fail tolerence
		debug	<on|off|runtime|spt>	On: turn on debug message Off: turn on debug message Runtime: show runtime data structure Spt: show SPT record data
	Drop		<policy index>	Drop an active tunnel.
	swSkipPPTP		[on|off]	Enable / disable to skip PPTP packets to go in ipsec tunnel.
	initContactMode		<gateway|tunnel>	Set initial contact mode to base on tunnel or gateway. Change to tunnel mode can support multiple VPN client which located at same NAT router.
	async	active	<on|off>	Enable / disable the asynchronous mode
		utility		Crypto engine utility rate
		queue	<on|off>	Enable / disable the asynchronous queue function
		display		Asynchronous mode function status
		debug	<on|off>	Show asynchronous debug message
	swDevTri		<on|off>	Enable / disable device trigger tunnel

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.
		active	<yes|no>		Active firewall or deactivate firewall
		cnt			
			disp		Display firewall log type and count.
			clear		Clear firewall log count.
		dynamicrule			SUPPORT_DYNAMIC_PORT
			timeout		Set dynamic ACL rule timeout value
		dos			
			smtp		Set SMTP DoS defender on/off

			display		Display SMTP DoS defender setting.
			ignore		Set if firewall ignore DoS in lan/wan1/wan2/dmz/wlan/vpn
		ignore			
			logBroadcast	<from> <to> <on|off>	Set ignore log broadcast flag. The <from> and <to> parameters include lan/wan1/wan2/dmz/wlan/vpn.
			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		
			self_signed <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>	Create a certificate request and save it to the

			<subject> [key size]	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_self_signed [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.
		replace_factory		
	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.
	vpnTraffic			<on|off>		Change BWM classifier do classify based on inner protocol header or IPSec header.
	packetBased			<on|off>		Change BWM classifier based on stream based or packet based

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
	fcs		<BriFcsCtl>	set bridge fcs control flag
	rstp			
		bridge		
			enable	enable this device RSTP function
			disable	disable this device RSTP function
			priority [pirority]	set RSTP pirority
			maxAge [max age]	set RSTP max age
			helloTime [hello time]	set hello time
			forwardDelay [forwarding delay]	set forwarding delay
			version <STP:0|RSTP:2>	switch STP or RSTP
		port		
			enable <Port_NO>	enable RSTP on this port
			disable <Port_NO>	disable RSTP on this port
			pathCost <Port_NO> [path cost]	set path cost on this port
			pirority <Port_NO> [pirority]	set pirority on this port
			edgePort <Port_NO>	set edge or non-edge on this port

			<True:1|False:0>	
			p2pLink <Port_NO> <Auto:2|True:1|False:0>	set per to per link on this port
			mcheck <Port_NO>	set migrate check on this port
		disp		display RSTP information
		trace		turn on debug/trace message
		state		display RSTP information

myZyXEL.com Command Home

Command				Description
sys				
	myZyxelCom			
		checkUserName	<username>	Check the username exists or not
		register	<username> <password> <email> <countryCode>	Inout the registration information, include username, password, email, and country code.
		trialService	<service>, 1 : CF, 2 : 3in1, 3 : CF + 3in1	Input the service that to be tried.
		serviceUpgrade	<licence key>	Inout license key that you want to let service from trial to standard
		serviceRefresh	NULL	Refresh the myZyXEL.com service status
		display	NULL	Display all myZyXEL.com setting
		serviceDisplay	NULL	Display all service status, include expired day.

IDP Command Home

Command					Description
idp					IDP CI commands
	display				Display the enable setting and the protected interface setting
	load				Load the enable setting and the protected interface setting
	config				Config the enable setting and the protected interface setting
		enable	<on|off>		Config the enable setting.
		lan-lan	<on|off>		Config the protected interface setting.
		lan-wan	<on|off>		Config the protected interface setting.
		lan-dmz	<on|off>		Config the protected interface setting.
		lan-wan2	<on|off>		Config the protected interface setting.
		lan-wlan	<on|off>		Config the protected interface setting.
		wan-lan	<on|off>		Config the protected interface

					setting.
		wan-wan	<on|off>		Config the protected interface setting.
		wan-dmz	<on|off>		Config the protected interface setting.
		wan-wan2	<on|off>		Config the protected interface setting.
		wan-wlan	<on|off>		Config the protected interface setting.
		dmz-lan	<on|off>		Config the protected interface setting.
		dmz-wan	<on|off>		Config the protected interface setting.
		dmz-dmz	<on|off>		Config the protected interface setting.
		dmz-wan2	<on|off>		Config the protected interface setting.
		dmz-wlan	<on|off>		Config the protected interface setting.
		wan2-lan	<on|off>		Config the protected interface setting.
		wan2-wan	<on|off>		Config the protected interface setting.
		wan2-dmz	<on|off>		Config the protected interface setting.
		wan2-wan2	<on|off>		Config the protected interface setting.
		wan2-wlan	<on|off>		Config the protected interface setting.
		wlan-lan	<on|off>		Config the protected interface setting.
		wlan-wan	<on|off>		Config the protected interface setting.
		wlan-dmz	<on|off>		Config the protected interface setting.
		wlan-wan2	<on|off>		Config the protected interface setting.
		wlan-wlan	<on|off>		Config the protected interface setting.
	save				Save the enable setting and the protected interface setting
	tune				The tune command for IDP/Anti-Virus/Anti-Spam
		Load			Load the tune configuration
		Save			Save the tune configuration
		display			Display the tune configuration
		config			Config the tune configuration
			14Udpcksum	<on|off>	Enable/Disable UDP checksum check

			14Icmpcjsum	<on|off>	Enable/Disable ICMP checksum check
			14Tcpcksum	<on|off>	Enable/Disable TCP checksum check
			14Tcpwindowck	<on|off>	Enable/Disable TCP window check
			14Tcpmssck	<on|off>	Enable/Disable TCP mss check
			17Smtpasm	<on|off>	Enable/Disable TCP assembly for SMTP
			17Pop3asm	<on|off>	Enable/Disable TCP assembly for POP3
			17Httpasm	<on|off>	Enable/Disable TCP assembly for HTTP
			17Ftpasm	<on|off>	Enable/Disable TCP assembly for FTP
			17Ftpdataasm	<on|off>	Enable/Disable TCP assembly for FTPDATA
			17Otherasm	<on|off>	Enable/Disable TCP assembly for other protocols
	update				The command about signature and signature update stuffs
		display			Show the signature information and the update setting
		load			Load the signature update setting
		save			Save the signature update setting
		start			Start the signature update
		config			Config the signature update setting
			autoupdate	<on|off>	Enable/Disable the autoupdate
			method	<1-3>	Config the update method
			dailyTime	<00-23>	Config the daily hour update schedule
			weeklyDay	<1-7>	Config the weekly day update schedule
			weeklyTime	<00-23>	Config the weekly hour update schedule
	signature				The command about signature post-process setting
		display			Display the current signature setting
		load	<Signature_ID>		Load the signature setting that its ID is SignatureIID
		save			Save the signature setting
		config			Config the current signature setting
			active	<on|off>	Enable/Disable the active option
			log	<on|off>	Enable/Disable the log option
			alert	<on|off>	Enable/Disable the alert option
			action	<1-6>	Set the post action
		reset			Reset the signature setting to the default setting
	device				
		reg			
		rxring			
		rxbuf			
		txbuf			
		disp			
	hardware				
		enable	<on|off>		

Anti-Virus Command

Home

Command					Description
av					Anti-Virus CI commands
	display				Show the anti-virus setting
	load				Load the anti-virus setting
	config				Config the anti-virus setting
		overZipSession	[0:Block| 1:Forward]		Forward session when the session number is over the maximum ZIP sessions.
		enable			Enable/Disable the anti-virus function
		httpScanAllMime	<on|off>		Enable/Disable scanning all mime type files. If we don't enable this option , ZyWall will just scan files with the application type
		pop3ScanAllMime	<on|off>		Enable/Disable scanning all mime type files. If we don't enable this option , ZyWall will just scan files with the application type
		smtpScanAllMime	Mon|off>		Enable/Disable scanning all mime type files. If we don't enable this option , ZyWall will just scan files with the application type
		decompress	<on|off>		Enable/Disable the decompress on the fly. You should also enable tcp assembly to support the decompress on the fly.
		ftp			Config the anti-virus setting for FTP
			display		Show the anti-virus setting for FTP
			active	<on|off>	Enable/Disable the anti-virus function for FTP
			log	<on|off>	Enable/Disable the log option
			alert	<on|off>	Enable/Disable the alert option
			breakfile	<on|off>	Enable/Disable the breakfile option
			sendmsg	<on|off>	Enable/Disable the sendmsg option
		dir			
			lan-lan	<on|off>	Config the protected interface setting
			lan-wan	<on|off>	Config the protected interface setting
			lan-dmz	<on|off>	Config the protected interface setting
			lan-wan2	<on|off>	Config the protected interface setting
			lan-wlan	<on|off>	Config the protected interface setting
			wan -lan	<on|off>	Config the protected interface setting
			wan -wan	<on|off>	Config the protected interface setting
			wan -dmz	<on|off>	Config the protected interface setting
			wan -wan2	<on|off>	Config the protected interface setting
			wan -wlan	<on|off>	Config the protected interface setting
			dmz -lan	<on|off>	Config the protected interface setting
			dmz -wan	<on|off>	Config the protected interface setting
			dmz -dmz	<on|off>	Config the protected interface setting
			dmz -wan2	<on|off>	Config the protected interface setting

			dmz -wlan	<on|off>	Config the protected interface setting
			wan2 -lan	<on|off>	Config the protected interface setting
			wan2-wan	<on|off>	Config the protected interface setting
			wan2-dmz	<on|off>	Config the protected interface setting
			wan2-wan2	<on|off>	Config the protected interface setting
			wan2-wlan	<on|off>	Config the protected interface setting
			wlan -lan	<on|off>	Config the protected interface setting
			wlan -wan	<on|off>	Config the protected interface setting
			wlan -dmz	<on|off>	Config the protected interface setting
			wlan -wan2	<on|off>	Config the protected interface setting
			wlan -wlan	<on|off>	Config the protected interface setting
		http			Config the anti-virus setting for HTTP
			display		Show the anti-virus setting for HTTP
			active	<on|off>	Enable/Disable the anti-virus function for HTTP
			log	<on|off>	Enable/Disable the log option
			alert	<on|off>	Enable/Disable the alert option
			breakfile	<on|off>	Enable/Disable the breakfile option
			sendmsg	<on|off>	Enable/Disable the sendmsg option
		dir			
			lan-lan	<on|off>	Config the protected interface setting
			lan-wan	<on|off>	Config the protected interface setting
			lan-dmz	<on|off>	Config the protected interface setting
			lan-wan2	<on|off>	Config the protected interface setting
			lan-wlan	<on|off>	Config the protected interface setting
			wan -lan	<on|off>	Config the protected interface setting
			wan -wan	<on|off>	Config the protected interface setting
			wan -dmz	<on|off>	Config the protected interface setting
			wan -wan2	<on|off>	Config the protected interface setting
			wan -wlan	<on|off>	Config the protected interface setting
			dmz -lan	<on|off>	Config the protected interface setting
			dmz -wan	<on|off>	Config the protected interface setting
			dmz -dmz	<on|off>	Config the protected interface setting
			dmz -wan2	<on|off>	Config the protected interface setting
			dmz -wlan	<on|off>	Config the protected interface setting
			wan2 -lan	<on|off>	Config the protected interface setting
			wan2-wan	<on|off>	Config the protected interface setting
			wan2-dmz	<on|off>	Config the protected interface setting
			wan2-wan2	<on|off>	Config the protected interface setting
			wan2-wlan	<on|off>	Config the protected interface setting
			wlan -lan	<on|off>	Config the protected interface setting
			wlan -wan	<on|off>	Config the protected interface setting
			wlan -dmz	<on|off>	Config the protected interface setting
			wlan -wan2	<on|off>	Config the protected interface setting
			wlan -wlan	<on|off>	Config the protected interface setting
		smtp			Config the anti-virus setting for SMTP
			display		Show the anti-virus setting for SMTP
			active	<on|off>	Enable/Disable the anti-virus function

					for SMTP
			log	<on|off>	Enable/Disable the log option
			alert	<on|off>	Enable/Disable the alert option
			breakfile	<on|off>	Enable/Disable the breakfile option
			sendmsg	<on|off>	Enable/Disable the sendmsg option
		dir			
			lan-lan	<on|off>	Config the protected interface setting
			lan-wan	<on|off>	Config the protected interface setting
			lan-dmz	<on|off>	Config the protected interface setting
			lan-wan2	<on|off>	Config the protected interface setting
			lan-wlan	<on|off>	Config the protected interface setting
			wan -lan	<on|off>	Config the protected interface setting
			wan -wan	<on|off>	Config the protected interface setting
			wan -dmz	<on|off>	Config the protected interface setting
			wan -wan2	<on|off>	Config the protected interface setting
			wan -wlan	<on|off>	Config the protected interface setting
			dmz -lan	<on|off>	Config the protected interface setting
			dmz -wan	<on|off>	Config the protected interface setting
			dmz -dmz	<on|off>	Config the protected interface setting
			dmz -wan2	<on|off>	Config the protected interface setting
			dmz -wlan	<on|off>	Config the protected interface setting
			wan2 -lan	<on|off>	Config the protected interface setting
			wan2-wan	<on|off>	Config the protected interface setting
			wan2-dmz	<on|off>	Config the protected interface setting
			wan2-wan2	<on|off>	Config the protected interface setting
			wan2-wlan	<on|off>	Config the protected interface setting
			wlan -lan	<on|off>	Config the protected interface setting
			wlan -wan	<on|off>	Config the protected interface setting
			wlan -dmz	<on|off>	Config the protected interface setting
			wlan -wan2	<on|off>	Config the protected interface setting
			wlan -wlan	<on|off>	Config the protected interface setting
		pop3			Config the anti-virus setting for POP3
			display		Show the anti-virus setting for POP3
			active	<on|off>	Enable/Disable the anti-virus function for POP3
			log	<on|off>	Enable/Disable the log option
			alert	<on|off>	Enable/Disable the alert option
			breakfile	<on|off>	Enable/Disable the breakfile option
			sendmsg	<on|off>	Enable/Disable the sendmsg option
		dir	lan-lan	<on|off>	Config the protected interface setting
			lan-wan	<on|off>	Config the protected interface setting
			lan-dmz	<on|off>	Config the protected interface setting
			lan-wan2	<on|off>	Config the protected interface setting
			lan-wlan	<on|off>	Config the protected interface setting
			wan -lan	<on|off>	Config the protected interface setting
			wan -wan	<on|off>	Config the protected interface setting
			wan -dmz	<on|off>	Config the protected interface setting
			wan -wan2	<on|off>	Config the protected interface setting

			wan -wlan	<on|off>	Config the protected interface setting
			dmz -lan	<on|off>	Config the protected interface setting
			dmz -wan	<on|off>	Config the protected interface setting
			dmz -dmz	<on|off>	Config the protected interface setting
			dmz -wan2	<on|off>	Config the protected interface setting
			dmz -wlan	<on|off>	Config the protected interface setting
			wan2 -lan	<on|off>	Config the protected interface setting
			wan2-wan	<on|off>	Config the protected interface setting
			wan2-dmz	<on|off>	Config the protected interface setting
			wan2-wan2	<on|off>	Config the protected interface setting
			wan2-wlan	<on|off>	Config the protected interface setting
			wlan -lan	<on|off>	Config the protected interface setting
			wlan -wan	<on|off>	Config the protected interface setting
			wlan -dmz	<on|off>	Config the protected interface setting
			wlan -wan2	<on|off>	Config the protected interface setting
			wlan -wlan	<on|off>	Config the protected interface setting
	save				Save the anti-virus setting
	update				The command about signature and signature update stuffs
		display			Show the signature information and the update setting
		load			Load the signature update setting
		save			Save the signature update setting
		start			Start the signature update
		config			Config the signature update setting
			autoupdate	<on|off>	Enable/Disable the autoupdate
			method	<1-3>	Config the update method
			dailyTime	<00-23>	Config the daily hour update schedule
			weeklyDay	<1-7>	Config the weekly day update schedule
			weeklyTime	<00-23>	Config the weekly hour update schedule
	tune				The tune command for IDP/Anti-Virus/Anti-Spam
		load			Load the tune configuration
		save			Save the tune configuration
		display			Display the tune configuration
		config			Config the tune configuration
			14Udpcksum	<on|off>	Enable/Disable UDP checksum check
			14Icmpcjsum	<on|off>	Enable/Disable ICMP checksum check
			14Tcpcksum	<on|off>	Enable/Disable TCP checksum check
			14Tcpwindowck	<on|off>	Enable/Disable TCP window check
			14Tcpmssck	<on|off>	Enable/Disable TCP mss check
			17Smtpasm	<on|off>	Enable/Disable TCP assembly for SMTP
			17Pop3asm	<on|off>	Enable/Disable TCP assembly for POP3
			17Httpasm	<on|off>	Enable/Disable TCP assembly for HTTP
			17Ftpasm	<on|off>	Enable/Disable TCP assembly for FTP
			17Ftpdataa	<on|off>	Enable/Disable TCP assembly for FTPDATA

			sm		
			l7Otherasm	<on|off>	Enable/Disable TCP assembly for other protocols
	zipUnsupport		zipEncrypDrop flag [0/1]		Processing ZIP file will destroy encrypted file if flag is on, otherwise pass it.

Anti-Spam Command Home

Command					Description
as					Anti-Spam CI commands
	asAction	[0|1]			Forward/Block exceeding mails sessions.
	debug				Debug for AntiSpam
		customListServ			Set custom server list server
			ip	[IP address]	Set custom server list server IP address
			enable	[0:disable|1:enable]	Enable/Disable custom server list server
		customRateServ			Set custom rating server server.
			ip	[IP address]	Set custom rating server IP address
			enable	[0:disable|1:enable]	Enable/Disable custom rating server
		envelope	[on|off]		Enable/Disable envelope debug message.
		http	[on|off]		Enable/Disable http debug message.
		mail	[on|off]		Enable/Disable mail debug message.
		pop3	[on|off]		Enable/Disable pop3 debug message.
		smtp	[on|off]		Enable/Disable smtp debug message.
	delete				Delete AntiSpam static filter.
		blackRule	<num start> [num end]		Delete black rule filter. User can delete one or a set of filter.
		whiteRule	<num start> [num end]		Delete white rule filter. User can delete one or a set of filter.
	display				
		antispam			Display AntiSpam configuration.
		serverlist			Display rating server list.
		runtimedata	<all|black|white>	[all|ip|mime|email|subject]	Display runtime data for anti-spam ACL structure.
	enable	<0:disable | 1:enable>			Enable/Disable AntiSpam.
	failTolerance	[time]			Set rating server fail tolerance time. If the rating server timeout interval over this tolerance, this server will be removed from server list.
	freeSession				Free all mail ssessions.
	getServerList	<Y:Yes|N:No>			Send server list request manually.
	dir	<lan|wan1|dmz|wan2|wla	<lan|wan1|dmz|wa	<on|off>	Enable or disable on direction of Anti Spam

		n>	n2|wlan>		
	scoreTimeout			value	Set the AS score query timeout value.