

ZyXEL

Firmware Release Note

ZyWALL 70

Release 4.03(WM.1)C0

Date:
Author:
Project Leader:

Jan 31, 2008
Wgang Wang
Joe Zhao

ZyXEL ZyWALL 70 Standard Version

Release 4.03(WM.1)C0

Release Note

Date: Jan 31, 2008

Supported Platforms:

ZyXEL ZyWALL 70

Versions:

ZyNOS Version: V4.03(WM.1) | 01/31/2008

BootBase : V1.10 | 07/31/2006

Agent Version: V2.1.6(WM.0)base

Notes:

1. Restore to Factory Defaults Setting Requirement: No.
2. The setting of ignore triangle route is on in default ROM FILE. Triangle route network topology has potential security crisis. If you are not clear about it, please refer to Appendix for the triangle route issue.
3. When firewall turns from "off" to "on", the firewall initialization procedure will disconnect all connections running through the ZyWALL.
4. 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.
5. 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.
6. 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.
7. For ZW5/35, the default port roles are LAN. For ZW70, the default port roles are DMZ.
8. In bridge mode, If LAN side DHCP clients want to get DHCP address from WAN side DHCP server, you need to turn on the firewall rule for BOOT_CLIENT service type in WAN→LAN direction.
9. Under Bridge Mode, all LAN ports will behave as a hub, and all DMZ ports will also behave as another hub.
10. 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)

11. 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.
12. 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.
13. If you do not want a mail to be scanned by Anti-Spam feature, you can add the mail into whitelist in eWC->Anti-Spam->Lists
14. If you want traffic redirect feature to work, you should turn on WAN ping check by "sys rn pingcheck 1". (For ZW5 only)
15. The first (first two) entry for static route is reserved for creating ZW5 (ZW35/70) WAN default route and is READ-ONLY.
16. 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.
17. WAN1 and WAN2 must be different subnet.
18. In Firewall/IDP/AV/AS/BM security rule, Dial backup traffic belongs to WAN interface. (In ZW35/70, the Dial backup traffic belongs to the higher priority WAN interface, for example, if WAN1 priority is higher than WAN2, Dial backup traffic will manage by WAN1 in Firewall/IDP/AV/AS/BM security rule.)
19. Support Vantage CNM – version 3.0.00.61.00.
20. For more information on commands, download the product line's CLI Reference Guide from the Download Library at www.zyxel.com.

Known Issues:

System Limitation

[Bandwidth Management]

1. Bandwidth Management doesn't work on wireless LAN.

[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.)

[Wireless]

1. The fragmentation threshold size support between 800~2432.

[MISC]

1. At SMT24.1, the collisions for WAN, LAN and DMZ port are not really counted.
2. 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.
- 3. When device is writing flash, all the interrupt/service will be stopped. (Firmware upload and signature update for full version will take tens of seconds)
- 4. Because of the memory shortage (ZW5/P1), device have to restart when customer need to upgrade firmware sometimes.

Issues

[ALG]

- 1. H323 does not support the server in LAN topology.
- 2. Currently, we do not support NAT loopback on SIP registration or proxy server, which means if your SIP client is located on LAN, your registration server address cannot use ZyWALL WAN IP to do loopback to SIP server which located on LAN.
 - (1) NAT loopback for SIP server on LAN.
 - (2) Client A(WAN) call Client B(LAN) using LAN's IP, and the reversed way. That is you should call phone number directly to each other without the IP address. There issue will be improved for future plan.
 - (3) Device can support direct ACK/BYE sip request, but for the following topology
 Client_A----SIP Server----- (L) ZW_1 (W) ----- (W) ZW_2 (L) ---- Client_B
 (Client/Server) ----- (LAN) DUT (WAN) ---- (client)
 Stop calling from answer client, the calling can't terminate normally.

[Anti-Spam]

- 1. Mail cannot pass through 2 devices with Anti-Spam enabled.
- 2. Customer need to turn off the redundant check for AS and AV for gathering more CPU resource or CPU will always reach 100%. When CPU reaches 100%, the AS/CF query will be timeout sometimes because there is no resource for it.
- 3. The maximum length of the mail subject is 2037 right now. The mail subject you input is 2037, but you need to add the length of (A)"subject: " and (B)"\r\n", (A)+(B) is 11 bytes. They equal to 2048.

[Bandwidth Management]

- 1. Bandwidth management H.323 service does not support Netmeeting H.323 application.
- 2. If H323/SIP ALG doesn't work, the Bandwidth management cannot manage the traffic too.

[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. In the following topology, Firewall VPN to LAN ping can't be permitted.
 PC1-----DUT1-----NAT Router-----PQA lab-----DUT2-----PC2
 IP: 192.168.1.33 IP: 192.168.1.2 LAN: 192.168.1.1 WAN: 172.25.21.24 IP: 192.168.2.33
 GW: 192.168.1.2 WAN: 172.25.21.200 LAN: 192.168.2.1 GW: 192.168.2.1
 (1) DUT1 is on bridge mode, DUT2 is on router mode, build VPN tunnel between them.

(2) On DUT1 enable Firewall, and set Drop for VPN to LAN, then add a firewall rule of VPN to LAN:

Source address = 192.168.2.33

Destination Address = 192.168.1.33

Selected Service = Any (ICMP)

Action for matched Packets = Permit.

(3) Can't ping 192.168.1.33 from 192.168.2.33 and you can find "Unsupported/out-of-order ICMP: ICMP (Echo Reply)" log on log page.

Note:

(1) Here, PC1's GW is DUT1's LAN IP. With the ICMP reply packet, the destination IP is 192.168.2.33. In PC1, the packet will match the default GW (192.168.1.2) and change the destination MAC as DUT's LAN MAC. DUT receive the packet and the destination MAC is DUT's LAN, DUT thinks this packet is send to itself and the ICMP out of order happens. This is because there is no ICMP request packet for the device itself but an ICMP reply packet for DUT.

(ICMP out of order scenario, not ICMP request but with ICMP reply)

(2) If set the default GW in PC1 as 192.168.1.1, the packet's destination MAC is NAT-Device's LAN (192.168.1.1), not DUT's IP. DUT knows the packet is not for itself and ready pass through it. But the packet match the VPN rule and it will encrypted by DUT.

[Content Filter]

1. CF Denied Access Message can run script.
2. And the categories function can also has some issue because of the OutpostPro firewall bug fix. When user want to block some categories, such as "Search Engines/Portals", external DB search work normally the first time. But after refreshing the page or open the website again in another Browser window, only "Please contact your network administrator!!" can be showed, without the link to bluecoat.
3. Web sites of category "Peer-to-Peer" were recognized as "Spyware/Malware Sources".
4. "Don't block Java/ActiveX/Cookies/Web proxy to trust Web site" function in content filter cannot work.
Symptom: "Don't block Java/ActiveX/Cookies/Web proxy to trust Web site" function in content filter cannot work.
Condition:
 - (1) In eWC->SECURITY->CONTENT FILTER->General page, enable "Content filter" and block "Java Applet/ActiveX/Cookies/Web Proxy".
 - (2) In eWC->SECURITY->CONTENT FILTER->Customization page, enable "Web site customization" and "Don't block Java/ActiveX/Cookies/Web proxy to trusted Web sites". Add "web.haccpsoft.it" to "Trusted Web Sites".
 - (3) A PC in ZYWALL's LAN side browses "http://web.haccpsoft.it:8080" website.
 - (4) Login in and click the date, the popup window should show a calendar instead of another login page.
 - (5) It is blocked by content filter.
5. <http://info.zyxel.com.tw> was recognised as "google".

Condition:

- (1) Input "google" in Keyword Blocking of Customization.
 - (2) Visit <http://info.zyxel.com.tw> in LAN PC. The web site is opened successfully. But there is a Keyword Blocking log say "info.zyxel.com.tw: Keyword blocking" (see attached file).
 - (3) Visit other web site is normal.
 - (4) This problem is also existed in 4.01 Patch 2 C0 too.
6. Keyword blocking has functioned even if "Web site customization" was disabled.

Condition:

- (1) Enable Content Filter.
- (2) Add google into Customization>>Keyword Blocking. Keep "Web site customization" was disabled.
- (3) PC in LAN visit www.google.com will be blocked there are blocked log (see attached picture).
- (4) This problem does NOT exist in "Forbidden Web Site List".
- (5) This problem is existed in 4.01 Patch 2 C0 too.

[Firewall]

1. Some limitations on Firewall CLI configuration, (1) User can not delete specific address or custom port entry from a rule. (2) CLI doesn't support Modify and Move for rules implemented in eWC. (3) eWC can not display firewall rule field correctly if rule is added by CI command and its type is port/address range.
2. Ping of Death Log has some fault when argument in CI "ip icmp death" bigger than 1500.

Conditions:

- (1) Type CI "ip icmp death 1000" or "ip icmp death 1500".
- (2) PC1 ping PC2 with DOS command "ping 172.25.21.254 -l 1600", the log is shown as: "ping of death. ICMP(Echo)".
- (3) Type CI "ip icmp death 1501" or other number bigger than 1500.
- (4) PC1 ping PC2 with DOS command "ping 172.25.21.254 -l 2000", the log is shown as: "ping of death. ICMP(Echo Reply)". That is to say when argument in CI "ip icmp death" is bigger than 1500, the log is different. And sometimes the log shown as "ping of death. ICMP(W to L, Echo Reply)".

[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.

[VPN]

1. SNMP tools get ZYWALL VPN MIB data, the index of received data are wrong if rules are larger than 1.
2. 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.
2. In eWC->Statistics, Tx data for Dial Backup is not correct.
3. ZyWALL does not support WAN 1/WAN 2 on the same sub-net. (For Multiple WAN products)
4. The function of new CI command "sys rn pingDrop" doesn't work. SPR ID: 070503103
5. Traffic is blocking. SPR ID: 070404256

[CNM]

1. DES/3DES encryption key doesn't unique.
2. [Symptom] Device will crash, when Vantage set Dial Back Fixed IP in the same subnet as WAN to device.
[Condition]
 - (1). Let device register to Vantage.
 - (2). Vantage set Dial Backup to enable.
 - (3). Vantage set Dial Backup Fixed IP in the same subnet as WAN to device.
 - (4). Device will crash after writing above settings.
3. Vantage will set incorrect root password to device when hash root password flag enable via ci command: "sys pwdHash on".
4. Vantage server can't check IP conflict with WAN on the following pages. LAN, WLAN, DMZ, Static Route and Dial Backup.
5. Agent can't response inquire success packet to Vantage when change port roles.
6. Only ZW70 with Model ID 0x1F55 supported. (Server release known issues).
7. Server remove online device from top-tree, but dose not sent "cnm active 0" message to device.
8. Vantage server won't retry to trigger TA inform again if SGMP triggered fail.

Features:

Modifications in V4.03(WM.1) | 01/31/2008

Modify for formal release.

Modifications in V4.03(WM.1)b1 | 01/17/2008

1. [ENHANCEMENT] SPR ID: 070724576
Provide a ci command "sys tos allow_FinPshAck [on/off]" to allow or block packet with FIN, PSH, and ACK flag. Default is off, that is to say, blocking packet with FIN, PSH, and ACK flag.
2. [ENHANCEMENT]
Provide a CI command "ip arp reqUpadteTable [on/off]" to enable/disable that the device would use receiving ARP packet to update ARP table. The default value is off and the value will return to off when the device re-start.
3. [ENHANCEMENT]

Enlarge the length of "User Name" in E-mail Report, Log Settings and Diagnostics from 31 to 63.

4. [ENHANCEMENT] SPR ID: 071114968
Free established TOS according to firewall schedule policy.
5. [ENHANCEMENT] SPR ID: 070614815
Modified DDNS Log is not readable.
(1) View DDNS Log in LOGS>>View Log.
(2) DDNS Log is not readable, for example:
2007-05-07 17:44:52 DDNS update IP:138.188.40.255 (host 1) successfully
Was: DNS update IP:138.188.40.255 (host 1) successfully
Is: Update domain name zywail2wg.dyndns.org with IP:138.188.40.255 successfully|DDNS

Was: DDNS update error: The hostname specified does not exist.| Code: nohost
Is: Update error: The hostname specified does not exist. |DDNS
6. [ENHANCEMENT]
DDNS client will force update with Dyndns.org server in every 28 days automatically.
7. [FEATURE CHANGE] SPR ID: 070806425
WAS: Some IPSec network policies can be saved even they conflict with each other.
IS: Device will check network policies under two condition:
(1) To save a network policy under static IKE rule --> compare with other network policies under static IKE rules.
(2) To save a network policy under dynamic IKE rule --> Do not compare it. This network policy will be compared with other network policies under static and dynamic rules during IKE negotiation.
8. [BUG FIX] SPR ID: 071022070
Symptom: when WAN1 restores connection, ZyWALL still dial up three or more times.

Condition:
(1) Let WAN1 down and dial backup up
(2) From LAN pc, downloading a file located at WAN
(3) During downloading, let WAN1 up
(4) Then you will find ZyWALL still dial up three or more times
9. [BUG FIX] SPR ID: 070927476
Symptom: ZyWALL uses PC MAC address as the source MAC to send ESP/AH packets.

Condition:

(bridge mode) (NAT router) (router mode)
PC1------(LAN)ZyWALL(WAN)----VSG-1200----IPSec gateway----PC2

- (1) Build a VPN tunnel between ZyWALL and IPSec gateway.
- (2) Ping PC2 from PC1.
- (3) Tunnel can be established, but no PING response.

10. [BUG FIX] SPR ID: 070809666

Symptom: ZyWALL crashes when receive pop3 mail from WAN.

Condition:

PC1------(192.168.100.33)router(192.168.1.33)-----(LAN)ZyWALL(WAN1)----mailserver

- (1) Enable Anti-spam WAN1->LAN direction and external DB on ZyWALL.
- (2) Add a static route (dest 192.168.100.0/24, gateway 192.168.1.33) in ZyWALL.
- (3) PC1 user uses MS Outlook to receive mails.
- (4) ZyWALL crashes.

11. [BUG FIX] SPR ID: 071114971

Symptom: IKE SA Leak in customer site.

Topology:

ZyWALL_DUT(WAN)-----(WAN)NAT Router(LAN)----|
|----ZyWALL1
|----ZyWALL2

Condition:

- (1) Configure one IKE rule IKE1 in ZyWALL_DUT, set NAT Router as "Remote Gateway".
- (2) Add two IPSec rules under IKE1 in ZyWALL_DUT.
IPSec1: ZyWALL_DUT--ZyWALL1
IPSec2: ZyWALL_DUT--ZyWALL2.
- (3) In ZyWALL1, configure IKE and IPsec rule. Enable Nailup. Make sure the Tunnel can be built successfully.
- (4) In ZyWALL2, configure IKE rule and IPsec rule correctly except Pre-shared Key. Enable Nail up. Make sure the Tunnel couldn't build successfully.
- (5) After long time run, ZyWALL_DUT will crash because of IKE SA leak.

12. [BUG FIX] SPR ID: 070726881

Symptom: ZyWALL doesn't forward "no answer section" to DNS client.

Condition:

- (1) Configure ZyWALL as DNS Server on Linux PC.
- (2) Execute "host -t MX www.playboy.com"
- (3) PC waits the response until timeout.
- (4) If DNS server is not ZyWALL, PC gets response immediately.

(6) Then, you will find PC2 can't ping PC4.

15. [BUG FIX] SPR ID: 070911459

Symptom: CI command "ip arp force on" does not take effect on WAN 2.

Condition:

- (1) Let WAN 1/WAN 2 active and has traffic on them.
- (2) CI command "ip arp status" to show that the timer of ARP entry would not decrease due to the existence of the traffic.
- (3) Use CI command "ip arp force on" to force the system to decrease timers of those WAN ARP entries periodically.
- (4) CI command "ip arp status" to show, timers of WAN 1 ARP entries would decrease, but timers of WAN 2 would not.

16. [BUG FIX] SPR ID: 070717916

Symptom: ZyWALL can not connect to port 139 through the IPsec tunnel in PPTP encapsulation mode when disable windows networking packet filter "Allow between LAN and WAN".

Condition:

Topology:

PC1------(LAN)ZyWALL2+_1(WAN+PPTP)----VPN----
(Ethernet+WAN)ZyWALL2+_2(LAN)----PC2

- (1) The encapsulation mode of ZyWALL2+_1 is PPTP, and the encapsulation mode of ZyWALL2+_2 is Ethernet.
- (2) Build the gateway to gateway VPN tunnel from ZyWALL2+_1 to ZyWALL2+_2.
- (3) PC1 can not visit PC2 share folder(\\PC2 address) if the "Allow between LAN and WAN" is not checked.

17. [BUG FIX] SPR ID: 070614825

Symptom: Time zone showed incorrect when daylight saving is checked and working at the same time.

Condition:

- (1) EWC>MAINTENANCE>Time and Date
- (2) Select Time Zone (GMT+03:00) Baghdad, Kuwait, Nairobi, Riyadh, Moscow
- (3) Enable daylight saving, make current time be in daylight saving
- (4) Click on Apply.
- (5) You will find Time Zone of Current Time showing "GMT+04:00"
- (6) This also happen in EWC>HOME>System Information>System Time.
- (7) In fact, whether enable Daylight saving or not, should not change time zone in current time display

18. [BUG FIX] SPR ID: 060927777

Symptom: The "Up Time" shown on the Port Statistics and Home page are quite different when the ZyWALL uptime is more than 100 hours.

Condition:

- (1) Let ZyWALL WAN1 uptime be more than 300 hours.
- (2) Go to eWC>HOME page, the "Up Time" is "4:00:00".
- (3) Click "Port Statistics" button, the WAN1 "Up time" of pop-up window is "300.00.00".

19. [BUG FIX] SPR ID: 070614811

Problem Symptom: Some formats of logs should be consistent.

LOG message in EWC->LOGS->View Log

WAS:

# Time	Message	Source Destination	Note
	WLAN STA Association		MACAddr:0013026c13a3
	WLAN STA Association Again		MACAddr:0013026c13a3
	WLAN STA denied by WLAN MAC Filter		MACAddr:0013026c13a3
	WLAN STA allowed by WLAN MAC Filter		MACAddr:0013026c13a3
	DHCP server assigns 10.10.101.222 to		
	Kurt-I6400(00:13:02:88:79:59)		

IS:

# Time	Message	Source Destination	Note
	WLAN STA Association MACAddr:0013026c13a3		
	WLAN STA Association Again MACAddr:0013026c13a3		
	WLAN STA allowed by WLAN MAC Filter		
	MACAddr:0013026c13a3		
	WLAN STA denied by WLAN MAC Filter		
	MACAddr:0013026c13a3		
	DHCP server assigns IP:10.10.101.222 to		
	Kurt-I6400(00:13:02:88:79:59)		

20. [BUG FIX] SPR ID: 071109692

Symptom: The property field of eWC>CERTIFICATES>MY CERTIFICATE>DETAILS is gone

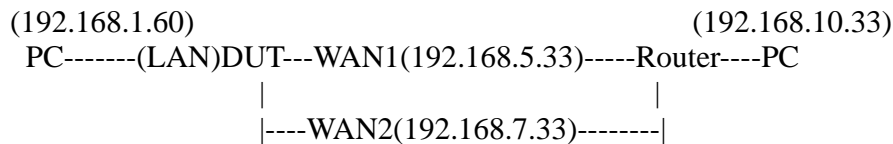
Condition:

- (1) Goto eWC>CERTIFICATES>MY CERTIFICATE>DETAILS page and you will find the property field is gone.

21. [BUG FIX] SPR ID: 071114943

Symptom: ZyWALL cannot reply packet on correct WAN interface.

Condition:

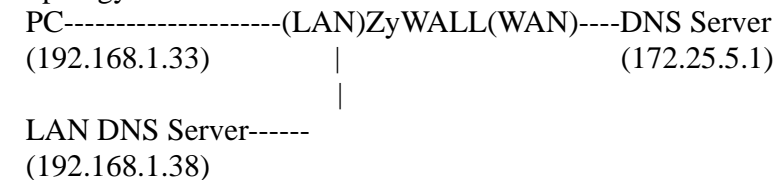


- (1) Set WAN=Active/Active mode, WAN1=192.168.5.33,WAN2=192.168.7.33.
- (2) Policy Route=Active, Source Address=192.168.1.60, Destination Address=0.0.0.0, Gateway=WAN2, Use another interface when the specified WAN interface is not available.
- (3) NAT 1-1 rule for WAN1: Local Start IP=192.168.1.60, Global Start IP=192.168.5.33.
- (4) NAT 1-1 rule for WAN2: Local Start IP=192.168.1.60, Global Start IP=192.168.7.33.
- (5) When WAN2 is down, policy route=active, from 192.168.10.33 can access 192.168.1.60 FTP server via WAN1.
- (6) When WAN2 is up, policy route = active, from 192.168.10.33 cannot access 192.168.1.60 FTP server via WAN1.

22. [BUG FIX] SPR ID: 071115018

Symptom: Log of DNS will show wrong port number when LAN DNS server forwards DNS request to external server.

Topology:



Condition:

- (1) Reset rom of ZyWALL
- (2) Add a LAN to WAN firewall permit rule, select DNS service, Enable Log Packet Information When Matched
- (3) eWC>SECURITY>FIREWALL>Threshold, Disable DoS Attack Protection on LAN
- (4) Configured LAN DNS Server(192.168.1.38) as DNS proxy to forward DNS request to DNS server(172.25.5.1)
- (5) Set PC DNS server as 192.168.1.38, ping some internet domains. For example, ping www.google.cn
- (6) eWC>LOGS, you will find some logs exist with LAN to WAN firewall rule of DNS service , but port is not 53
- (7) eWC>SECURITY>FIREWALL>Threshold, Enable DoS Attack Protection on LAN, then the logs show correctly

23. [BUG FIX] SPR ID: 071115021

Symptom: When adding a new sub-class with bandwidth budget = 0, can save, but Can not edit or delete.

Condition:

- (1) Reset rom
- (2) eWC>ADVANCED>BW MGMT>Summary, active bandwidth management on WAN1
- (3) eWC>ADVANCED>BW MGMT>Class Setup, Add a sub-class with budget = 0 and enable bandwidth filter
- (4) After click on Apply, it will display under "Enabled classes Search Order"
- (5) Unfolding tree of root class, can not find the new added sub-class

24. [BUG FIX] SPR ID: 071113828

Symptom: When create My Certificates, and the certificates name includes spaces, the certificate can be created successful, the DUT didn't show error message, but this certificate can not be exported.

Condition:

- (1) Edit eWC>CERTIFICATES>My Certificates, create a certificate as Certificate Name="DUT IP" Host IP Address="192.168.12.100" Organizational Unit="DUT_IP" Organization="DUT_IP" Country="DUT_IP" Key Length="1024"
- (2) Then apply, it can be created successful, the DUT didn't show error message. Check web eWC>My Certificates, the DUT IP is on the table.
- (3) When export this certificate, it fails.

25. [BUG FIX] SPR ID: 071122504

Symptom: One field in Diagnostics page can not be changed by using Firefox.

Condition:

- (1) Use Firefox.
- (2) Go to eWC>MAINTENANCE>Diagnostics.
- (3) The field of CPU utilization can not be inputted.

26. [BUG FIX] SPR ID: 071219091

Symptom: ZyWALL hung when Nessus scan. P1 DON'T NEED TEST

Topology:

PC1 with Nessus ----(LAN) ZyWALL (DMZ)----PC2 (192.168.4.33)

Condition:

- (1) Install Tenable Nessus 3 (you can get it at www.nessus.org) in PC1. Updates it's plug-in.
- (2) PC1 starts Nessus by the following steps:
 - (a) Start Scan Task.

- (b) Input PC2 IP 192.168.4.33.
 - (c) Enable all plug-in with default settings (Even dangerous plug-in are enabled).
 - (d) Scan from the local host.
 - (e) Scan Now.
- (3) When scan finished, ZyWALL will hung.
- (4) Another easier way to reproduce the hang is that send the attached packet by Sniffer.

27. [BUG FIX] SPR ID: 071120328

Symptom: Log for connectivity check fail Source IP and Destination IP should be NULL when domain name doesn't exist. Shouldn't show the Destination IP of the last time ping.

Condition:

- (1) Goto eWC>Network>WAN>General.
- (2) Enable "Check WAN1 Connectivity, and let system PING 1.1.1.1 this IP.
- (3) Log show ping check fail, Source IP= WAN IP, Destination IP=1.1.1.1
- (4) Enable "Check WAN1 Connectivity" and let system PING "www.abcdefg123aabbccdd.com" which doesn't exist.
- (5) There is log for ping check fail, but, Source IP =WAN IP, Destination IP=1.1.1.1, so, log is incorrect. If your domain inexistent, Source IP and Destination IP should equal to NULL.

28. [BUG FIX] SPR ID: 071120338

Symptom: The static DHCP rule cannot be saved under special condition.

Condition:

- (1) Add a static DHCP rule at the end of the DHCP table.
- (2) Add the same MAC address with different IP address before the end rule, it shows "Duplicate MAC Address" message.
- (3) Delete the end rule added in step 1.
- (4) Add other different MAC address rule, and then apply. It can't be saved with the message "Duplicate MAC Address".

29. [BUG FIX]

Fixed the DDNS service provider FQDN as follows:

WWW.DynDNS.ORG => WWW.DynDNS.COM

30. [BUG FIX] SPR ID: 080114603

Symptom: ZyWALL can't send allowed CF log to report server

Topology:

PC----(lan)ZyWALL(wan)----report server

Condition:

- (1) Register CF service on alpha.myzyxel.com
- (2) Configure CF log server address using CLI command

"ip cf externalDB exDblogserver 220.128.56.38"

- (3) Go to eWC>SECURITY>CONTENT FILTER>General, do following settings
Enable Content Filter = selected
Enable External Database Content Filtering = selected
Matched Web Pages, unselect Block, select Log
Enable Report Service = selected
- (4) Go to eWC>SECURITY>CONTENT FILTER>Policy
insert one policy,
- (5) Go to eWC>SECURITY>CONTENT FILTER>EDIT POLICY>GENERAL,
Active this policy, Address Setup = Any
- (6) Go to eWC>SECURITY>CONTENT FILTER>EDIT POLICY>EXTERNAL
DATABASE
Active External Database Service Configuration
Select Categories:Search Engines/Portals
Click on Apply
- (7) Under lan pc, visit www.google.cn
- (8) Then view CF report using URL "http://203.160.254.52?mac=0000AA780145",
you will find URL "www.google.cn" in blocked list. In fact, it should be in
allowed list.

Modifications in V4.03(WM.0) | 11/07/2007

Modify for formal release.

Modifications in V4.03(WM.0)b4 | 10/29/2007

1. [ENHANCEMENT]
Add Vantage CNM device agent – 2.1.6(WM.0) which support Vantage CNM
server – version 3.0.00.61.00.
2. [BUG FIX] SPR ID: 070924386
Symptom: CF schedule works abnormal.
Condition:
 - (1) Enable CF. In CF>Object, add a Forbidden Website "www.google.com".
 - (2) Add a new policy, set IP group as "Any" and add "www.google.com" to
Forbidden website. Set Schedule as "Everyday from 09:00 to 17:00".
 - (3) Open www.google.com in 17:01 ~ 17:59, the website still be blocked and that's
wrong.
3. [BUG FIX] SPR ID: 070809666
Symptom: ZyWALL crashes when receive pop3 mail from WAN.
Conditions:
PC1---(192.168.100.33)router(192.168.1.33)---(LAN)ZyWALL(WAN1)---mailserver
 - (1) Enable Anti-spam WAN1->LAN direction and external DB on ZyWALL.
 - (2) Add a static route (dest 192.168.100.0/24, gateway 192.168.1.33) in ZyWALL.
 - (3) PC1 user uses MS Outlook to receive mails.

(4) ZyWALL crashes.

4. [BUG FIX] SPR ID: 070914803

Symptom: Dial Backup will be dialed in Active/Active mode even when two WAN interfaces are up.

Conditions:

- (1) Enable Active/Active mode and LB algorithm = "None".
- (2) Edit a correct Dial Backup configuration, enable "Always On" and then apply.
- (3) Make sure WAN1 and WAN2 are both up, after that, Dial Backup will be dialed and we can see three WANs in eWC>Home.

5. [BUG FIX] SPR ID: 071002097

Symptom: CF unrated website block flag cannot save and function doesn't work in specified condition.

Conditions:

- (1) Restore default romfile.
- (2) In CF, enable "Unrated Website Page -- Block" and save it. You will find that it cannot save.
- (3) If you add a policy(policy name: aaa) and repeat step 2 again and it works.
- (4) Add another policy again(policy name: bbb) and save it.
- (5) Disable policy aaa and test the unrated functionality for policy bbb. It will fail.

6. [BUG FIX] SPR ID: 070914803

Symptom: Policy route doesn't work correctly.

Conditions:

```
(LAN: 192.168.1.1)          (192.168.1.33)
ZW_A -----Switch-----PC_A
|---(WAN: 192.168.2.33) ZW_B (LAN: 192.168.10.1) -----PC_B
                                   (192.168.10.33)
```

- (1) In ZyWALL_A, LAN Alias IP = 192.168.2.1.
- (2) In ZyWALL_A, create a policy route : Source IP = 192.168.1.33. Destination IP = 192.168.10.33. Gateway = 192.168.2.33.
- (3) In ZyWALL_A, turn on firewall. In eWC>Firewall>Summary, check "Allow asymmetric route".
- (4) PING from PC_B to PC_A, and it fails.

7. [BUG FIX] SPR ID: 071005383

Symptom: Content filter configuration is gone after upload 403 FW.

Conditions:

- (1) Load 4.00 FW and enable "Gambling" category.
- (2) Upload 4.03 FW and the "Gambling" category is gone.

8. [BUG FIX] SPR ID: 071009535

Symptom: User cannot access "tw.msn.com" website when enable CF>block cookie functionality.

Conditions:

- (1) Enable content filter and block cookie.
- (2) Access "tw.msn.com" website and you will get "Bad Request (Invalid Header Name)" in browser.

9. [BUG FIX] SPR ID: 070921355

Symptom: Device crashes when doing the stress testing.

Conditions:

PC_A == [LAN]ZyWALL_A[WAN] == [WAN]ZyWALL_B[LAN] == PC_B

- (1) Enable all UTM functionality.
- (2) Build up a VPN tunnel for PC_A and PC_B.
- (3) Upload a zip file from PC_A to PC_B.
- (4) PC_A and PC_B send a lot of UDP packet to each other.
- (5) In ZyWALL_A and ZyWALL_B, go to eWC>Home, set the "Automatic Refresh Interval" as 10 seconds.
- (6) After few hours(it may take several days), device crashes.

10. [BUG FIX] SPR ID: 071015779

Symptom: Device hang when input command "ip cf ob add trust aa.aa".

Conditions:

- (1) Input command "ip cf ob add trust aa.aa" in SMT 24.8 and device hangs.

11. [BUG FIX] SPR ID: 071017888

Symptom: Missing help page in VPN>Network Policy>Edit>Port Forwarding Rules.

Conditions:

- (1) Go to eWC>VPN>Network Policy>Edit>Port Forwarding Rules page, click help page and you will find there is no help page in it.

12. [BUG FIX] SPR ID: 070926450

Symptom: Device cannot receive any packet after several days.

Conditions:

- (1) Restore default romfile.
- (2) Do not put any host in private network(LAN/DMZ/WLAN) and make sure device can access internet.
- (3) After few days, device cannot receive packet any more.

Modifications in V 4.03(WM.0)b3 | 09/20/2007

13. [BUG FIX] SPR ID: 070905161

Symptom: Wizard internet access setup has wrong URL link

Condition:

- (1). Go to eWC>Home>Wizard>Internet Access setup>Product registration and service activation for free.
- (2). The URL link of registration shouldn't be <http://www.zyxel.com>, it should be <http://www.myzyxel.com>.
- (3). Click this URL to redirect to www.zyxel.com.tw in this wizard window, and then can't back to wizard setup page.

14. [BUG FIX] SPR ID: 070905185

Symptom: ZyWALL crashes when testing content filter.

Conditions:

- (1). Restore default romfile and Enable CF.
- (2). Enable external DB in default policy.
- (3). Enable "Gambling" in default policy.
- (4). Set schedule in default policy with "Every day" + "01:01" and "02:02" (the schedule will not match current time)
- (5). PC in LAN access "www.gambling.com" and device crashes.

15. [ENHANCEMENT]

- (1). Change wording for CF. ("profile" ==> "policy")
- (2). The CF default policy can be edited.

16. [FEATURE CHANGE]

- (1). Remove CF schedule "Active" field in CF>Policy>Schedule page.
- (2). Change CF rom convert behavior as,
 - (2.1) If old rom file is configured, there will be one/two policy created.
 - (2.2) If old rom file is not configured, there will be no policy created.
- (3). Refine CF GUI/CI/CLI code.

Modifications in V 4.03(WM.0)b2 | 08/28/2007

1. [ENHANCEMENT] (For 3G product only)

Add new 3G cards support and some 3G-function enhancements.

Please see below feature descriptions:

- ** 3G works only for WAN2.
- ** Support Sierra Wireless AirCard AC875 , Huawei E612 / E620 for HSDPA.
- ** Support Sierra Wireless AirCard AC595 for EVDO.
- ** Support SIM authentication / management on GUI (AC875/AC850/E612/E620)
- ** Support 3G card lock status checking / unlock / activation status checking on GUI (AC595)
- ** Support Network Type Selection on GUI. (AC875/ AC850)
- ** Support manual/auto Service Provider Selection on GUI. (AC875/AC850/E612/E620)
- ** Device can update signal strength while data is transferring. (AC875/AC595/E612/E620)
- ** Device can update network type, registered service provider while data is transferring. (AC875/E612/E620)
- ** Device can update roaming status while data is transferring. (AC875)
- ** Device can update dormant status while data is transferring. (AC595)
- ** Support Budget Control for 3G WAN. (AC850/AC875/AC595/E612/E620)
- ** Support Card Selection, if device can insert multiple 3G cards, only one card can be selected and enabled at once. (For ZyWALL 5H only)
After selecting new 3G card in different slot, device will reboot.
- ** New Log category for 3G, supports easy-read log description.

Condition:

The NAT setup of WAN 1 is full feature, and NAT setup of WAN 2 is SUA.
Can't see the site on the public DMZ from Internet

1. Set LAN to 192.168.1.1/24, DMZ to a public subnet.
2. Add a static route to let PC3 can routing to PC2 from WAN1.
3. WAN1 and WAN2 all active and have public IP addresses.
4. Set WAN1 NAT to Full Feature and modify the first default NAT rule to:

#	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
1	192.168.1.1	192.168.1.254	0.0.0.0		N/A M-1
5. Set WAN2 NAT to SUA.
6. PC3 Ping PC2 will failed.

8. [BUG FIX] SPR ID: 070228410 ITS #: 15616

Symptom: ZyWALL35 BW MGMT class search order shows wrong when moving classes.

Condition:

- (1) Restore romfile (password:fenris120) from SPR, go to Class Setup under WAN1.
- (2) Add sub-class FTP, bandwidth budget 180k, priority:5, service type:FTP.
- (3) Add sub-class PC1, bandwidth budget 150k, priority:4, borrow,service type:custom, Source IP:single 192.168.1.37.
- (4) Cannot move class 1 to 2.

9. [BUG FIX] SPR ID: ITS#16018

Symptom: Modem initializations process cannot finish, LG-340E CDMZ Wireless phone

Topology: PC-----(LAN)ZyWALL (AUX0)---- LG-340E CDMA Wireless phone

Condition:

- (1) Connect this CDMA phone(LG-340E) to my PC directly (Baud rate 115200)
- (2) Key in the AT commands "AT OK AT+CRM=1 OK AT\$LGPKT=3 OK ATDT#777 CONNECT"
- (3) ZyWALL print message ※AUX Port init Done Modem Init Failed!!!§ in console.

10. [BUG FIX] ITS #: 15405

Symptom: BM for SIP doesn't work on WAN interface

Condition:

- (1) Add a BM filter for SIP on WAN interface
- (2) Enable SIP ALG
- (3) SIP connection can be built successfully with Customer's SIP server
- (4) But SIP Traffic can't be monitored.

11. [ENHANCEMENT] (For 3G product only)

Add new 3G card support for Option Globe Trotter HSDPA 7.2 .

12. [BUG FIX] SPR ID: 070614811

Symptom: Some formats of logs should be consistent. LOG message in eWC->LOGS->View Log

WAS:

#	Time	Message	Note	
		WLAN STA Association		
		MACAddr:0013026c13a3		
		WLAN STA Association Again		
		MACAddr:0013026c13a3		
		WLAN STA denied by WLAN MAC Filter		
		MACAddr:0013026c13a3		
		WLAN STA allowed by WLAN MAC Filter		
		MACAddr:0013026c13a3		
		DHCP server assigns 10.10.101.222 to		
		Kurt-I6400(00:13:02:88:79:59)		

IS:

#	Time	Message	Note	
		WLAN STA Association MACAddr:0013026c13a3		
		WLAN STA Association Again MACAddr:0013026c13a3		
		WLAN STA allowed by WLAN MAC Filter		
		MACAddr:0013026c13a3		
		WLAN STA denied by WLAN MAC Filter		
		MACAddr:0013026c13a3		
		DHCP server assigns IP:10.10.101.222 to		

13. [ENHANCEMENT] SPR ID: ITS #14868

Add CI "sys log mail port" to change the port number which ZyWALL Email logs to SMTP server.

Note:

- (1) "sys log mail port" without port number.
Show SMTP port number current used.
- (2) "sys log mail port [port number]"
Set SMTP port number to argument [port number].
The valid port number is between 1 to 65535.

14. [BUG FIX] ITS #: 17165

Symptom: Can't change the default route on ZyWALL

Condition:

- (1) Using ci command "ip route status" to make sure default route of WAN1 or WAN2 exist in current route table.
- (2) Using ci command "ip route drop default" to delete default WAN1 or WAN2 route.
- (3) Can't delete the default route.

15. [BUG FIX] SPR ID: 070621307, 070621308

Symptom: DHCP has multiple entries for the same PC

Condition:

- 1). Set a PC to DHCP using the default config - PC will have 192.168.1.3
- 2). Click the windows network icon for the PC get static IP address and input the ip address as example: 192.168.1.7 and save
- 3). Change the pc get IP address is dynamic, and login in the router maintenance"->"DHCP table", you can see the pc get two IP address.

16. [BUG FIX]

Symptom: ZyWALL cannot connect to port 139 through the IPsec tunnel in PPTP encapsulation mode when disable windows networking packet filter "Allow between LAN and WAN".

Condition:

Topology:

PC1------(LAN)ZyWALL2+_1(WAN+PPTP)----VPN----(Ethernet+WAN)ZyWALL 2+_2(LAN)----PC2

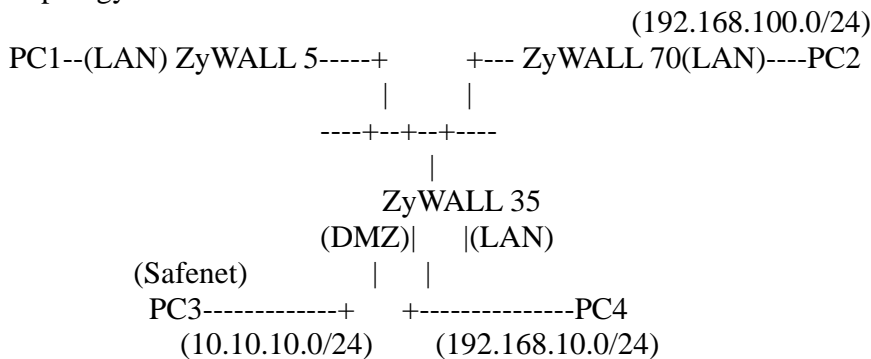
- (1) The encapsulation mode of ZyWALL2+_1 is PPTP, and the encapsulation mode of ZyWALL2+_2 is Ethernet.
- (2) Build the gateway to gateway VPN tunnel from ZyWALL2+_1 to ZyWALL2+_2.
- (3) PC1 can not visit PC2 share folder(\\PC2 address) if the "Allow between LAN and WAN" is not checked.

17. [BUG FIX] SPR ID: 070411473, 070411474, 070411475, 070411476 ITS #: 16872

Symptom: VPN traffic stops between two gateways.

Condition:

Topology:



- (1) Reset ZyWALL5/35/70 ROM file.
- (2) Configure the DMZ IP(10.10.10.1/24) and LAN(192.168.10.0/24) for ZyWALL35, LAN IP 192.168.100.0/24 as ZyWALL70's LAN.
- (3) Build the Gateway-to-Gateway VPN between ZyWALL35 and ZyWALL70 with the both LAN IP, then PC2 ping PC4, at this moment, it should be okay.
- (4) Configure the Dynamic VPN rule in the ZyWALL5 with the Local IP as PC1.
- (5) Build the VPN tunnel from PC3 (Safenet) to the ZyWALL5, after the tunnel build successfully, remove the PC1, then using the PC3 ping the PC1's IP.
- (6) Then, you will find PC2 can * t ping PC4.

18. [BUG FIX] ITS #: 17937

Symptom: ZyWALL CPU usage goes up to 100% with AS enable.

Condition:

Topology:

Mail server(A)-----(LAN)ZyWALL35(WAN)----Internet----Mail Relay(B)

- (1) Enable AS and select the WAN1->LAN.
- (2) Send mail from Mail Relay(B) to Mail Server(A). Mail server(A) is a sendmail on linux.
- (3) The usage of CPU will go up to >95% if the mail traffic includes PWAS option.

19. [ENHANCEMENT] SPR ID: 070614815, 070614816, 070614817, 070614818

Modified DDNS Log is not readable.

- (1) View DDNS Log in LOGS>>View Log.
- (2) DDNS Log is not readable, for example:
2007-05-07 17:44:52 DDNS update IP:138.188.40.255 (host 1) successfully

Was: DNS update IP:138.188.40.255 (host 1) successfully

Is: Update domain name zywall2wg.dyndns.org with IP:138.188.40.255 successfully|DDNS

Was: DDNS update error: The hostname specified does not exist. | Code: nohost
Is: Update error: The hostname specified does not exist. |DDNS

20. [BUG FIX] IITS: 17038 (For 3G product only)

Symptom & Condition: The port forwarding table of a disabled 3G-WAN 2 will be binded to the dial backup.

Condition:

1. Use ZyWALL device as the test device. ZyWALL is with the 3G-WAN 2 interface.
2. Setup different port forwarding tables on WAN 1 and WAN 2 interface.
3. Don't install or active 3G-WAN 2.
4. Setup and enable dial backup feature.
5. Made the connectivity of WAN 1 to fail, and the device will trigger the dial backup.
6. Outside devices can visit hosts on the LAN side according to WAN 2's port forwarding table.

21. [BUG FIX] ITS #14567

Symptom: IPSec tunnel cannot be built.

Condition:

ZyWALL-----NAT Router-----Fortinet 200

- (1) Create a VPN tunnel with Fortinet.
- (2) Enable NAT-Traversal.
- (3) Dial up this VPN tunnel but failed.

22. [FEATURE CHANGE]

For GUI->VPN Global Setting page, VPN skip overlapped check box changes to radio boxes and changes the description according to technical writer suggestion.

23. [ENHANCEMENT]

Add "WIRELESS" group in left panel and move the wireless features (network>wireless card, 3G) into it

24. [BUG FIX] SPR ID: ITS #:20283

Symptom: CI command "ip arp force on" does not take effect on WAN 2.

Condition:

1. Let WAN 1/WAN 2 active and has traffic on them.
2. CI command "ip arp status" to show that the timer of ARP entry would not decrease due to the existence of the traffic.
3. Use CI command "ip arp force on" to force the system to decrease timers of those WAN ARP entries periodically.
4. CI command "ip arp status" to show, timers of WAN 1 ARP entries would decrease, but timers of WAN 2 would not.

25. [ENHANCEMENT] SPR ID: ITS #:19903

Provide a CI command "ip arp reqUpadteTable [on/off]" to enable/disable that the device would use receiving ARP packet to update ARP table. The default value is off and the value will return to off when the device re-start.

26. [ENHANCEMENT] SPR ID: ITS #:18000

Add a hidden CI command "ipsec maxIkePskLength [31|32]" to turn on 32-byte PSK. After turn on 32-byte PSK, the user can save a 32-byte length IPsec Pre-share key. 32-byte PSK only can be used in ASCII format.

Modifications in V 4.03(WM.0)b1 | 05/04/2007

1. [ENHANCEMENT]

Support multiple profiles in the original content filter design.

The feature can define different group by IP and each group has its own profile which can

- (1) Have its own group definition to distinguish with other groups.
- (2) Restrict web features (Block ActiveX/Java Applet/Cookies/Web Proxy).
- (3) Restrict access according to selected categories.
- (4) Customize the list for trusted web site/Forbidden web site/Keyword blocking
- (5) Decide when the profile works by schedule.
- (6) Provide the information about which profile a packet belongs to in the log.

2. [ENHANCEMENT]

Add NAT over IPSEC feature for ZyWALL.

3. [ENHANCEMENT]

Design an Anti-Spam wizard GUI for helping users quickly configure the direction to check mail traffic.

4. [ENHANCEMENT] SPR ID: 060616955.

Customized port for ZyNOS 4.03 feature, it supports FTP, H323 and SIP protocols (ALG) now. It supplies 12 entries for user to define a new port number or a port range for FTP, H323 or SIP. Note: The default port of well known service will still work well even if the user customized another port for the same service. e.g. When the user defined port 1688 for FTP, the ZyWALL will support both port 21 and 1688 for FTP service at the same time.

5. [ENHANCEMENT]

Add Diagnostic feature for the ZyWALL to send out the system information automatically when the CPU load is reached the threshold. The purpose is for system diagnostic.

6. [ENHANCEMENT]

Add host-based load balance feature. Please see appendix 15 for more information.

CI command:

- (1) "ls hostBase enable" to enable or disable the feature.
- (2) "ls hostBase timeout" to set the timeout value.

7. [ENHANCEMENT]

Add 5 private SNMP traps for ZyWALL.

- (1) WAN interface down.
 - (2) WAN IP changes to x.x.x.x.
 - (3) CPU load reaches 100%.
 - (4) ZyWALL switches to Dial Backup.
 - (5) NAT table is full.
8. [ENHANCEMENT]
Support IXP425 B1 version CPU.
WAS: Support IXP425 A0/B0 version CPU.
IS: Support IXP425 A0/B0/B1 version CPU
9. [ENHANCEMENT] SPR ID: 060915885
GUI Enhancement on Firewall page.
- (1) Add rule number and edit icon in eWC>Default Rules for quick check rule summary..
 - (2) Change the packet direction to 2 list box for user to select "From" and "To" interface.
 - (3) Add "Any" selection in packet direction.
 - (4) Refine eWC>Rule Summary GUI data structure and fetch process.
 - (5) Change the "Move" process to alike ZW1050.
10. [ENHANCEMENT]
- (1) In eWC>VPN>VPN Rules (IKE) page, add an Active/Inactive hyperlink in every network policy.
 - (2) In eWC>VPN>GATEWAY POLICY-EDIT page, add Edit/Delete icons of "Associated Network Policies".
11. [ENHANCEMENT] SPR ID:060906253
Extend the length of Anti Spam Xtag from 23 to 47.
12. [ENHANCEMENT] SPR ID: 060807425
Enhancement of GUI Home page.
- (1) Add a link for Intrusion Detected/Virus Detected/Spam Mail Detected/Web Site Blocked to connect to its corresponding web page.
 - (2) Change the status of Intrusion Detected/Virus Detected/Spam Mail Detected
 - (a) N/A --- No Turbo Card.
 - (b) Disable --- UTM or main feature not active.
 - (c) Numeric --- The count of detected.
 - (3) Add note for UTM report.
13. [ENHANCEMENT] SPR ID: 060814859
Check if the decompressed inspection code size is over than the pre-allocated memory size for the software based IDP/AV.
14. [ENHANCEMENT] SPR ID : 060815905,050414612
We change the ZyWALL break mechanism for the infected file.

The ZyWALL just breaks the first infected file packet and stop track the file session in the previous mechanism. The old one has better performance, but there is a risk that it couldn't break the file with more than one virus. Now ZyWALL breaks the first infected file packet and the following file packet as well. It is safer but downs performance for handling infected files. Wet also fix the line-assembly bug for FTP and HTTP in this enhancement.

15. [ENHANCEMENT]

Support user defined Xheader in mail.

Note: User can use "%status" and "%score" to display mail status and SPAM score in XHeader. There are four kinds of mail status:

- (1) Black List (score always is 100)
- (2) SPAM
- (3) Phishing
- (4) Timeout (score always is 0)

16. [ENHANCEMENT] SPR ID: 060508423

Besides IE, the GUI IP field is supported in Netscape/Mozilla/Firefox.

- (1) The enhancement supports users copy/paste IP field to IP field on Netscape/Mozilla/Firefox.
- (2) The enhancement can also work in Linux.

17. [ENHANCEMENT]

Add direction information in logs of Anti-Virus, IDP and Firewall Attack.

18. [ENHANCEMENT] SPR ID: 060522258

If users let "Redirect URL" in Content Filter be blank, the blocking page will be displayed on the forbidden object only.

19. [BUG FIX] SPR ID: 060705202

Symptom: The format and content of "System Resources" is shown different in eWC>>Home and SNMP management software.

Condition:

- (1) See "System Resources" in eWC>>Home. They are shown like:

Flash	9/16 MB
Memory	42/64 MB
Sessions	87/10000
CPU	0%

- (2) See "sysCPUUsage", "sysFlashUsage", "sysRAMUsage" and "sysSessionUsage" in SNMP management software, e.g. SNMPC Network Manager. They are shown like:

```
sysCPUUsage.0=0
sysFlashUsage.0=3
sysRAMUsage.0=30
sysSessionUsage.0=0
```

- (3) You will find that the format and content shown in eWC>>Home is different

from SNMP management software.

20. [BUG FIX] ITS#: 14936

Symptom: This kind of URL request such as "http://www.host:80" can not pass through content filter trusted web site.

Condition:

- (1) Enable content filter and website customization.
- (2) Disable all web traffic except for trusted Web sites.
- (3) Add the website "http://www.sina.com" into trusted Web site.
- (3) Browse "http://www.sina.com:80" by Firefox and find it can not be visited.

21. [BUG FIX] ITS#: 14612

Symptom: ZyWALL cannot reply packet on correct WAN interface if the packet from some WAN subnet.

Condition:

- (1) Set ZyWALL WAN on A/A mode.
- (2) Put a PC on WAN2 subnet, and its IP is same subnet as WAN2 interface.
- (3) PC adds a route entry to redirect all packets to WAN1 interface.
- (4) PC cannot receive the reply packets.

22. [BUG FIX] SPR ID: 070123093,070123094,070123095

Symptom: Memory leak when doing IDP CLI operation.

Condition:

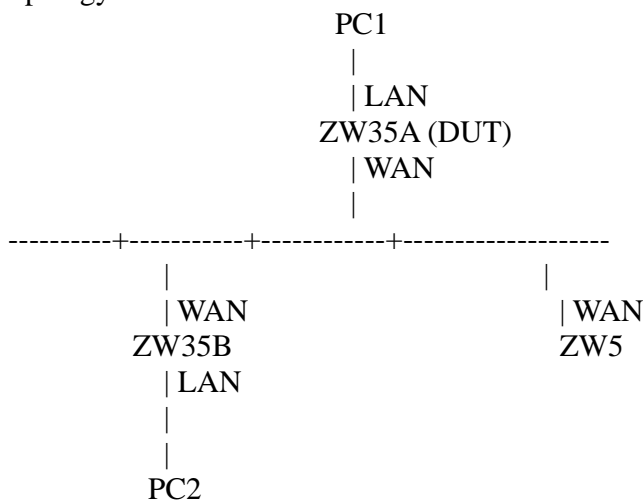
- (1) CI> idp sig load 12345
- (2) Repeating (1).
Memory leak!!

23. [BUG FIX] ITS#: 15003

Symptom: There will be a large latency in VPN1 if an new SA set up.

Condition:

Topology:



VPN1: ZW35B build a VPN with ZW35A

VPN2: ZW5 build a VPN with ZW35A

- (1) Build the VPN1 and ping PC1 from PC2.
- (2) Build VPN2.
- (3) There will be a large delay in the ping.

24. [BUG FIX] SPR ID: 060627810

Symptom: If the encapsulation type of WAN interface is PPPoE/PPTP, the conflict check will be failed when configuring LAN/DMZ/WLAN interface IP.

Condition:

- (1) Set WAN encapsulation as PPPoE/PPTP, and make sure the device can get the IP correctly.
- (2) In eWC->NETWORK->LAN->LAN, set "IP Address" to an IP which is the same subnet as WAN interface.
- (3) Finally the configuration can be saved but it should not.

25. [BUG FIX] SPR ID: 060705184

Symptom: The ordering of IDP signature is wrong.

Condition:

- (1) In eWC>AV>Signature>Switch to query view: select Signature Search by Attributes, Severe, DDOS and click search.
- (2) Click ordering by name. Check the result.
- (3) Do step (2) again and you will find the ordering is not right.

26. [BUG FIX] SPR ID: 060707351

Symptom: Can't enter SMT menu 4.

Condition:

- (1) In SMT menu 4, delete ISP's name. Save it.
- (2) In SMT menu 11, edit ISP's name as "WAN". Save it.
- (3) We can't enter SMT menu 4 anymore.

27. [BUG FIX] SPR ID: 060714836, 060714837, 060714838.

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.

28. [BUG FIX] SPR ID: 060721405.

Symptom: Traffic log does not work in bridge mode.

Condition:

- (1) Restore default romfile.
- (2) Switch to bridge mode.
- (3) Go to eWC>SYSTEM REPORTS page, enable "Send Raw Traffic Statistics to

Syslog Server for Analysis".

- (4) Go to eWC>LOGS>Log Settings page, activate "Syslog" and setup the syslog server IP as PC_A.
- (5) PC_A enables the Kiwi Syslog Daemon.
- (6) There is no traffic log sent to kiwi Syslog Daemon anymore.

29. [BUG FIX] SPR ID: 060725664.

Symptom: DNS cannot be updated in bridge mode.

Condition:

- (1) Restore default romfile.
- (2) Switch device to bridge mode (do not set DNS right now).
- (3) Go to eWC>BRIDGE>Bridge, set the DNS server as 172.23.5.1 and save it.
- (4) Go to another page and back to this page, you will find the DNS server is 0.0.0.0.

30. [BUG FIX] SPR ID: 060714862

Symptom: IPSec High Availability failed when enable Nailed-Up. The VPN connection swaps between primary and secondary gateway continuously.

Condition:

```
PC1-----| /------(W)ZW35(L)----PC2
            | \------(W)ZW70(L)----PC3
            |
```

- (1) Create one VPN tunnel for PC1 and PC2
- (2) Redundant Remote Gateway = ZW70
- (3) Enable Nailed-Up for DUT, ZW35 and ZW70.
- (4) DUT always reconnect tunnel between ZW35 and ZW70.

31. [BUG FIX] SPR ID: 060731994, 060731995

Symptom: Policy route is failed in a special topology.

Condition:

Topology:

```
                ZyWALL 70
                ||
PC1(192.168.1.33)------(SWITCH)------(192.168.2.33)ZyWALL
35(192.168.10.1)-----PC2(192.168.10.33)
```

- (1) The device under test is ZyWALL 70, the LAN subnet is 192.168.1.x with a LAN IP alias 192.168.2.x.
- (2) In ZyWALL 70, there is a policy route rule that will redirect the range 192.168.10.1-192.168.10.250 to 192.168.2.33.
- (3) In ZyWALL 35, disable NAT and firewall feature.
- (4) Ping PC1 from PC2, there is no response.

32. [BUG FIX] SPR ID: 060822312, 060822309, 060822310

Symptom: Trigger dial function is abnormal if we blocked all traffic from LAN to

WAN.

Condition:

- (1) Reset to default factory.
- (2) Setting a correct PPPoE connection in WAN interface, disable "nailed-up", and idle timer is 20 seconds.
- (3) Enable firewall, and block all traffic from LAN to WAN.
- (4) Ping "168.95.1.1" continuously in a LAN side PC, WAN interface still can get IP. (It means WAN interface still can be triggered but the ping packet should be dropped by firewall.)

33. [BUG FIX] SPR ID: 060918066

Symptom: Bridge mode VPN AV can not recognize ZIP file.

Condition:

[Topology]

FTP Server --- DUT1(Bridge) ----- PC

- (1) DUT1 is in bridge mode, and then enables AV for FTP Server to PC and PC to FTP Server.
- (2) PC uploads a zip file to FTP Server. (The file is zipped with WinZIP)
- (3) DUT logs AV can not recognize the zip type; and there are many logs for it.

34. [BUG FIX] SPR ID: 060914870

Symptom: There will be lots of "Common TOS double free" log by SYN flooding tool.

Condition:

- (1) Reset to default factory.
- (2) Change the device to bridge mode.
- (3) Set a firewall rule for port 21 in WAN to LAN direction.
- (4) The PC in WAN side uses SYN flooding tool (destination port is 21) to attack a PC in LAN side.
- (5) Keep attacking and reboot the device.
- (6) Check the centralized log, there be lots of "Common TOS double free" log.

35. [BUG FIX] SPR ID: 060926698

Symptom: The default route learning from LAN side router cannot work.

Condition:

Topology:

PC-----(192.168.1.1)DUT(WAN)

|
---(192.168.1.100)Router(WAN)----- (Internet)

- (1) Disconnect WAN cable of DUT, and connect WAN cable of router.
- (2) DUT and router restore default romfile.
- (3) Change router's LAN IP as "192.168.1.100" and disable LAN DHCP server.
- (4) DUT will learn a default route from router.
- (5) PC cannot access internet from the default route.

36. [BUG FIX] SPR ID: 060915931,060919187

Symptom: SIP phone can not dial to VPN peer for PPPoE.

Condition:

Topology:

P2002(A) --- DUT1(PPPoE) =====VPN TUNNEL===== DUT2 --- P2002(B)

- (1) DUT1 WAN is PPPoE.
- (2) DUT1 and DUT2 enable SIP ALG.
- (3) DUT1 and DUT2 build a VPN tunnel.
- (4) P2002(A) dials P2002(B). Connection is success, but P2002(A) can not hear P2002(B)'s voice; P2002(B) can hear P2002(A).

37. [BUG FIX] SPR ID: 061020683

Symptom: PPPoE and PPTP can't be dropped in SMT24.1.

Condition:

- (1) WAN1 is PPPoE or PPTP.
- (2) Go to SMT24.1 and click "1" to drop WAN1.
- (3) But WAN1 is still alive.

Note: This problem only happens on the device that include 3G WAN.

Modifications in V 4.02(WM.0) | 03/21/2007

Modify for formal release.

Modifications in V 4.02(WM.0)b1 | 03/21/2007

Convert firmware version to 4.02.

Modifications in V 4.01(WM.4) | 03/20/2007

Modify for formal release.

Modifications in V 4.01(WM.4)b2 | 03/12/2007

1. [BUG FIX] 070206549

Symptom:"Ping of Death" function work error when set packet length !=1500.

Condition:

Case 1:

- (1) Use command "ip icmp death 800" to set the packet length for "Ping of Death" check.
- (2) On LAN pc, use DOS command "ping 192.168.1.1 -l 1000",
- (3) Result should be can't ping success, and in DUT, display ping of death log. But actual result is ping success, and no log.

Case 2:

- (1) Use command "ip icmp death 2000" to set the packet length for "Ping of Death" check.
- (2) On LAN pc, use DOS command "ping 192.168.1.1 -l 1600",
- (3) Result should be can ping success. But actual result is can't ping success.

2. [BUG FIX] 061019655, 061025917, #ITS 15659

Symptom: Device does not log any CF customization events.

Condition:

- (1) Enable content filtering.

- (2) Enable Web site customization in the Customization page.
 - (3) Add Forbidden Web Site or Keyword Blocking.
 - (4) Access the Web Page which should be blocked.
 - (5) You can see the blocked page but there is no blocked log in the Logs page.
3. [BUG FIX] #ITS 14936
Symptom: This kind of URL request such as "http://www.host:80" can not pass through content filter trusted web site.
Condition:
 - (1) Enable content filter and website customization.
 - (2) Disable all web traffic except for trusted Web sites.
 - (3) Add the website "http://www.sina.com" into trusted Web site.
 - (4) Browse "http://www.sina.com:80" by Firefox and find it can not be visited.
4. [BUG FIX] 070206508, 070206509, 070206510
Symptom: Remove PPP option in Help page of 'Dial Backup>PPP option'.
5. [BUG FIX] 070206501, 070206502, 070206503
Symptom: Content Filter "Restrict Web Features" is inconsistent behavior on appeared of page when enable or disable "Don't block trusted Web sites".
Condition:
 - (1) Enable Content Filter and block ActiveX, Java Applet.
 - (2) Denied Access Message is "page denied!", redirect url is "http://www.zyxel.com".
 - (3) Visit ActiveX or Java Applet web site like as
http://dob.tnc.edu.tw/themes/old/showPage.php?s=152&t=5&at=".
 - (4) The "dob.tnc.edu.tw" will be blocked and redirect to www.zyxel.com.
 - (5) Enable customization, enable "Don't block Java/ActiveX/Cookies/Web proxy to trusted Web sites.", then visit "dob.tnc.edu.tw" web site again, the ActiveX or Java Applet site page will not blocked and redirect.
6. [BUG FIX] 070209906
Symptom: IXIA AS stress test will cause DUT crash.
7. [BUG FIX] #ITS 14652 , 070210001, 070212045, 070212047
Symptom: A crash issues reported by Studerus.
Condition:
 - (1) Enable Content Filter and External DB.
 - (2) Sometimes DUT will crash in WuXi PQA LAB and customer site.
8. [BUG FIX] 070212068
Symptom: Device crash sometimes.
Condition:
 - (1) Let device register to Vantage with Ether encapsulation.
 - (2) Change WAN encapsulation from Ether to PPPoE and fill incorrect login name and password.

- (3) Device's WAN can't dial up because incorrect login name and password.
- (4) Device crash after 2 minutes.

9. [BUG FIX] 070208756

Symptom: Device crash.

Condition:

- (1) Configure device via Vantage.
- (2) Reset device to default setting. Then register to Vantage again.
- (3) Start synchronizes all setting from Vantage to device.
- (4) Device crash sometimes.

10. [BUG FIX]

Symptom: DUT will crash when some URL longer than specific array.

Condition:

- (1) Enable Content Filter and External DB.
- (2) Sometimes DUT will crash in WuXi PQA LAB.

11. [BUG FIX] #8753, #ITS 14652

Symptom: DUT will crash sometime.

Condition:

- (1) Enable NAT.
- (2) Sometimes DUT will crash in customer site.

12. [ENHANCEMENT]

Add Vantage CNM device agent – 2.1.4(WM.0) which supported with Vantage CNM server -- version 2.3.01.61.00.

Modifications in V 4.01(WM.4)b1 | 01/29/2007

1. [BUG FIX] 061102088

Symptom: The MIB OID for UTM AV and IDP does not work.

Condition:

- (1) Reset to default romfile.
- (2) PC installs SNMP software, such as MG-SOFT MIB Browser.
- (3) Try to get value of OID, 1.3.6.1.4.1.890.1.6.1(the AV/IDP signature version and Sigdate) will fail.

2. [ENHANCEMENT] 061120101

Add CI command "ip icmp death [size (0~65535, 0: default)]" to set the packet length for "Ping of Death" check.

Note: Default size is 1500.

3. [BUG FIX] 061107359

Symptom: Traffic can not be sent out through WAN port when using AV+IDP+VPN.

Condition:

PC1--- (LAN) ZyWALL5 (WAN) ---- (WAN) ZyWALL70 (LAN) --- PC2 (FTP, HTTP Server)

- (1) Setup one VPN between ZW5 and ZW70.
 - (2) Enable the AV and IDP in ZW5, and enable the zip file scan in AV.
 - (3) PC1 start FTP and HTTP download one 50Mbps ZIP file.
 - (4) About 3 minutes, PC1 can not ping PC2 and can not access Internet.
4. [ENHANCEMENT]
- (1) Support direct ACK/BYE sip request.
 - (2) Support different global IP address for SIP clients and SIP server.
- Note: Please refer to the appendix 14, we solve the limitation about item 2 and 3.
5. [BUG FIX] 061106276
- Symptom: Content filter cache log error.
- Condition:
- (1) Reset default romfile.
 - (2) Registration to gfnet.zyxel.com.tw
 - (3) eWC> Content Filter> General, enable content filter.
 - (4) eWC> Content Filter> Categories, select Business categories, click "Apply".
 - (5) Access <http://www.tcc.net.tw>
 - (6) Check log OK.
 - (7) Again to access <http://www.tcc.net.tw>
 - (8) Log should be displayed as “www.tcc.net.tw: Business/Economy(cache hit)|WEB BLOCK”, not “(cache hit)|WEB BLOCK”.
6. [BUG FIX] 061113707
- Symptom: Content filter trusted web will be blocked when select "Don't block Java/ActiveX/Cookies/Web proxy to trusted Web sites."
- Condition:
- (1) Enable Content filter, enable blocking Active X, Cookie, Java Applet, and Proxy server.
 - (2) Edit web eWC/Content Filter/Customization. Add Trusted Web Site “www.google.com.tw”, “update.microsoft.com”, “www.csie.nctu.edu.tw” to trusted web sites list.
 - (3) Enable "Don't block Java/ActiveX/Cookies/Web proxy to trusted Web sites."
 - (4) PC open web “<http://www.google.com.tw>”, “<http://update.microsoft.com>”, it will be blocked.
7. [BUG FIX] 061123342, 061123343
- Symptom: ZyWALL (bridge mode) does not support more than 1 VPN client at the same time.
- Condition:
- Topology:
- ZyXEL VPN Clients ----- Internet ----- ZyWALL 70(Bridge Mode) ----- LAN
- (1) Configure one dynamic VPN rule in ZyWALL 70.
 - (2) In above topology, two or more clients over the internet can successfully establish VPN tunnel with ZyWALL 70.
 - (3) But only the first connected VPN client can access ZyWALL 70's LAN side at a

time.

8. [BUG FIX] 061128584, 061128585 (ITS#13932)
Symptom: Device crashes by hardware watchdog.
Condition:
Topology:
(a) PC --- [LAN]ZyWALL[WAN] --- HTTP server
(b) HTTP server --- [LAN] ZyWALL [WAN] --- PC
(1) Restore default romfile.
(2) When the PC connects to HTTP server (<http://www.alektogroup.com>) by ZyWALL, the ZyWALL will crash sometimes.
9. [BUG FIX] ITS#12880
Symptom: ZyWALL configured to establish Dial Backup with CDMA ISP through RWT FCT CDMA, but does not work.
Condition:
(1) Configure Dial Backup setting.
(2) Turn off ZyWALL PPP PFC (Protocol Field Compression) setting. This can be showed by CI command "ppp lcp pfc". Default PFC setting is off.
(3) WAN1 & WAN2 down, Dial Backup is up.
(4) The Dial Backup session between the ZyWALL and ISP is established, ZyWALL got an IP address provided by the ISP, but the PC in LAN can't ping to an Internet host. ZyWALL can receive and transmit the ping request, and can receive reply from remote host, but ZyWALL won't transmit the reply to the PC in LAN.
10. [BUG FIX] 061121145 (ITS#13200)
Symptom: Failed to call the SIP phone on DMZ side with Firewall enabled.
Condition:
(1) Turn on Firewall. Set ZyWALL5's default firewall rule for WAN-->DMZ is dropped.
(2) Turn on SIP ALG setting.
(3) Set up following topology:
 phone --- P2002 --- [DMZ]ZW5[WAN] --- SIP server --- VoIP phone
(4) As soon as P2002 registers to the SIP server, there is no problem for the phone both call in and call out. But after a while, the phone on DMZ side cannot receive any phone calls, although it's still far before "SIP ALG Timeout" configured on the ZyWALL. Only after the P2002 register again, can the phone on DMZ side receive calls, and the cycle repeats.
11. [BUG FIX] ITS#13995
Symptom: ZyWALL cannot show the the block message of content filter complete in MSIE7.0 and Firefox.
Condition:
Topology:
PC --- [LAN] ZyWALL [WAN] --- Internet

- (1) In router mode, enable content filter and set the block message but leave the Redirect URL blank.
 - (2) Enable external database content filtering and block matched web pages.
 - (3) Select search engines/portals categories.
 - (4) Open the <http://www.sina.com.cn> in Firefox and MSIE7.0. The block message cannot be shown completely in MSIE7.0 and nothing in Firefox.
12. [BUG FIX] 061122298, 061122299, 061122300, 061107323
Symptom: Sometimes DUT cannot detect eicar AV.
Condition:
Topology: PC1 --- [LAN] DUT [WAN/Public IP] --- Internet.
- (1) Restore default romfile.
 - (2) Register DUT AV function.
 - (3) Set WAN IP= Ethernet/Static IP(Public IP).
 - (4) Go to eWC>>ANTI-VIRUS>>General page, enable Anti-Virus, enable ZIP file Scan, active HTTP service for all interface.
 - (5) PC1 accesses http://www.eicar.org/anti_virus_test_file.htm to download eicar.com file.
 - (6) Sometimes DUT cannot detect this Anti-Virus file (eicar.com).
13. [BUG FIX] 061218035
Symptom: Device crashes sometimes when you use Anti-Spam function.
Condition:
- (1) Restore default romfile.
 - (2) Register Anti-Spam service.
 - (3) Go to eWC>>ANTI-SPAM>>General page, enable Anti-Spam for all directions, active "Discard SMTP mail.Forward POP3 mail with tag in mail subject".
 - (4) Go to eWC>>ANTI-SPAM>>External DB page, enable External Database, set Threshold= 0.
 - (5) Send a large mail (> 20K) from LAN to WAN, the device will loss mbuf.
14. [BUG FIX] 061212754
Symptom: Device crashes sometimes when you use Anti-Spam function.
Condition:
- (1) Enable Anti-Spam & External Database.
 - (2) System crashes sometimes on customer site.
15. [FEATURE CHANGE] 061218034
For Anti-Spam external database server control,
WAS: ZyWALL will refresh server list if available server <= 2.
IS: ZyWALL will refresh server list if available server <= 1 but keep the last available server.
16. [ENHANCEMENT]
Combine cnm encryption CLI from two commands to one command.
WAS: Change cnm encryption mode with 2 CLIs: 'cnm encrykey <key>' and

'cnm encrymode <mode>'.

IS: Change cnm encryption mode with one CLI: 'cnm encry <mode> <key>'

17. [BUG FIX] 070105291

Symptom: DUT reboot.

Condition:

- (1) Set DUT WAN as PPPoE connection
- (2) Enable H323 alg
- (3) Firewall forward H323 protocol from WAN1 to LAN
- (4) DUT forward 1720 port from WAN1 to LAN
- (5) Make a H323 connection from WAN to LAN using OpenH323 software, DUT can reboot.

18. [BUG FIX]

Symptom: Ping DMZ IP from PC in DMZ. You can't get response

Condition:

- (1) Set LAN IP and add two IP Alias. Make sure they like 192.168.200.100. That is each number separated by periods is ≥ 100 .
- (2) Set DMZ IP and add two IP Alias. The rule is the same with description above
- (3) PC connects to devcie's DMZ port and ping device's DMZ IP.
- (4) Can't get response from device.

19. [BUG FIX]

Symptom: iChat behind ZyWALL can not make a video call with another iChat in WAN.

Condition:

Topology:

iChat_1----- (LAN) ZyWALL (WAN) ----- iChat_2

- (1) In router mode Apple Mac iChat_1 made a video call request to iChat_2 on WAN.
- (2) iChat_1 failed to set up the video call with iChat_2.

20. [BUG FIX]

Symptom: Help info about "domain name" in h_AS_Custom_Edit.html is not consistent with ZyWALL function.

Condition:

Help info about "domain name" in h_AS_Custoe_Edit.html is not consistent with ZyWALL function.

21. [FEATURE CHANGE]

Remove PPP Option configuration in WAN>>>Dial Backup and SMT.

22. [BUG FIX]

Symptom: ZyWALL70 loses static route entry when WAN down and up again.

Condition:

- (1) Set WAN operation mode as Active/Active mode.
- (2) Set a static route, let traffic go to some destination A by WAN2.

- (3) When WAN2 is down, using "ip route" to show route table, the static route disappears, the traffic goes to some destination will go through WAN1.
- (4) After WAN2 is up again, the static route won't come back, the traffic to destination A still goes through WAN1.

23. [ENHANCEMENT]

Support IXP425 B1 version CPU.

WAS: Support IXP425 A0/B0 version CPU

IS: Support IXP425 A0/B0/B1 version CPU

24. [BUG FIX] 061213832; 061213856; 061213859; 061213854; 061213855;
061213858

Symptom: ZyWALL can't tag the mails sent by Exchange 2003 SP2.

Topology:

Exchange 2003(SP2)---ZyWALL---Other mail servers(not Exchange 2003 SP2)

Condition:

(1) Configure a Black list.

(2) Send mails (with subjects configured in the Black list) from the Exchange 2003(SP2) to other mail servers. The ZyWALL will not tag the mails pass through it.

Modifications in V 4.01(WM.3) | 12/04/2006

Modify for formal release.

Modifications in V 4.01(WM.3)b1 | 11/24/2006

1. [ENHANCEMENT] SPR ID: 061109533

Enlarge mail header size from 1024 to 2048.

2. [BUG FIX] SPR ID: 060711576

Symptom: Content filter is fail when user installs Outpost Firewall.

Condition:

(1) Install OutpostPro Firewall software.

(2) Set "disable all web traffic except for trusted web sites" and enable content filter.

(3) Enable Outpost Firewall, user can surf the website as usual.

(4) If we disable Outpost Firewall, web surfing will be blocked besides trusted web sites.

3. [BUG FIX] SPR ID: 060810690

Symptom: Redirect URL have not limit special character, it will caused DUT crash.

Condition:

(1) In eWC>CF Denied Access Message or Redirect URL, input %s%s%s%s and apply, DUT will be crash.

4. [BUG FIX] SPR ID: 060927777

Symptom: The "Up Time" shown on the Port Statistics and Home page is quite different when the ZyWALL uptime is more than 100 hours.

Condition:

- (1) Let ZyWALL WAN1 uptime be more than 300 hours.
- (2) Go to eWC>HOME page, the "Up Time" is "4:00:00".
- (3) Click "Port Statistics" button, the WAN1 "Up time" of pop-up window is "300.00.00".

5. [BUG FIX] SPR ID: 060420608

Symptom: Two SIP clients cannot talk to each other when both of them are in LAN.

Condition:

Topology:

SIP Client_A -----(LAN) ZyWALL (WAN)-----SIP Server
SIP Clinet_B -----|

- (1) Two SIP clients register on SIP server which is in the WAN.
- (2) Create a call between client A and client B, they cannot hear each other.

6. [BUG FIX] SPR ID: 060419442, 060512720, 060601086

Symptom: The VoIP client cannot hear the voice when SIP server is set behind the LAN.

Condition:

Topology:

P2002A-----+-(LAN)ZW70(WAN)-----P2002B
SIP Server-----|

(1) Create a port forwarding rule on ZW70 to let SIP traffic of P2002B can be forwarded to SIP server.

(2) Dial a phone call from P2002A to P2002B, P2002B can hear the voice of P2002A but P2002A cannot hear the P2002B.

7. [ENHANCEMENT]

Symptom: SIP alg enhancement. Additional SIP ALG codes to supports SIP server on LAN or WAN

Condition: SIP function has some issues to work correctly.

Topology:

- (1) Client_A-----(L)ZW_1(W)-----SIP Server----- (W)ZW_2(L)-----Client_B
- (2) Client_A----SIP Server----(L)ZW_1(W)----- (W)ZW_2(L)-----Client_B
- (3) SIP Server----(L)ZW_1(W)----Client_A----(W)ZW_2(L)-----Client_B
- (4) SIP Server----(L)ZW_1(W)----- (W)ZW_2(L)+-----Client_A
+-----Client_B

8. [ENHANCEMENT] SPR ID: 061102140

Add PPTP CHAP v2 support.

9. [BUG FIX]

AV side effect fix.

10. [BUG FIX] SPR ID: 061024810

15. [BUG FIX] SPR ID: 060822272

Symptom: ZyWALL will not mail its LOG if the IP specified on the One-To-One Public IP.

Condition:

Topology:

```
Mail Server------(DMZ)ZyWALL(WAN)
192.168.2.33      192.168.2.1    10.0.0.1
                                     10.0.0.2
```

(1) Restore to default romfile.

(2) Set NAT type to full feature.

(3) Build a one-to-one rule for mail server in DMZ.

```
Local IP      Global IP
192.168.2.33 <-> 10.0.0.2
```

(4) In the LOG setting, set mail server IP to 10.0.0.2.

(5) Then, disable the firewall and press the "Email Log Now" button to send mail.

(6) You will see the log "SMTP fail (Cannot connect to SMTP server 10.0.0.2)".

16. [BUG FIX]

Symptom: ZyWALL cannot trigger dial backup.

Condition:

Topology:

PC--(LAN)ZyWALL(dial backup)--Internet

(1) Restore default romfile.

(2) Set up dial backup.

(3) PC sets ZyWALL to be DNS proxy server.

(4) PC starts to ping a domain name, but ZyWALL do not trigger dial backup.

17. [BUG FIX] SPR ID: 061005220

Symptom: Device crashes because of mbuf double free in Anti-Spam.

Condition:

(1) System crashes sometimes on customer site.

18. [ENHANCEMENT]

Vulnerability bug: It depends on an error in verifying the PKCS-1 padding of the signed hash and we update the patch file from safeNet.

Modifications in V 4.01(WM.2) | 10/25/2006

Modify for formal release.

Modifications in V 4.01(WM.2)b1 | 10/18/2006

19. [ENHANCEMENT] SPR ID : 060815905,050414612

We change the ZyWALL break mechanism for the infected file. The ZyWALL just breaks the first infected file packet and stop track the file session in the previous mechanism. The old one has better performance, but there is a risk that it couldn't

break the file with more than one virus. Now ZyWALL breaks the first infected file packet and the following file packet as well. It is safer but downs performance for handling infected files. We also fix the line-assembly bug for FTP and HTTP in this enhancement.

20. [ENHANCEMENT] SPR ID: 060809590, 060809591, 060809592.
The Anti-Spam will modify the server response string ""250[-]PIPELINING" to "250[-]PIPE*****". Because ZyWALL does not the SMTP PIPELINING function.
21. [ENHANCEMENT] SPR ID: 060830643
Add an option to enable or disable the "Dynamic ACL" log in ZyWALL.
The check box is in:
(1) "eWC->LOGS->Log Settings->Dynamic ACL".
(2) SMT 24.8.
I. "sys logs load".
II. "sys logs switch dynacllog".
III. "sys logs save".
IV. "sys logs switch display".
Note: "2006-08-09 00:42:30 Firewall matches a dynamic ACL rule of an ALG session: TCP 192.168.111.2:50999 66.59.243.66:26397 ACCESS PERMITTED"
Engineer Note: The value in default ROM file is "on" in 4.01.
22. [ENHANCEMENT]
Wording changed. Out of memory when F/W upload.
(1) FTP
Was: file size too large.
Is: file size too large. Please reboot device, and try again.
(2) HTTP/HTTPS
Was: disk full!
Is: disk full! Please reboot device, and try again.
23. [ENHANCEMENT] SPR ID: 060522258
If users let "Redirect URL" in Content Filter be blank, the blocking page will be displayed on the forbidden object only.
24. [ENHANCEMENT] SPR ID: 060925662
In eWC>MAINTENANCE>Time and Date, add "Madrid" capital in "GMT+1" time zone.
25. [FEATURE CHANGE] SPR ID: 060705182, 060705183
WAS: Set "My IP" as WAN2 IP Address in VPN IKE rule, the IKE and IPSec traffic still go through WAN1 because WAN1 has higher metric than WAN2.
IS: The IKE and IPSec packets will be sent out according to "My IP" field in VPN IKE rule.
Engineer note: The bug fix only applies to multiple WAN products.

26. [BUG FIX] SPR ID: 060809598

Symptom: PC can not access the web server (www.fapa.com.pl) via our ZyWALL.

Condition:

PC---(LAN)ZyWALL(WAN)---internet

- (1) Get a ZyWALL with default romfile.
- (2) Let PC try to access www.fapa.com.pl.
- (3) PC can not access the web server.
- (4) It is OK without ZyWALL.

Special case packet flow:

Client(PC)

Server(www.fapa.com.pl)

SYN ->

<- ACK = 0

<- SYN, ACK = 1

ACK = 1 ->

HTTP Get ->

27. [BUG FIX] SPR ID: 060711547

Symptom: "Don't block Java/ActiveX/Cookies/Web proxy to trust Web site" function in content filter cannot work.

Condition:

(1) In eWC->SECURITY->CONTENT FILTER->General page, enable "Content filter" and

block "Java Applet/ActiveX/Cookies/Web Proxy".

(2) In eWC->SECURITY->CONTENT FILTER->Customization page, enable "Web site customization" and

"Don't block Java/ActiveX/Cookies/Web proxy to trusted Web sites".

Add "web.haccpsoft.it" to "Trusted Web Sites".

(3) A PC in ZYWALL's LAN side browses "http://web.haccpsoft.it:8080" website.

(4) Login in and click the date, the popup window should show a calendar instead of another login page.

(5) It is blocked by content filter.

28. [BUG FIX] SPR ID: 060607461

Symptom: After run 5 hours BT, no traffic can be forwarded by ZyWALL.

Condition:

(1) Restore to default romfile.

(2) In NAT port forwarding page, add a rule with port range from 20000 to 40000.

(3) After running about 5 hours BT, no traffic can pass through ZyWALL.

29. [BUG FIX] SPR ID: 060925635, 060727788.

Symptom: System crashes.

Condition:

(1) Enable Firewall, Content Filter, IDP, Anti-Virus and Anti-Spam Functions, and turn on all related logs.

(2) System crashes sometimes.

30. [BUG FIX] SPR ID: 060831744

Symptom: PC cannot ping WLAN interface IP.

Condition:

Topology:

PC1(10.0.0.1)----(10.0.0.2)(WAN)ZyWALL(WLAN)(192.168.7.1)

- (1) Restore default ROM file.
- (2) Disable firewall feature.
- (3) In SMT 24.8, type "ip nat routing 2 1".
- (4) Set WLAN interface IP as "192.168.7.1".
- (5) Set NAT to "Full Feature" mode.
- (6) PC1 generates a PING packet to "192.168.7.1".
- (7) There is no response from "192.168.7.1" and the centralized log will show "Packet without a NAT table entry blocked: ICMP(Echo)"

31. [BUG FIX] SPR ID: 060703050

Symptom: Local PC cannot find Remote Host by NetBIOS via VPN tunnel.

Condition:

PC1----(WLAN)DUT----- (VPN)-----ZYWALL(LAN)----PC2

- (1) The configured romfile please refer to SPR.
- (2) PC1 cannot see PC2 by NetBIOS via VPN tunnel.

Note: This problem only happens when policy index is not equal to IKE index.

Engineer Note: This problem happens in 4.00 and 4.01.

32. [BUG FIX] SPR:060925632

The firmware of 4.01's self-assigned-certificate can't be used in Mozilla-firefox

33. [BUG FIX] SPR ID: 060908449

Symptom: The ZyWALL assigns a used IP to a DHCP client.

Condition:

Topology ZyWALL(LAN)-----PC1,PC2

- (1) Let the PC1 get a DHCP IP(192.168.1.33).
- (2) Pull out the cable of PC1 and set PC2 to use a static IP 192.168.1.33.
- (3) Plug back the PC1, PC1 starts to get a DHCP IP, but it still gets 192.168.1.33, although the ZyWALL has asked if someone is using this IP and gets a response. IDP module.

Modifications in V 4.01(WM.1) | 09/07/2006

Modify for formal release.

Modifications in V4.01(WM.1)b1 | 08/31/2006

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. [ENHANCEMENT]
Add ALG type on policy route.
7. [BUG FIX]
Symptom: ZyWALL WAN fixed 100/full negotiation fail against cisco 3550/2900.
Condition:
 - (1) Configure cisco 3550/2900 port to fixed 100/full.
 - (2) Configure ZyWALL WAN to fixed 100/full.
 - (3) ZyWALL WAN can not sync up; remain down.
8. [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.
9. [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.

10. [BUG FIX]

Symptom: PPTP can not pass through ZyWALL from time to time.

Condition:

Topology:

PPTP server --LAN ZYWALL WAN 1--PPPoE—internet WAN 2--PPPoE--internet

- (1) Choose Active/Active mode in WAN setting.
- (2) Build PPPoE connection both on WAN1 and WAN2
- (3) Set Port forwarding 1723 to LAN PPTP server both on WAN1 and WAN2
- (4) PPTP client builds connection, and disconnect it through WAN1; then PPTP client can not builds PPTP connection through WAN2.

11. [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)

12. [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.

13. [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.

14. [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.

15. [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.

16. [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(WM.0) | 08/08/2006

Modify for formal release.

Modifications in V4.01(WM.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.

2. [BUG FIX]

Symptom: PC in LAN side sometimes can get IP address from DHCP server in WAN side after downgrading from v4.01 with bootbase v1.09 to previous firmware version.

Condition:

- (1) With bootbase v1.09,downgrading firmware from v4.01(WM.0)b4 to v3.62(WM.7)c0 then factory reset.

- (2) PC in LAN side sometimes can get IP address from DHCP server in WAN side.

Modifications in V4.01(WM.0)b4 | 07/11/2006

1. [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.
2. [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.
3. [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 V 4.01(WM.0)b3 | 06/25/2006

4. [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>
5. [FEATURE CHANGE]
Change some wordings which contain "fail back" in GUI and log.
Was: "Fail back *****".
Is: "Fall back *****".
6. [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"
7. [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%.
8. [ENHANCEMENT]
Enlarge Anti-Spam session number from 30 to 200
9. [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.

10. [ENHANCEMENT]
 - (3) In eWC>HOME page, show MAC address in Network Status Table.
[060606360]
 - (4) Change ZyWALL eWC refresh pages to consistent with HOME page.
[060606359]

11. [BUG FIX]

Symptom: Device will crash in bridge mode AV testing.
Condition: PC(mail client)----(LAN)DUT(WAN)----Mail Server

 - (5) In bridge mode, enable AV and activate SMTP from LAN to WAN direction.
 - (6) Disable Outlook SMTP authentication in PC.
 - (7) PC on LAN and sent out Microsoft Outlook testing mail.
 - (8) Device will crash immediately.

12. [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.

13. [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.

14. [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.

15. [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.

16. [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.

17. [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.

18. [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'.

19. [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.

20. [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.

21. [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.

Modifications in V 4.01(WM.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>Anti-Virus> 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][060502049]

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] [060516907]

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][060517002]

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][060423782]

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 proposal.

(3) This IKE rule cannot save.

12. [BUG FIX][060515863]

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][060427219]

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][060424803]

Symptom: ZyWALL crashes after changing MAC address.

Condition:

- (1) Take a registered device and reboot it.
- (2) After device boot up, use CLI "sys my serviceR" to refresh the registration.
- (3) When you get the "Service refresh successfully" message, use the CLI "sys atwz 0000aazzzzzz" (Change the MAC address you want) to change the MAC address.
- (4) Device will crash when rebooting.

15. [BUG FIX][060509567]

Symptom: Bridge mode Network Status Bridge Port loss DMZ port.

Condition:

Bridge mode in GUI Home> Network Status>More> Bridge Port loss DMZ port.

16. [BUG FIX][060509570]

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.

17. [BUG FIX][060426102]

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.

18. [BUG FIX][060503068]

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.

19. [BUG FIX][060502057]

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.

20. [BUG FIX][060424820]

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".

21. [BUG FIX][060502036]

Symptom: The eWC>DNS>DHCP cannot get WAN2 DNS.

Condition:

- (1) Restore default romfile.
- (2) WAN2 connects to DHCP server and gets IP and DNS successfully.
- (3) Go to eWC>DNS>DHCP page, the IP field cannot get WAN2 DNS.

22. [BUG FIX][060427214]

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.

23. [BUG FIX][060329452]

Symptom: In eWC>VPN, VPN Rules page shows incorrect domain name.

Condition:

- (1) Go to eWC>DNS>DDNS, set a WAN domain name as "123456789.123456789.123456789.123456789.123456789.123".
- (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.

24. [BUG FIX][060420654]

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".
- (2) Wireless Client can scan the "testWlan" network by Odyssey tool.
- (3) Disable wireless card.
- (4) Wireless Client still can scan the "testWlan" network by Odyssey tool.

25. [BUG FIX][060426084]

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.

26. [BUG FIX][060424869]

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".

27. [BUG FIX][060426102]

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".

28. [BUG FIX][060424823]

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.

29. [BUG FIX][060423784]

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.

30. [BUG FIX][060412729]

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).

31. [BUG FIX][060420625]

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.

32. [BUG FIX][060411623]

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.

33. [BUG FIX][060425022]

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

34. [BUG FIX][060418336]

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 use the tfgen, all the traffic from LAN can't go outside.

Modifications in V 4.01(WM.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 addresses.
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.

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.

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.

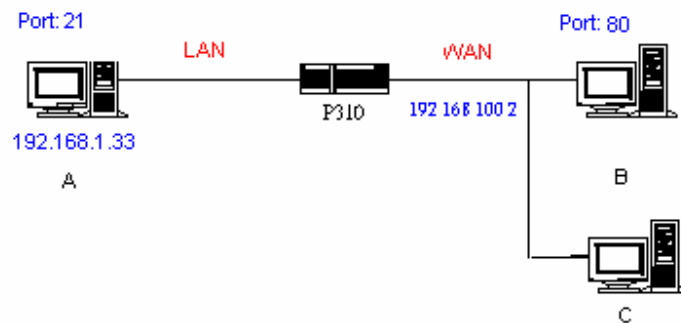
These triggered events can be timed so that they erase the port mapping as soon as they are done with the data transfer, so that the port mapping can be triggered by another Client computer. This gives the *illusion* that multiple computers can use the same port mapping at the same time, but the computers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

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

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

Type	Description	Default mode
0	LAN to WAN	Forward
1	WAN to LAN	Forward
6	IPSec pass through	Forward
7	Trigger dial	Disabled

Example commands:

```
sys filter netbios config 0 on => block LAN to WAN NBT packets  
sys filter netbios config 1 on => block WAN to LAN NBT packets  
sys filter netbios config 6 on => block IPSec NBT packets  
sys filter netbios config 7 off => disable trigger dial
```

Appendix 4 Traffic Redirect/Static Route Application Note

Why traffic redirect/static route be blocked by ZyWALL

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

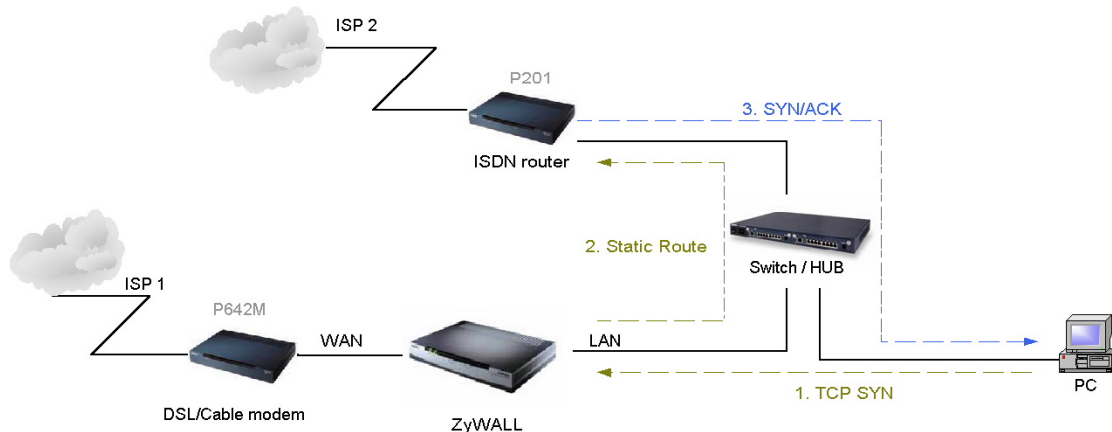


Figure 5-1 Triangle Route

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

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

That causes all of outgoing TCP traffics being reset!

How traffic redirect/static route works under protection - Solutions

(1) Gateway on alias IP network

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

normal function.

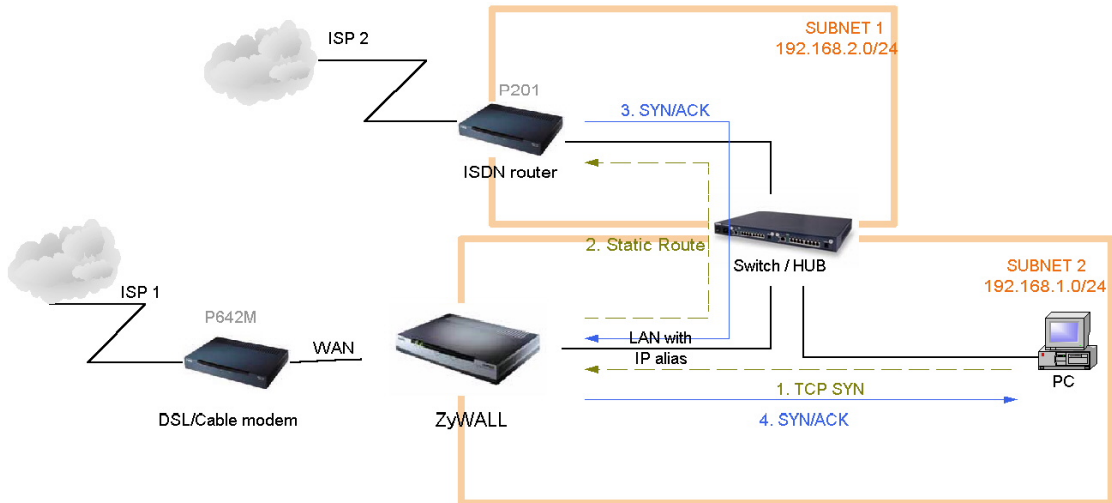


Figure 5-2 Gateway on alias IP network

(2) Gateway on WAN side

A working topology is suggested as below.

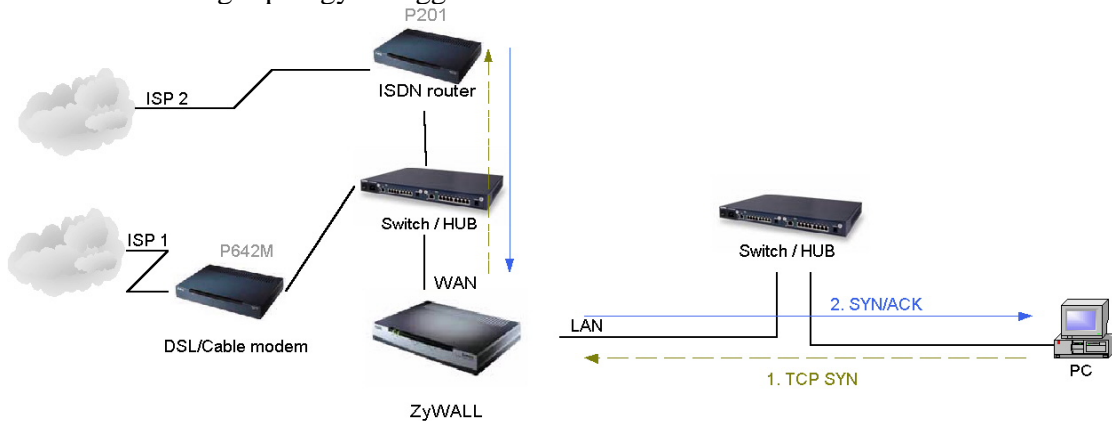


Figure 5-3 Gateway on WAN side

Appendix 5 IPSec FQDN support

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

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

In FQDN design, all three types, IP, DNS, E-Mail, can set ID content. For ID type is DNS or E-mail, the behavior is simple. ZyWALL A and ZyWALL B only checks the ID

contents are consistent and they can connect.

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

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

We can put all combinations in to these two tables:

(Local ID Type is IP):

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

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

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

(Peer ID Type is IP):

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

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

Summary:

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

Appendix 6 Embedded HTTPS proxy server

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

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

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

Appendix 7 Multiple WAN Access

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

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

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

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

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

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

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

Appendix 8 Wi-Fi Protected Access

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

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

Appendix 9 IPsec IP Overlap Support

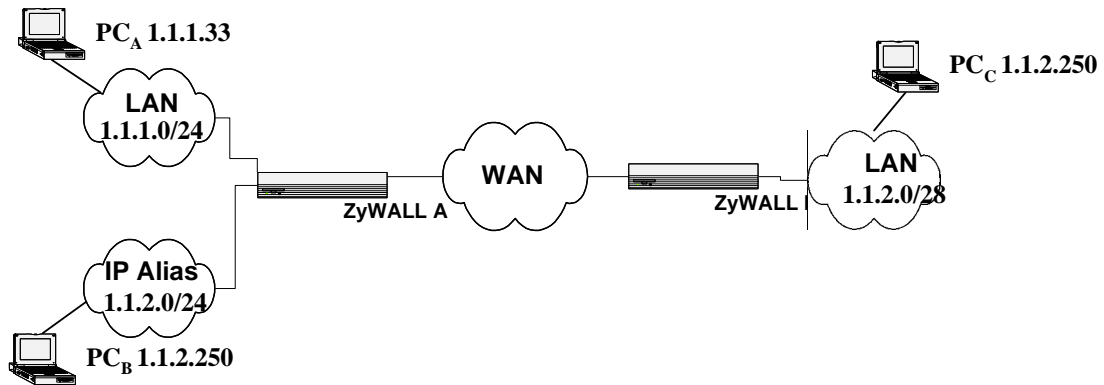


Figure 1

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

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

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

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

(1) Enter “ipsec swSkipOverlapIp off”:

To trigger the tunnel for packets from 1.1.1.33 to 1.1.2.250. If there is traffic from LAN to IP Alias (Like the traffic from PC_A to PC_B in Figure 1), the traffic still will be encrypted as VPN traffic and routed to WAN, you will find their traffic disappears on LAN.

(2) Enter “ipsec swSkipOverlapIp on”:

Not to trigger the tunnel for packets from 1.1.1.33 to 1.1.2.250. Even the tunnel has been built up, the traffic in this overlapped range still cannot be passed.

[Note]

If you configure a rule on the ZyWALL A whose

```
Local IP Address Start= 0.0.0.0
```

```
Remote IP Address Start= 1.1.2.240 End = 1.1.2.254
```

No matter swSkipOverlapIp is on or off, any traffic from any interfaces on the ZyWALL A will match the tunnel. Thus swSkipOverlapIp is not applicable in this case.

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 Client 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 12 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.

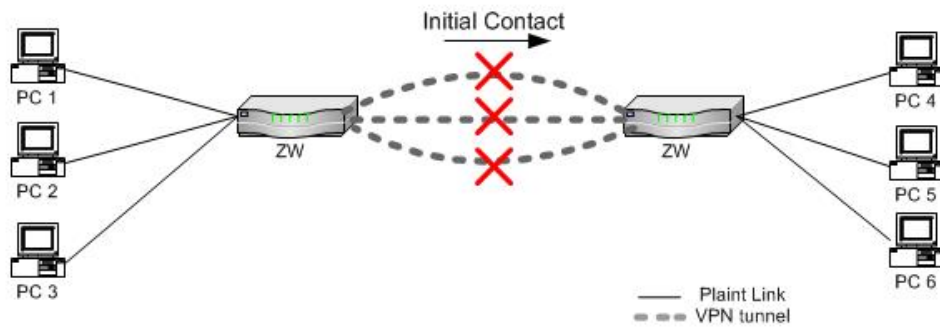
Appendix 13 The mechanism when the ZyWALL receives a IKE packets with IC

[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':

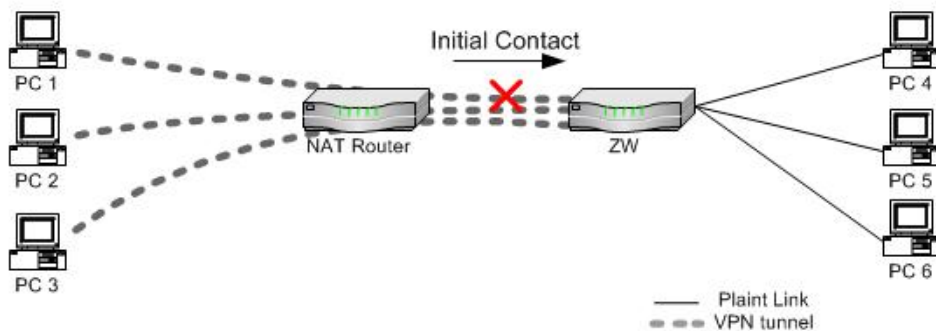
(1)ipsec initContactMode gateway

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.



Appendix 14 The topologies ZyWALL doesn't supported:

Previously, the ZyWALL supports most of SIP topologies except:

- (1) SIP server on the ZyWALL's LAN/DMZ/WLAN.
- (2) Two SIP clients behind the ZyWALL and talk to each other.

Now we have solved these two problems, all directions of SIP calls can work. You can refer to the Figure 1, all of the SIP clients in the picture can register to the SIP server behind the ZyWALL and any two SIP clients can talk to each other.

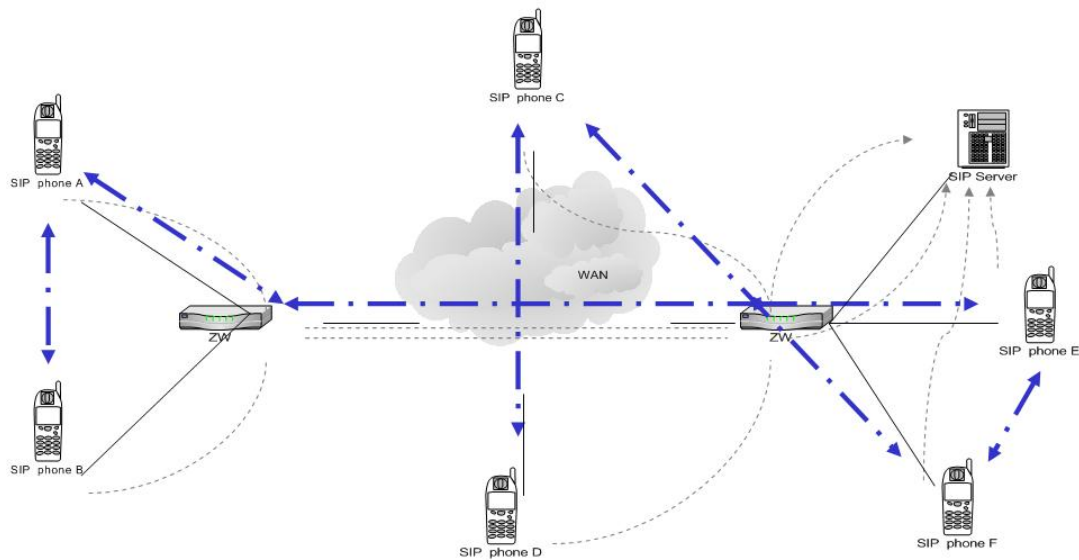


Figure 1.

But there are still some limitations remain that we need to overcome in the future. **When you deploy your SIP server on LAN for SIP service, please make sure that prevent your topology from any case listed as below.**

(1) When SIP client is on LAN, do not use NAT lookback on SIP server.

When there is a SIP server on the LAN, for those SIP clients on WAN, we can set a port forwarding rule or address mapping rule to let them to use WAN IP to access the SIP server behind the ZyWALL, but for those SIP clients which is behind the ZyWALL, please just use the SIP server's LAN IP and **DON'T** use the public IP as their SIP server IP, the ZyWALL doesn't support such a loopback case on SIP registration/proxy server.

For instance, in Figure 2, there is a SIP server on LAN, and there are also two SIP phones E and F on LAN want to talk to each other. Although there is a NAT port forwarding rule for outside SIP clients to use 211.72.158.200 to connect to SIP server, but please let phone E and F use SIP server's LAN IP 192.168.1.200 to connect to SIP server directly.

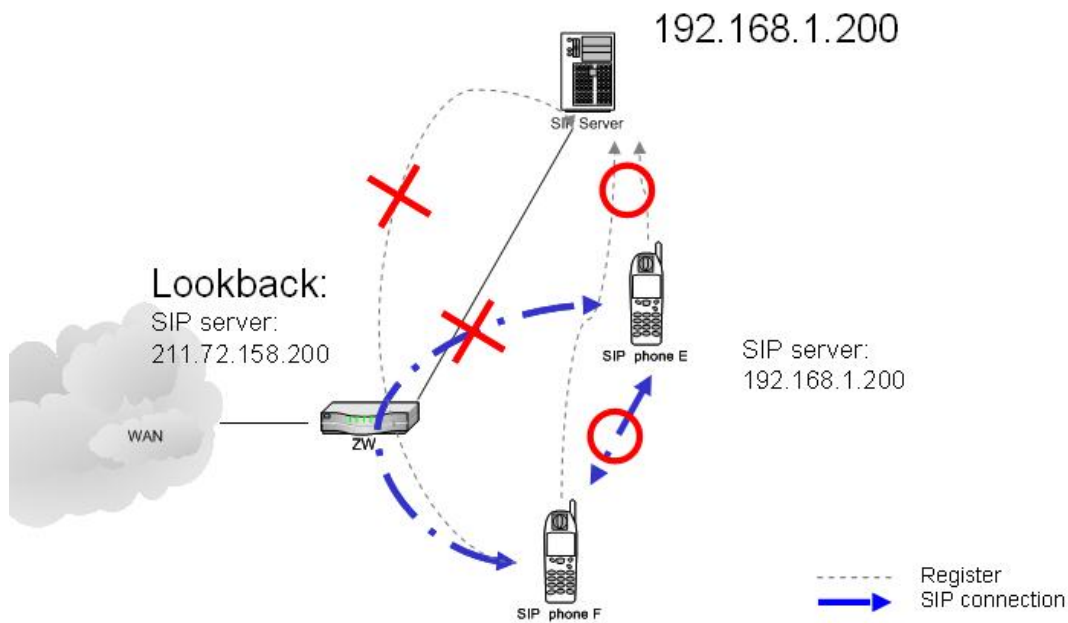


Figure 2.

(2) Try not use different global IPs for SIP client and SIP server on NAT.

Currently, there are still some limitations when use different global IPs for SIP client and SIP server. For instance, in Figure 3, SIP server and a SIP client B are on the same LAN. If we use different global IP for SIP server and the SIP client, the SIP client A which is behind another NAT router will fail to communication with SIP client B.

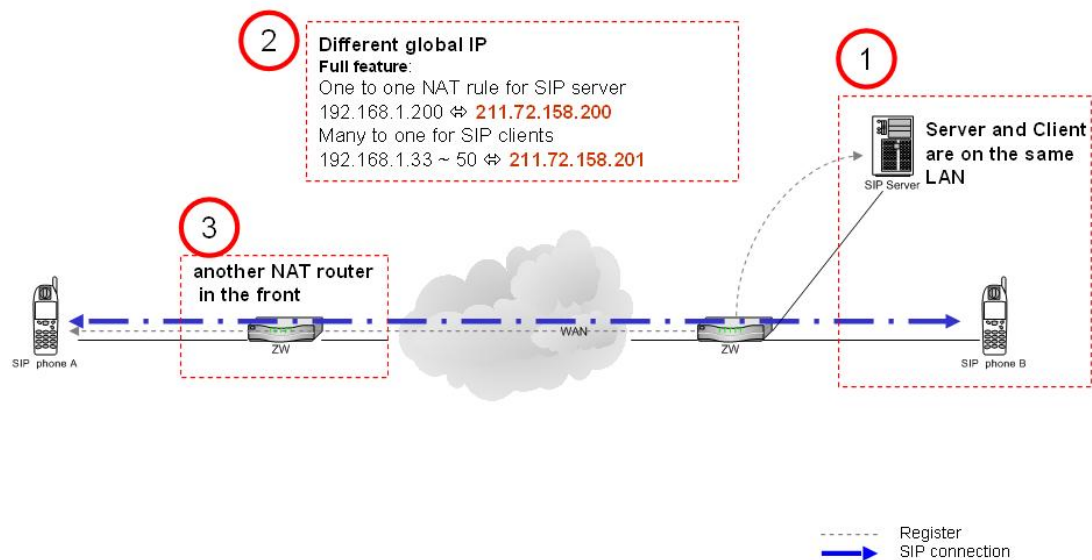


Figure 3.

(3) We do not support that SIP client sends ACK directly to a peer client.

For instance, in Figure 4, when SIP phone A want to send ACK request direct to SIP phone B, because of the limitation, this ACK request will not successfully transmit to SIP

phone B. Thus will be fail on call setup. This limitation is SIP client related issue, some SIP clients will send ACK request direct to the remote clients, some may send through proxy server.

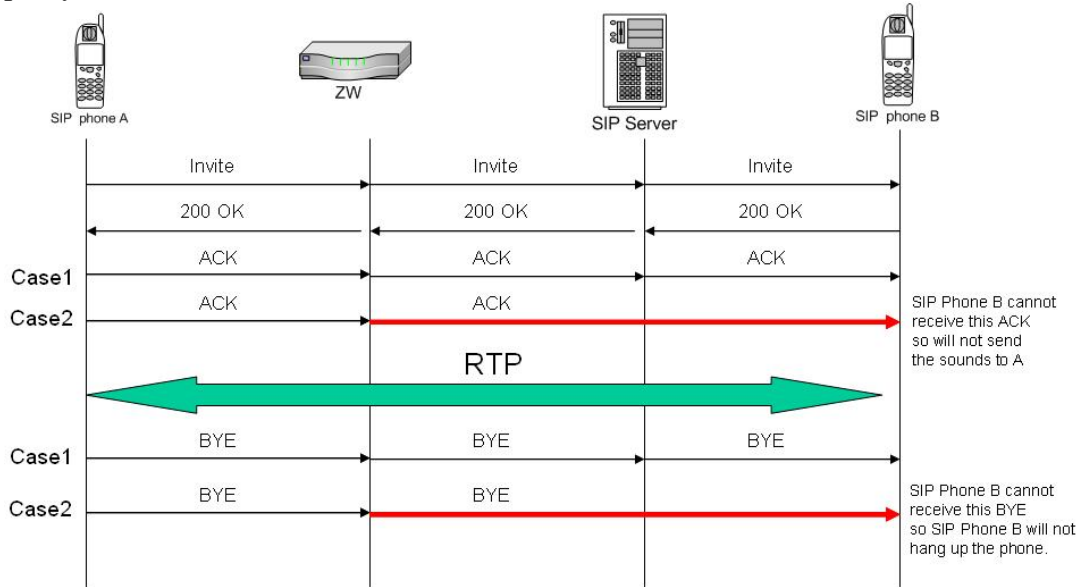


Figure 4.

(4) We do not support multiple SIP proxies in the middle of way.

We haven't implemented or take care on this kind topology (Figure 5), so the result is still unknown.

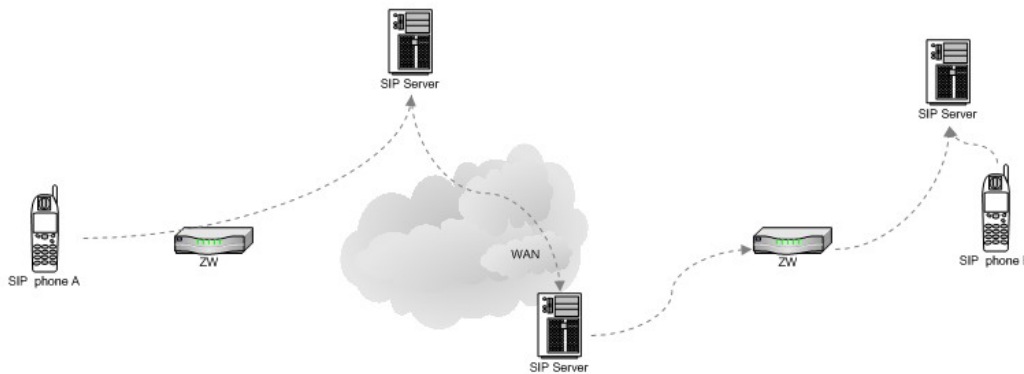
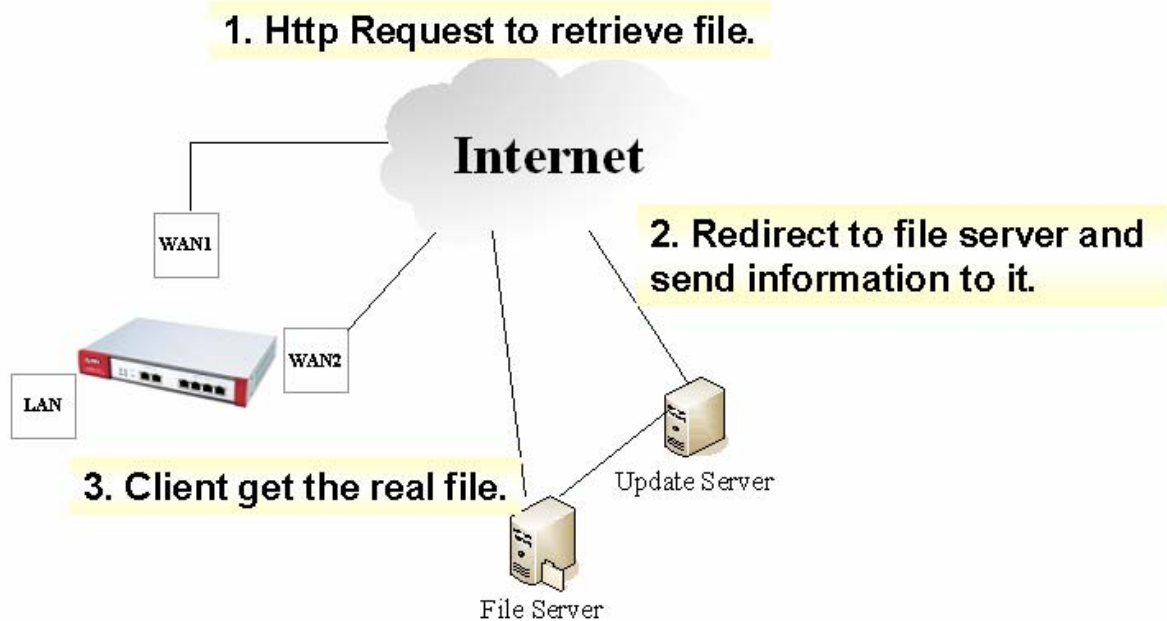


Figure 5

Appendix 15 The mechanism of hose-based load balance feature

- (1) A PC in LAN side wants to download a file from the remote server in the Internet.
- (2) ZyWALL 35 or ZyWALL 70(Multiple WAN product with Load Sharing feature in Active/Active mode)
- (3) PC sends a request to "Update Server" through "WAN1".

- (4) "Update Server" will reply a file list to the PC, the download address of the fill will be "File Server", at the same time "Update Server" will inform that there is a PC located at "WAN1" IP address will get file from you.
- (5) PC knows the file address and retrieve the file through "WAN2".
- (6) "File Sever" think the PC's IP should be "WAN1" instead of "WAN2". It rejects the PC's request.



In this scenario, we should have a mechanism to ensure that the second session should follow the first session's path to avoid this kind of problem.

That's why we add this feature.

How does this feature work?

- (1) PC sends a request to "Update Server" through "WAN1".
- (2) "Update Server" will reply a file list to the PC, the download address of the fill will be "File Server", at the same time "Update Server" will inform that there is a PC located at "WAN1" IP address will get file from you.
- (3) PC knows the file address and want to retrieve the file. ZyWALL finds that the PC already created a session **five seconds ago**, the session went out through "WAN1". It will route this new session by "WAN1".

Five seconds is a key point.

We will have a timeout value.

In this case, if we set the timeout value as "1 seconds". The device **will not** route the new session to the same interface.

If we set the timeout value as "10 seconds", 5 seconds is not timeout. The device **will** route the new session to the same interface.