ZyXEL

Firmware Release Note

ZyWALL 10W

Release 3.62(WH.1)

Date: **Feb 26, 2004**
Author: **Jason Chiang**

s

ZyXEL ZyWALL 10W Standard Version
Release 3.62(WH.1)
Release Note

Date: Feb 26, 2004

Supported Platforms:

ZyXEL ZyWALL10W

Versions:

ZyNOS version: V3.62(WH.1) | 02/26/2004
BootBase : V1.06 | 12/19/2003

Notes:

1. In order to switch connections among default WAN, traffic redirect and dial backup smoothly, we recommend user to activate the traffic redirect function and enter a valid IP address in the "Check WAN IP Address" in Web configuration WAN -> Traffic Redirect page.
2. Because the DNS setting mechanism is changed, the CI command “ip dns order” is obsolete and no longer available. Users can set the DNS setting in menu 3.2 or in web MAIN MENU->LAN->IP page to make the behavior the same as before.
3. The setting of ignore triangle route is on in default ROM FILE. Triangle route network topology has potential security crisis. If you are not clear about it, please refer to Appendix for the triangle route issue.
4. IKE process in phase 2 will check ID information between system and the peer. If you found that the IPSEC connection is failed, please check your settings.
5. Using Web to configure VPN, the phase 1 algorithms have been fixed to DES + MD5. If other algorithms are preferred, please use ADVANCE page to configure them.
6. When firewall turns from “off” to “on”, the firewall initialization procedure will disconnect all connections running through the ZyWALL.
7. Different certificates can’t use same subject name.
8. SUA/NAT address loopback feature was enabled on ZyWALL10W by default, however, if users do not need it, a C/I command “ip nat loopback off” could turn it off.
9. 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.
10. When users upgrade firmware from 3.61 (or 3.60) to 3.62, after system reboots users

have to wait for 60 seconds and do not power off during this period.

11. ZyWALL A ----------NAT Router---------- ZyWALL B
(WAN) (LAN)
ZyWALL A has one VPN rule with NAT traversal on.
ZyWALL B has two rules:
Rule 1 is NAT traversal off, and wrong phase 2 SA parameters.
Rule 2 is NAT traversal on, and other parameters are correct.
When trigger VPN tunnel by ZyWALL A, tunnel will never be up.

Known Issues:

1. Sometimes eWC→time zone page can't be configured under IE 5.00.3315
2. When going inside an empty VPN rule, pre-shared key sometimes has been filled by some values which belong to other rules automatically.
3. eWC→WAN IP has bugs when WAN→ISP is PPPoE or PPTP. Leaving some values in remote IP or remote masks for WAN→IP and then switch to dynamic IP, ZyWALL cannot dial anymore.
4. Sometimes on screen the "Local Area Connection" icon for UPnP disappears. The icon shows again when restarting PC.
5. UPnP problems:
   (1) Sometimes XP can not find router in "My Network Place" after rebooting PC.
   (2) Service items in Internet Gateway→Service can not be saved and is always empty.
6. Symptom: When turning on to many web sites at same time, it may cause content filter fail.
   Condition: When turning on browser to access a lot of websites (for example, 30 sites) at same time may cause content filter fail.
7. If we set system DNS from IPS for first, second and third and then save. Web will set second and third as none, and we can only get 1 DNS from IPS.
8. We can not change dial backup port IP from dynamic to static by telnet.
9. In web MAIN MENU->SYSTEM->General page, the IP addresses of "System DNS Servers" fields are empty when router connects to Internet using dial backup.
10. For DNS server for IPSec,
    (1) set 1 existing ISP DNS on LAN
    (2) create a VPN tunnel rule with DNS server
    (3) OC give DNS from device first is ISP DNS and second is VPN DNS
    (4) When try to access domain on remote LAN, it will fail.
11. In GUI, there are 19 entries in eWC→SUA/NAT→SUA Server. But in SMT there are only 12 entries (including an entry for default server).
12. The certificates generated by the ZyWALL of 3.62(WH.0)b1 and 3.62(WH.0)b2 firmware version may contain a field which is not recognizable to browsers such as MSIE and Netscape. If you select this kind of certificate as the ZyWALL HTTPS server's certificate, your browser might experience problems on

connecting to the ZyWALL HTTPS server. To ensure that the ZyWALL HTTPS server's certificate is recognizable to your browser, please do not use the certificates generated by the ZyWALL prior to this firmware release, instead, generate some new certificates by the upgraded ZyWALL and then select one of them as the HTTPS server's certificate.

13. Sometimes message “!! Un-consistent SA happens!! 1” shows on screen.
14. When VPN tunnel can’t be up, changing rule configuration may causes system reset.
15. Concussion may happen in bandwidth reservation. ZyWALL’s bandwidth management mechanism reserves bandwidth for traffic, and the amount of reserved bandwidth may change by time.
16. When WAN is down, VPN tunnel will be fail with dial backup.

Restore to Factory Defaults Setting Requirement: No

Features:

Modifications in V3.62(WH.1) | 02/26/2004

1. Modify for formal release.

Modifications in V3.62(WH.1)b1 | 02/20/2004

1. [ENHANCEMENT] Add new CI command “ip arp period” to change the ARP lifetime interval.
2. [ENHANCEMENT] Add a new CI command "ip arp force <on|off>". When the user uses "ip arp force on", the age function of APR function will be disabled. That means even the ARP entry has been refered, the timer of it will not reset to 300 seconds, it will be still time out.
3. [BUG FIX] Symptom: System memory leak and eventually causing the reboot.
   Condition:
   (1) Start collecting data in eWC->LOGS->Reports.
   (2) Run for some time.
   (3) System will run out of memory and become very unstable.
4. [BUG FIX] Symptom: Packets will not go through ZyWALL.
   Condition:
   (1) There is heavy traffic through router.
   (2) Sometimes PC A send a DNS query to outside DNS server, but the reply packet will be forwarded to another PC.
5. [BUG FIX] Symptom: Packet can’t be transmitted under Half Duplex mode.
   Condition:
   (1) Connect ZyWALL LAN (or WAN) port to a 10M Hub so that the port will operate in 10M/Half-Duplex mode.

(2) Generate a lot of traffic over the 10M Hub.
(3) Have the ZyWALL LAN (or WAN) port continuously transmit a lot of packets.
(4) After some time, ZyWALL's LAN (or WAN) port may not transmit packets forever.

6. [BUG FIX] Symptom: IPSec XAUTH cannot work with SoftRemote.
   Condition:
   (1) Configure corresponding IPSec rule with XAUTH on SoftRemote and ZyWALL.
   (2) Trigger SoftRemote IPSec rule.
   (3) SoftRemote log shows "no proposal chosen" and connection fails.
7. [BUG FIX] Symptom: IPsec NAT-Traversal can not work.
   Condition:
   (1) Setup NAT-Traversal rule at Initiator and Responder, both sides are Tunnel encapsulation mode.
   (2) Connect from Initiator side.
   (3) Tunnel can not be established.
8. [BUG FIX] Symptom: ICMP packet of NAT loopback will be blocked by Firewall.
   Condition:
   (1) Enable Firewall.
   (2) NAT default server is set to host A.
   (3) Turn on NAT loopback.
   (4) Host A pings router's WAN IP address.
   (5) Host A does not receive echo reply packet and Firewall log shows "Land Attack".

Modifications in V3.62(WH.0) | 12/19/2003

Modify for formal release.

Modifications in V3.62(WH.0)b12 | 12/17/2003

1. [BUG FIX] Symptom: Firewall policy log is not correct.
   Condition: In eWC→LOGS, if the firewall policy is WAN to WAN/ZyWALL, router will show "W to W/P" which should be "W to W/ZW".
2. [BUG FIX] Symptom: Garbage shows on console.
   Condition: There are some firewall dump message shows on screen.

Modifications in V3.62(WH.0)b11 | 12/10/2003

1. [BUG FIX] Symptom: XAUTH doesn't work correctly.
   Condition: When XAUTH is on, even the password is not correct the VPN negotiation will still keep going and won't be stopped.
2. [BUG FIX] Symptom: Bandwidth management doesn't work correctly.

Condition: When there are several firewall rules with total bandwidth exceeds the restricted bandwidth, some firewall rules' bandwidth restriction will disappeared and on these rules bandwidth is unrestricted.

3. [BUG FIX] Symptom: Deleting Firewall rules will cause bandwidth management abnormal.
   Condition:
   (1) Set up several firewall rules with restricted bandwidth.
   (2) Delete all firewall rules.
   (3) Reboot router.
   (4) All setting about bandwidth management will still exist. i.e., the total restricted bandwidth is not zero.
4.

Modifications in V3.62(WH.0)b10 | 12/09/2003

1. [BUG FIX] Symptom: eWC→VPN→SA Monitor: SA status is not correct.
   Condition: In eWC→VPN→SA Monitor, when phase 2 encryption is NULL, eWC→VPN→SA Monitor->IPSec Algorithm shows "ESP ???—SHA1" in which "???" should be "NULL".
2. [BUG FIX] Symptom: Bandwidth management may be wrong when transmitting data.
   Condition:
   (1) Set up a firewall rule with bandwidth management active.
   (2) Transmit data by using the firewall rule mentioned in (1).
   (3) Now set up a new firewall rule with different bandwidth restriction.
   (4) The bandwidth which is used by the firewall rule in (1) will be changed to the new one which is mentioned in (3).
3. [BUG FIX] Symptom: Bandwidth management is not accurate.
   Condition: The real bandwidth restriction is not the same as what users set in Bandwidth management.

Modifications in V3.62(WH.0)b9 | 12/02/2003

1. [BUG FIX] Symptom: System shows debug message on screen.
   Condition: When TLS/TTLS is on, system will show debug message.
2. [BUG FIX] Symptom: VPN stress test will cause system crash.
   Condition: When running stress test with 10 tunnels (PKI and PSK), system will crash.
3. [BUG FIX] Symptom: VPN tunnels can't be up when there are several rules in responder.
   Condition: When there are several rules with PSK and PKI, some of them are with XAUTH, some are not. Rule parameter checking will fail when checking phase 1 authentication method.
4. [BUG FIX] Symptom: System parameter may be wrong after IPSec re-key in dynamic rule.

Condition: When responder is dynamic rule, all VPN parameters will change to wrong number or garbage after re-key.

5. [BUG FIX] Symptom: Content filter can't be registered in dial backup or traffic redirect.
   Condition: In dial backup or traffic redirect mode, we can't register for Cerberian content filter.
6. [BUG FIX] Symptom: Device reboots when WAN is up/down for several times.
   Condition: After up/down WAN for several times in SMT menu 24.1, system will crash.
7. [BUG FIX] Symptom: System may crash or can't login by GUI when traffic is heavy in LAN.
   Condition: When traffic is heavy in LAN, we may not login system or system may crash.
8. [BUG FIX] XAUTH may cause VPN fail.
   Condition:
   (1) Initiator has only one rule with XAUTH on.
   (2) There are several static rules in Responder.
   (3) In Responder, suppose there are some rules that have same phase 1 parameters with the correct rule, and these rules are XAUTH disabled and located in front of the correct rule (for example, rule 3 is the correct rule, and rule rules 1, 2 have the same phase 1 parameters and both of them are XAUTH disabled.
   (4) Dial rule from Initiator, rule 3 (the correct rule) will never be chosen and tunnel establishment will be fail.

Modifications in V3.62(WH.0)b8 | 11/10/2003

1. [BUG FIX] Symptom: VPN tunnel can be up, but data can't transmit.
   Condition: ZyWALL 10 W can set up VPN tunnel with peer, but data can't be transmit through the tunnel.
2. [Bug FIX] Symptom: Modified wording in GUI and SMT.
   Condition: Modify following wording in GUI and SMT:
   (1) eWC→VPN→Rule Edit: Authentication Key is modified as Authentication Method.
   (2) In SMT 27.1.1.1, there are two selections in "Authentication method": Pre-shared Key and Certificate.
   (3) In SMT 27.1.1.1, change "PSK" field name to "Pre-shared Key".
   (4) eWC→Content Filter→Categories: Change "Enable Web Site Categories" to "Enable External Database Content Filtering".
   (5) eWC→Content Filter→Categories: Change "Matched Web Sites" to "Matched Web Pages".
   (6) eWC→Content Filter→Categories: Change "Unrated Web Sites" to "Unrated Web Pages".
3. [BUG FIX] Symptom: VPN tunnel can't be up.
   Condition:
   (1) Set up a VPN tunnel with PKI.

(2) Disconnect the tunnel.
(3) Build the tunnel again.

4. [BUG FIX] Symptom: In console mode, users can only save “MAC Address” related fields in SMT 2.
   Condition: In console mode, users can change “Dial-Backup” related fields in SMT 2, but system should not save them. i. e., when users go to SMT 2 again, dial backup should be non-active.
5. [BUG FIX] Symptom: Bandwidth management doesn’t work.
   Condition: Bandwidth can’t be restricted by bandwidth management.
6. [BUG FIX] Symptom: eWC→VPN→Rule Edit→Local: “Ending IP address / Subnet Mask” should be gray out when Local Address type is Single.
   Condition: eWC→VPN→Rule Edit→Local: “Ending IP address / Subnet Mask” is writable when choosing Local Address Type as Single Address.

Modifications in V3.62(WH.0)b7 | 10/31/2003

1. [ENHANCEMENT] Add HTTPS proxy server support.
2. [ENHANCEMENT] eWC→CONTENT FILTER→Categories, add two new category setup, “Unrated Web Sites” and “When Content Filter Server Is Unavailable”. Users can setup to block/unblock and log/un-log those kind of web access..
3. [BUG FIX] Symptom: When Bandwidth Management is up, system may crash.
   Condition: When bandwidth management is active, and change “WAN port speed”, system will crash.
4. [BUG FIX] Symptom: NAT table is full.
   Condition: NAT sometimes may be full and will cause system crash.

Modifications in V3.62(WH.0)b6 | 10/14/2003

1. [ENHANCEMENT] Add “SSH” login message in Centralized Log.
2. [ENHANCEMENT] Support rule swapping by phase 1 ID (Local ID type / content and Peer ID type / content) in IPSec.
3. [ENHANCEMENT] When restore default ROM file in SMT, system will ask users to reconfirm.
4. [FEATURE CHANGE] Add a new item “CERTIFICATES” in panel, and remove certificate related subjects in VPN rule editing page.
5. [FEATURE CHANGE] Enlarge number of rules in eWC→SUA/NAT→SUA Server to 19.
6. [FEATURE CHANGE] In eWC->CONTENT FILTER->Categories, change the wording of button from "Registration and Reports" to "Register".
7. [BUG FIX] Symptom: In AUX mode router can’t start normally when connect with USR modem in console.
   Condition: When connecting with USR modem by console, router won’t be able to start up in AUX mode.
8. [BUG FIX] Symptom: When client PC is Windows NT 4.0 or Linux, system may

crash.
Condition: When client PC's OS is NT 4.0 or Linux, and request IP from ZyWALL, ZyWALL may crash.

9. [BUG FIX] Symptom: System will treat IPSec rule as dynamic rule when Secure Gateway is an un-resolvable domain name.
   Condition: If Secure Gateway in VPN rule setting page is a domain name and can't be resolved, system will take this rule as dynamic.
10. [BUG FIX] Symptom: After apply in eWC→Firewall→BW Management, system will reboot.
    Condition: When Firewall is on, press apply in eWC→Firewall→BW Management, system will crash even BW management is not active.
11. [BUG FIX] Symptom: NAT hash table may be full after some time.
    Condition: After some time later, NAT table may be full and no traffic can go out.
12. [BUG FIX] Symptom: System may crash during heavy traffic.
    Condition: After several hours in heavy traffic, system will crash.

Modifications in V3.62(WH.0)b5 | 9/16/2003

1. [BUG FIX] Symptom: For eWC WIZARD
   (1) we set WAN IP as dynamic IP
   (2) changing WAN information by wizard
   (3) change WAN dynamic IP to static IP the change DNS server setting the web page will refresh
   (4) The WAN static IP will change to dynamic IP.
2. [BUG FIX] Symptom: For VPN SMT setting, phase 1 ID is not correct.
   Condition:
   (1) Set VPN ID type as IP then save
   (2) Change ID type as DNS → go to menu 27.1.1.1 → back to menu 27.1.1, we will find the ID will be changed to IP.
   (3) If we save the type as IP then try to clear content will fail.
3. [BUG FIX] Symptom: Upload ROM file or RAS fail when console is disconnected.
   Condition: When using GUI to upload ROM file or RAS, and he console is disconnected, system won't restart after ROM file or RAS is uploaded.
4. [BUG FIX] Symptom: When using CI command ip nat iamt with wrong parse, the system will reboot.
5. [BUG FIX] Symptom: eWC→Wireless LAN→MAC Filter doesn't work.
   Condition: System can't block remote by MAC address in eWC→Wireless LAN→MAC Filter.
6. [BUG FIX] Symptom: In SMT, second remote node should be non-active if it is empty.
   Condition: If the second remote node is not configured, it should be non-active in SMT.
7. [BUG FIX] Symptom: In default setting, RR-reserved port 1027 for NAT server disappears.
8. [BUG FIX] Symptom: eWC→Firewall→Edit Rule→ Bandwidth for This Rule behavior is not correct.

Condition: There is error message "Status: The bandwidth exceeds 4195067 Kbps" shows when change value in eWC→Firewall→Edit Rule→ Bandwidth from larger value to smaller value.

9. [BUG FIX] Symptom: eWC→Remote Management→SSH→Server Port should be 22.
10. [BUG FIX] There is pre-shared key related log shows when building a VPN tunnel from X-Auth server.
    Condition: While we build a VPN connection from X-AUTH server then we will get VPN error message as " phase 1 preshared key mismatch"

Modifications in V3.62(WH.0)b4 | 9/01/2003

1. [BUG FIX] Symptom: ZyWALL can not establish IPSec tunnel with other vendor products.
   Condition: When choosing 3DES as encryption algorithm, ZyWALL can't establish tunnel with other vendor products.

Modifications in V3.62(WH.0)b3 | 7/18/2003

1. [BUG FIX] eWC->LOGS->LOG SETTINGS: TCP Reset, PKI and Packet filter should be enabled.
2. [BUG FIX] During establishing VPN connection, sometimes device reboots.
3. [BUG FIX] If we establish VPN with PKI self-signed CA, then connection will be fail.
4. [BUG FIX] We will get error message as "!!ID type mismatch. Local/peer : FQDN/IPV4_SINGLE.".
5. [BUG FIX] When setting SA lifetime less than 180 seconds, the rule still can be saved.
6. [BUG FIX] System may crash without doing anything.
   Condition: System may crash directly after going to RAS.
7. [BUG FIX] Symptom: LOG is not correct in VPN.
   Condition:
   (1) During VPN connection, we will get message in red "IKE negotiation is in process" even connection is successfully.
   (2) We will get wrong LOG message when X-AUTH is on.
8. [BUG FIX] Bandwidth management behavior is not correct.
   Condition:
   (1) If we set 10000k for LAN and WAN, then we can set 10000K for LAN and 10000K for WAN each other.
   (2) While we set the ACL rule and let total bandwidth is more than we allocate, then we will get error message "there is no enough bandwidth to allocate" and rule will be saved and some setting will be changed.
9. [BUG FIX] Symptom: VPN SMT ID behavior is not correct.
   Condition: While we set VPN rule with ID type is DNS or EMAIL, the peer ID

Content will be empty after saving the rule.

10. [BUG FIX] S ymptom: System crash happens.
    Condition: Change VPN setting after VPN tunnel is up, system will reboot.
11. [BUG FIX] Symptom: IKE log is not correct.
    Condition: Sometimes, we will get error message in IKE log "Cannot resolve secure gateway for rule 1" even we use IP as secure gateway address.
12. [BUG FIX] Symptom: IPSec log is not correct.
    Condition: Sometimes we will get error message "Start Phase 2: Quick Mode" in red.
13. [BUG FIX] Symptom: SA doesn't exist after rekey.
    Condition: Sometimes after VPN rekey, phse 2 doesn't exist and phase 2 newsession fail. Then we will find none in SA monitor but data is still in transferring.
14. [BUG FIX] Symptom: System crashes in stress test.
    Condition: Device reboots during VPN stress test with PKI and X-AUTH.
15. [BUG FIX] Static route is not in good behavior.
    Condition: WEB can enter the gateway IP in different subnet.
16. [BUG FIX] Symptom: VPN can be up even with different authentication method.
    Condition: When both sides using different authentication method, the tunnel still can be up.
17. [BUG FIX] Symptom: VPN rule saving mechanism is not correct.
    Condition: While we select AH as phase 2 active protocol, then phase 1 authentication algorithm will be changed to "N/A".
18. [BUG FIX] Symptom: Router reboots when setting VPN rule.
    Condition: In eWC→VPN→RULE SETUP: Set SA lifetime less than 180 second and then save, there will be an error message. If now press "Advance" button, system will crash.
19. [BUG FIX] Symptom: When saving a rule with PKI, system will crash.
    Condition: When activating PKI, go to advanced page, save and go to this page again, system will crash.
20. [BUG FIX] PKI causes system crash.
    Condition: After saving VPN rule in web and if PKI is on, system will crash during the tunnel establishment.
21. [BUG FIX] Symptom: VPN LOG message is not correct.
    Condition: While establishing VPN rule with one side's negotiation mode is aggressive, and the other side is main mode. There will be a log shown "Rule [%d] phase 1 negotiation mode mismatch".

Modifications in V3.62(WH.0)b2 | 7/18/2003

1. [ENHANCEMENT] Add more information in CI command "ipsec disp #rule". If the secure gateway of an IPSec rule is configured as domain name, this command will show both domain and actual IP resolved by system.
2. [ENHANCHMENT] Add new eWC firewall rules storage space utilization status bar in summary page.
   Previous: We used firewall rule numbers to count the usage space, but the rule size is depended on content (like IP pairs and total service numbers). The rule size is

different from rule to rule.
Now: We ignored the counter of firewall rules and just care of the remained size we can use.

3. [ENHANCEMENT] In the past, when My IP Address is configured as 0.0.0.0 in IPSec rule, system will use the WAN's IP address as my IP address during IKE. Now it will use the IP of dial backup as my IP address when the WAN is disconnected. In the case of traffic redirect, it will use LAN IP as my IP address.
4. [FEATURE CHANGE] Do not check protocol and port information during IKE phase 1 negotiation.
5. [FEATURE CHANGE] Remove connectivity monitor starting log.
6. [FEATURE CHANGE] Modify the content filter register mechanism.
7. [FEATURE CHANGE] When Local / Peer ID type is DNS or E-Mail, ID content should not be empty.
   Previous: When Local / Peer ID type is DNS or E-Mail, ID content can be empty.
   Now: When Local or Peer ID type is DNS or E-mail, and if the related ID Content is empty, the rule won't be saved and error message will be shown at the bottom of menu 27.1.1 or eWC->VPN->VPN Rule Edit.
8. [FEATURE CHANGE] Modify the message format of remote management centralized Log as: Remote Management: [TELNET|FTP|WWW|DNS|SNMP|ICMP Ping response] denied
9. [FEATURE CHANGE] In previous design in IKE, responder sends initial contact only when it receives initial contact notify from initiator. Now the responder sends initial contact notify to initiator when first contact with peer.
10. [FEATURE CHANGE] Change the length of phase 1 ID payload during IKE negotiation.
    Previous: local machine builds phase 1 ID with fixed length (The length equals to peer's ID length).
    Now: the local machine builds phase 1 ID with ID's real length.
11. [FEATURE CHANGE] In web page “Firewall->BM Global Setting”, the check boxes for all interfaces are integrated into one.
12. [FEATURE CHANGE] When users insert a firewall rule, the default setting of bandwidth management is none.
13. [BUG FIX] Symptom & Condition: In web MAIN MENU->LAN page, the value "Allow between LAN and WAN" cannot be saved.
14. [BUG FIX] Symptom: After firmware upgrade, the user defined values for DNS server don't work anymore.
    Condition: 1. There existed two user defined DNS servers in 3.60 / 3.61 firmware.
    2. Upgrade firmware to a 3.62(WH.0)b1.
    3. LAN PC gets the DNS server from ISP instead of user defined value set in the previos version.
15. [BUG FIX] Symptom: User cannot set the static route rule in SMT 12.1.
    Condition: 1. Enter SMT 12.1
    2. Set destination IP address as 1.1.1.1, IP subnet mask as 255.255.0.0, and gateway IP address as 1.2.1.1
16. [BUG FIX] Symptom: Policy route can't work without binding any IP policy set.
    Condition: With new integrated DNS menu (SMT3.2), user can't bind the IP

policy rules.

17. [BUG FIX] Symptom & Condition: Policy route only checks the rules in set 1. For eWC, Policy route only checks rules from 1 to 6.
18. [BUG FIX] Symptom: Two IPSec hosts can establish IPSec connection when one uses main mode and the other chooses aggressive mode.
    Condition: When local and peer hosts use different IKE phase1 negotiation mode, they still can establish IPSec connection.
19. [BUG FIX] Symptom: IPSec packets will use ZyWALL's LAN IP as source IP.
    Condition: 1. There is a full feature NAT rule to transferred WAN IP to a LAN IP.
    2. ZyWALL plays as RESPONDER.
    3. IPSec tunnel can be established successfully; however the source IP IPSec packet will become the LAN IP set in full feature NAT rule. As a result, the traffic cannot be transmitted.
20. [BUG FIX] Symptom: Centralized log displays incorrect message in IKE.
    Condition: 1. If XAUTH is enabled; the centralized log displays incorrect message "[Keep Alive]" when sending and receiving XAUTH payloads.
    2. If the initiator and the responder use different exchange mode, the centralized log will display XAUTH client success; if the initiator and the responder use different encryption algorithm, the centralized log will display XAUTH client failed.
21. [BUG FIX] Symptom & Condition: When changing WAN IP address from static to dynamic in web MAIN MENU->WAN->WAN IP page, the default route rule shown in web MAIN MENU->STATIC ROUTE page is not disabled automatically.
22. [BUG FIX] Symptom: Firewall can't block packet with default policy when ACL schedule is enabled.
    Condition: When firewall ACL schedule is enabled, the "BLOCK" action will not take effort. In other words, packets will be transmitted even it should be blocked. The log will show "BLOCK", but the packet will still go through the system.
23. [BUG FIX] Symptom: The filter's set/rule number in centralized log does not match the set/rule number in SMT21.1.
    Condition: 1. Enter SMT menu 21.1 to edit the set 1.
    2. Add two rules in set 1.
    3. Enter SMT menu 11.5 to add the set 1 in output filter set.
    4. Generate the packet to match set 1/ rule 2
    5. The centralized log will display "packet match set 0/ rule 0", not "packet match set 1/ rule 2"
24. [BUG FIX] Symptom & Condition: The router cannot send log via qmail server.
25. [BUG FIX] Symptom: When phase 2 encryption algorithm is AES, SMT 27.2 shows question mark in "IPSec Algorithm".
    Condition: When choose AES as the phase 2 encryption algorithms, after the tunnel is up, SMT 27.2 shows the tunnel's information with question mark in "IPSec Algorithm". For example, if one VPN rule's phase 2 Encryption algorithm is AES, Authentication algorithm is SHA1, after the tunnel is up SMT 27.2 shows " ESP ???-SHA1" in "IPSec Algorithm".
26. [BUG FIX] Symptom & Condition: In web Maintenance->DHCP Table page, the DHCP table is always empty.

27. [BUG FIX] Symptom & Condition: In SMT menu 2->Edit Advanced Setup, when moving cursor in "Call Control" fields, system will show some unknown characters.
28. [BUG FIX] Symptom & Condition: MSN 4.7 file transfer can't work when firewall is enabled.
29. [BUG FIX] Symptom & Condition: While we establish VPN connection, we will find IKE message [HASH][Keep-Alive] in log.
30. [BUG FIX] Symptom & Condition: VPN SA monitor display is not correct while we select encryption as AES. It should be AES-SHA1, not???-SHA1.
31. [BUG FIX] Symptom: SSH telnet / Sftp.
    Condition: 1.While we login router by SSH secure shell, we will get message "dispatch_protocol_ignore: Type 11" in SSH client.
    2. There are many debug messages display in console while login router by SSH telnet or sftp.
    3. There is no message in Log to identify user login by SSH.
32. [BUG FIX] Symptom: The priority for SSH and telnet is not correct.
    Condition: 1. Telnet and login to device
    2. Try to access device by SSH but fail. It should terminate telnet session.
33. [BUG FIX] Symptom: SSH & telnet.
    Condition: 1. login device by SSH first.
    2. try to access device by telnet, all message that should pop on telnet screen will pop on SSH client.
34. [BUG FIX] Symptom: Bandwidth management for LAN to LAN or WAN to WAN.
    Condition: 1. Create new firewall ACL rule with bandwidth management.
    2. Create new firewall ACL rule without BW then first rule will be overwrite.
35. [BUG FIX] Symptom: Firewall setting.
    Condition: 1. We can not change all directions setting in firewall to Block or Forward.
    2. Sometimes, we will get "Status : An Error Was Detected on this page HTML item value : 0"
36. [BUG FIX] Symptom: Bandwidth management in firewall.
    Condition: 1. While create FTP ACL rule with BW, then the BW can not function in this rule.
37. [BUG FIX] Symptom & Condition: Sometimes, we should login device eWC by second time.
38. [BUG FIX] Symptom & Condition: When ZyWALL powers up, the initiation of LAN / WAN / WLAN will take more 10sec then 3.61 then pop "Press ENTER To continue".
39. [BUG FIX] Symptom & Condition: For VPN setting, device will copy "My IP Address" to " Local ID content" and "Secure Gateway Addr" to "Peer ID content.
40. [BUG FIX] Symptom & Condition: To enable syslog and fill in IP address will cause device reboot repeatedly
41. [BUG FIX] Symptom: System reboots.
    Condition: 1. Create firewall ACL rule then change packet direction from LAN to LAN to WAN to LAN.
    2. Select one service to "Selected service" and Apply → reboot.
42. [BUG FIX] Symptom & Condition: While content filter enables, there are many

debug messages popped on console.

Modifications in V3.62(WH.0)b1 | 6/20/2003

4. [ENHANCEMENT] Add new feature: X-Auth as the authentication method in VPN IKE phase.
5. [ENHANCEMENT] Add new feature: PKI supported in VPN..
6. [ENHANCEMENT] Add new feature: WLAN 802.1X TLS/TTLS.
7. [ENHANCEMENT] Add new feature: SSH
8. [ENHANCEMENT] Add new feature: Support new encryption algorithm AES in IPSec..
9. [ENHANCEMENT] Add new feature: Bandwidth Management Lite.
10. [ENHANCEMENT] Add new feature: In content filer, use Cerberian to replace Cybernot.
11. [ENHANCEMENT] Add new feature: DNS Server for IPSec VPN. Please refer to Appendix 7 for detail.
12. [ENHANCEMENT] Add CI command "ip dropIcmp [0|1]"(default value is 0) to setup the device to drop ICMP fragment packets.
13. [ENHANCEMENT] Add two new categories "TCP Reset" and "Packet Filter" in Centralized Log.
14. [ENHANCEMENT] Separate DNS servers into system DNS servers & DNS servers assigned to LAN hosts. The system DNS servers are used by router and the DNS servers assigned to LAN hosts are for LAN hosts. There will be no embedded default DNS server for this design.
15. [ENHANCEMENT] Add CI command "sys upnp reserve [0|1]"(default value is 0) to reserve UPnP NAT rules in flash after system boot up.
16. [ENHANCEMENT] Add UPnP "Ports" page to show the UPnP NAT ports.
17. [ENHANCEMENT] IPSec related logs are enhanced.
    (1) Add success log and error messages in IKE in centralize log .
    (2) Add new IPSec debug log method.
18. [ENHANCEMENT] Add dynamic local and dynamic remote in IKE/IPSec. There are two CI commands, "ipsec config dynamicLocal" and "ipsec config dynamicRemote", to configure these two features.
    (3) When dynamic local turns on, My IP Addr = 0.0.0.0, Local Addr Type = single, Local Addr Start = 0.0.0.0, ZyWALL will use WAN IP as local address.
    (4) When dynamic remote turns on, secure GW = domain name, Remote Addr Type = single, Remote Addr Start = 0.0.0.0, ZyWALL will use IP resolved from peer domain name as remote address.
19. [ENHANCEMENT] Add new category "PKI" in Centralized Log.
20. [ENHANCEMENT] Add Local ID Type, Local ID Content, Remote ID Type, and Remote ID Content check when using RSA signature in IKE.
    (5) When using RSA signature, we can not set Local ID Type and Local ID content from UI. The Local ID Type and Local ID content depends on the certificate we select.
    (6) When using RSA signature, we can set and check Remote ID Type and Remote

ID Content. There are two type added, one is "Subject Name" and the other is "Don't Care". The "Subject Name" measn we will check peer ID content using peer's certificate subject name. And "Don't Care" means that we won't chech peer's ID content when we receive it.

21. [FEATURE CHANGE] eWC->VPN->VPN-IKE: In previous design, system will copy "My IP Address" to "Local ID Content" and copy "Secure Gateway Addr" to "Peer ID Content" when ID type is IP . Now the system won't do it, but users still can change Local & Peer ID Content. In other words, now the FQDN behavior in GUI and SMT are the same.
22. [FEATURE CHANGE] We change maximum Firewall custom port number from 10 to <Plz see below>.
23. [BUG FIX] WAN connection will drop in case of using PPTP for ADSL modem (Alcatel ANT1000, Alcatel SpeedTouch Home and Thomson SpeedTouch 510), especially if there is "high speed" on ADSL (512/256).
24. [BUG FIX] Run ping plotter and it will show lots of packet lost errors.
25. [BUG FIX] Unselect "Remote Management"-->"Security"-->"Do not respond to requests for unauthorized service", the HTTP, TELNET and FTP service on the test web site still shows stealth. Test web site is "http://grc.com/x/ne.dll?bh0bkyd2".
26. [BUG FIX] When user telnets to router from the LAN side and changes the router's LAN IP, the telnet console will hang. And user cannot telnet to router until router timeout.
27. [BUG FIX] When enabling access control in logs->log settings-> send immediate alert-> access control and telnet from WAN, the router will crash.
28. [BUG FIX] FTP can’t work when firewall is enabled.
29. [BUG FIX] Symptom: If user turns on Firewall TCP reset mechanism (via CI command: "sys firewall tcprst"), log shows "Firewall sent TCP packet in response to DoS attack" when Firewall sends TCP RST to the sender. This wording is incorrect and replaces by "Access block, sent TCP RST".
30. [BUG FIX] Symptom: IPSec IV value may set the wrong value for AES support and set the compiler flags for CRYPTIC_1141 and CRYPTIC_1140 in the same time. It will not cause any problem but ICSA certification.
31. [BUG FIX] Symptom: Setting dial backup through eWC, dial backup can’t work. Reason: Some initial values and flags are lost when we store this page.
32. [BUG FIX] Symptom: The router will not an error message while the Timeout is greater than Period in the "Traffic Redirect" web page.
33. [BUG FIX] Symptom: FTP data connection halted because Firewall sent TCP reset to FTP server.
    Condition: Firewall only sent TCP reset to server when peer TCP connection state was out of order. That cause FTP client waited and resent packets until TCP timeout.
34. [BUG FIX] Symptom: Sometimes "Message" field of catalog "Access Control" log is blank.
    Condition: "Message" field of catalog "Access Control" log is blank randomly whatever Firewall enables or disables.
35. [BUG FIX] Symptom: Web connection through traffic redirect is blocked by Firewall.
    Condition: When traffic redirect deploy on LAN IP alias and Firewall bypass triangle route, the TCP connection through traffic redirect is blocked and generate a log "Peer

TCP state out of order, sent TCP RST". If user disables "Bypass Triangle Route", the symptom disappears.

36. [BUG FIX] Symptom: ZyWall detects normal DNS answers of as UDP port scan attacks.
    Condition: When router enables syslog service, the DNS reply packets to syslog server are sometimes detected as UDP port scan.
37. [BUG FIX] Symptom: After firmware upgrade, VPN rules cannot work.
    Condition: After firmware upgraded from 3.50 to 3.52 or 3.60, the VPN rules cannot work anymore. The only solution is to save these rules again.
38. [BUG FIX] Symptom: There will be more than one tunnels showed on SA monitor for one static rule, and this connection is not stable.
    Condition:
    (1) Under a special VPN routing setting:

    A: Rule1: Local / Remote = 192.168.2.0 /192.168.3.0, SG = C
    Rule2: Remote / Local = 192.168.3.0 / 192.168.2.0, SG = B

    (2) Traffic from C to B can be tranmitted by rule 2 and then rule 1.
    (3) But sometimes there will be more than 2 connections built and the connection became unstable.
39. [BUG FIX] Symptom: After phase 2 rekey, dynamic rule cannot pass traffic anymore.
    Condition:
    (7) Set secure gateway of a rule to 0.0.0.0, it becomes a dynamic rule and only can be responder. Trigger the tunnel by inbound request from the peer.
    (8) After the phase 2 rekey, traffic cannot pass this tunnel anymore.
40. [BUG FIX] Symptom: When "keep alive' flag turns on, disconnection in SA monitor didn't work correctly.
    Condition:
    (9) Turn on keep alive flag.
    (10) Use SA monitor to disconnect the tunnel.
    (11) The tunnel will not be disconnected properly. There will be still tunnels showed on SA monitor.
41. [BUG FIX] Symptom: IKE will fail when using RSA signature.
    Condition: IKE will fail in processing ID payload when using RSA signature.
42. [BUG FIX] Symptom: The authentication will always success when using RSA signature.
    Condition: Process peer's certificate and signature will always success.
43. [BUG FIX] Symptom: The DNS server IP address in SMT1 and SMT3.2 is junk.
    Condition:
    (12) Select "User-Defined" and enter "168.95.1.1" then save.
    (13) Select "From ISP" and save.
    (14) Select "User-Defined".
44. [BUG FIX] Symptom: When changing Menu 4 "Encapsulation", the other items do not change immediately.

Condition:
(15) Configure the remote node 2 in the SMT11.
(16) Change the Encapsulation type in the SMT4.
(17) The "Service Type", "My Login", "My Password" will not change immediately.

45. [BUG FIX] Symptom: SMT 27.2 always show one tunnel when there are actually more than one tunnel exist.
    Condition: After one tunnel is up, the SAs in following tunnels are marked as "isReNegotiated".
46. [BUG FIX] Symptom: Enable dial backup and WLAN hangs up our system.
    Condition:
    (18) Enable dial backup and WLAN, and use WLAN to access the dial backup connection, system hanged.
    (19) Enable dial backup and WLAN, and use LAN to access the WLAN, system hanged.

Modifications in V3.61(WH.0)b7 | 06/11/2003

1. [BUG FIX] Symptom: eWC→MAINTENANCE→Restart doesn't work.
   Condition: When press the Restart button in eWC→MAINTENANCE, nothing will happen.
2. [BUG FIX] Symptom: Tunnel will be dropped after phase 1 SA timeout.
   Condition: Set up a dynamic rule in which phase 1 SA life time is shorter than phase 2 SA life time. When the tunnel is up, after phase 1 SA timeout, the tunnel will be dropped, and the traffic will use the old IPSEC SA until it is timeout.
3. [BUG FIX] Symptom: Wireless station can't PING other machines in LAN when activate the Wireless.
   Condition: When the router is up with Wireless inactive, and then activate the WIRELESS, the station can't PING other PCs in LAN.

Modifications in V3.61(WH.0)b6 | 05/30/2003

1. [BUG FIX] Symptom: Firewall log is not correct.
   Condition: When firewall blocks packets from WAN side, log shows "Firewall default policy: UDP (W to W/ P)" which is not correct. The correct log should be "(W to W/ ZW)".
2. [BUG FIX] Symptom: eWC→System→General→Administrator Inactivity Timer is missed.
3. [BUG FIX] Symptom: The default value in eWC→System→General→Domain name should be empty.
   Condition: The default value in eWC→System→General→Domain name was www.zyxel.com.tw. It should be empty.

Modifications in V3.61(WH.0)b5 | 05/26/2003

1. [BUG FIX] Dial backup doesn't work.
   Condition: Dial backup doesn't work when some field is filled up in the second remote node in default ROM file.

Modifications in V3.61(WH.0)b4 | 05/21/2003

1. [BUG FIX] Symptom: Web help pages are not correct.
   Condition: Following web help pages are modified:
   (1) eWC→LAN→IP Alias
   (2) eWC→REMOTE MGNT→DNS
   (3) eWC→REMOTE MGNT→FTP
   (4) eWC→REMOTE MGNT→SNMP
   (5) eWC→REMOTE MGNT→TELNET
   (6) eWC→REMOTE MGNT→WWW
   (7) eWC→SUA/NAT→Address Mapping
   (8) eWC→FIREWALL→RULE CONFIGURATION
   (9) eWC→FIREWALL→SOURCE ADDRESS
   (10) eWC→FIREWALL→Custom Port
   (11) eWC→VPN→Maunal Key
   (12) eWC→CONTENT FILTER→Free
   (13) eWC→CONTENT FILTER→iCard

Modifications in V3.61(WH.0)b3 | 05/19/2003

1. [BUG FIX] Symptom: Telnet console hangs when changing router's LAN IP. Condition: When user telnets to router from the LAN side and changes the router's LAN IP, the telnet console will hang. And user cannot telnet to router until router timeout.
2. [BUG FIX] Symptom: 802.1X is not stable.
   Condition: When router is DHCP server, it will assign IP to station periodically and the WLAN connection up and down for every 5 seconds.
3. [BUG FIX] RADIUS is not stable.
   Condition: In some RADIUS software, our router can not access the RADIUS server. Sometimes router doesn't communicate with RADIUS server.
4. [BUG FIX] Symptom: CNM doesn't work.
5. [BUG FIX] Symptom: After firmware upgrade, VPN rules cannot work.
   Condition: After firmware upgraded from 3.60, the VPN rules cannot work anymore. The only solution is to solve these rules again.
6. [BUG FIX] WAN will drop when using PPTP in ADSL modem.
   Condition: WAN connection will drop in case of using PPTP for ADSL modem (Alcatel ANT1000, Alcatel SpeedTouch Home and Thomson SpeedTouch 510), especially if there is "high speed" on ADSL (512/256).

Modifications in V3.61(WH.0)b2 | 5/08/2003

1. [FEATURE CHANGE] Custom port is expended as 30.
2. [BUG FIX] Symptom: Sometimes "Message" field of catalog "Access Control" log is blank.
   Condition: "Message" field of catalog "Access Control" log is blank randomly whatever Firewall enables or disables.
3. [BUG FIX] Symptom:Dial backup priority should be 15.
   Condition: The default setting of dial backup was 2 which should be 15.
4. [BUG FIX] Symptom: PPPoE will be triggered by port 53.
5. [BUG FIX] Symptom: Add product name in page title
6. [BUG FIX] Symptom:UPnP problem:
   Condition: When UPnP is up:
   (1) Tere is no “Network gateway” in network connection.
   (2) While MSN is up, applications can not run successfully.
7. [BUG FIX] Symptom: Dial backup problem:
   Condition:
   (1) The default setting of AT command initial string is lost
   (2) While we enter dial backup page and do nothing, then we view this page again, We find login name is empty and SUA is off, RIP is active at this time.
   (3) If we change any setting in web dial backup page, then CHAP login to remote will fail. And set the password again, it will work.
8. [BUG FIX] Symptom: Enable both custom DNS will cause system crash.
9. [BUG FIX] Symptom: When dial backup is up, SMT menu 4 won’t change related setting when changing encapsulation.

Modifications in V3.61(WH.0)b1 | 4/03/2003

1. [FEATURE CHANGE] Show the reason of forward/block by content filter feature in the centralized log message.
2. [FEATURE CHANGE] In our previous design, "SA monitor" shows SAs including the old SA. So even the re-negotiated SA will be showed on SA monitor. In this case, after a tunnel re-keyed, there will be two SAs on SA monitor. The new behavior is that SA monitor just shows SA which is "non-negotiated", i.e., SA monitor shows new SA but skips old SA.
3. [FEATURE CHANGE] Extend eWC->WAN SETUP->WAN ISP->User name size from 30 character to 45 characters.
4. [FEATURE CHANGE] [FEATURE CHANGE]Add back the inbound idle timer. When a tunnel has no inbound traffic for a certain period, the tunnel will be dropped.

NOTE:

(1) Please use "ipsec timer chk_input <minute> to configure this timer.
(2) A value "0" means disable this timer.
(3) The default value is "disabled".
(4) The inbound idle timer can work with existed "idle timer". The latter monitors if

atunnel with "only outound traffic but no inbound traffic" for a certain period, and then delete that tunnel.

5. [FEATURE CHANGE] Change the mechanisam of initial contact in reboot detection. (original: tunnel-based, now: machine-based).
   Initiator:
   Initiator sends notify payload of "initial contact" when first contact to peer.
   Responder:
   When Responder receives initial contact flag, it checks all tunnels and delete the one in which peer gateway address is the same with Initiator's IP address.
6. [FEATURE CHANGE] Strengthen port scan capability and support both TCP and UDP port scan attack. We add a port scan number to record the incomplete destination port. The recorded bit is port number mod magic number. When the port scan number is compiled fill to the full, firewall consider that the destination host is under attack!
7. [FEATURE CHANGE] Firewall support Windows Messenger 4.7
8. [FEATURE CHANGE] Centralize Log GUI color define. Block color is normal log messages and red color is alert log messages.
9. [ENHANCEMENT] Check Point UDP port 2746 timeout value enlarge support.
10. [ENHANCEMENT] [ENHANCEMENT]When the remote address range and local address range overlap in a IPSec rule, packets from local to local can skip this rule for checking. For example, a rule: local=> start= 192.168.1.0 mask= 255.255.255.0; remote=> start= 192.168.0.0 mask= 255.255.0.0. Then user can define if a packet from 192.168.1.2 to 192.168.1.3 matches this rule.
11. [ENHANCEMENT] Under anti-probe mode the router will drop the IDENT packet without sending the TCP reject packet back to sender. If enabling the reject IDENT function under antiprobe mode, the router will response a reject message to the sender.
12. [ENHANCEMENT]
    (1) In SMT menu 1.1, change words "Addr" to "Address".
    (2) In SMT menu 27.1.1, change word "Addr" to "Address"
13. [ENHANCEMENT]
    (1) Add product name at page title.
    (2) Title will show "ZyXEL ZyWALL 100 Internet Security Gateway",if product is ZW100.
    (3) If the product is Prestige,title shows "ZyXEL Prestige 324 Broadband Access Router".

[ENHANCEMENT]
(1) The web GUI synchronizes with CI command for ZyReport.
(2) Add some protocols besides TCP and UDP for ZyReport.
(3) Change the measurement from bytes to bytes/Kbytes/Mbytes/Gbytes.

14. [ENHANCEMENT] Add NAT Traversal debug messages.
15. [ENHANCEMENT] Add NAT traversal feature. This feature is suppored only ESP tunnel and ESP transport when key management is IKE.
16. [ENHANCEMENT] Add centralized logs for phase 1 ID (FQDN). When ID check fails during IKE phase 1, LOG will show the incoming ID type and content for reference.

17. [ENHANCEMENT] Add full path + file name check for keyword blocking.
18. [ENHANCEMENT] Add a retype password confirmation mechansim for PPTP and PPPoE setup in smt menu 4 and 11
19. [BUG FIX] In IPSec setup page, when phase 1 ID type is IP and phase 1 ID content is empty, setting can not be saved in smt27.1.1, and the warning message "ID Content Should be IP Format" shows at the bottom of smt27.1.1.
20. [BUG FIX] Symptom: "Enable firewall" check box will be automatically checked.
    Condition:
    (1) Disable firewall check box.
    (2) Disable service blocking.
    (3) Firewall check box will be automatically selected.
21. [BUG FIX] Symptom: Configure through eWC in VPN page can't save the per-shared key.
    Condition: In VPN page with rule setup, the pre-shared key can't be saved.
22. [BUG FIX] Symptom: IPSec CI command display the wrong messages.
    Condition: Using "ipsec disp rule#", the messages are not correct when local/remote address type is range/subnet.
23. [BUG FIX] [BUG FIX]Symptom: When phase 1 ID check failed, IKE log didn't show the ID content correctly.
    Condition:
    (1) Set Peer ID type = IP and leave Peer ID content as blank.
    (2) Set different ID content in the peer site.
    (3) Establish the tunnel. Due to phase 1 ID content is different, the procedure will fail. But in the log, "configured peer ID content" doesn't show correctly.

24. [BUG FIX] Sympton: Even the parameter is correct, negotiation for IKE phase 1 may fail.

Condition: There are two types of conditions.
    (1) When two rules have same secure gateway address, sometimes the second tunnel cannot be established after the first one is built.
    (2) This situation also happens in rekey. If the initiator did not send DEL phase 1 information packet first and then start another phase 1 negotiation directly, this negotiation may fail.
25. [BUG FIX] Symptom: The trusted/untrusty/keyword entry cannot be deleted.
    Condition:
    (1) Add "12345678901234567890123456789012345678901234567890123456789012345678901234567890" to trusted/untrusty/keyword and save.
    (2) Delete this entry.
26. [BUG FIX] Symptom: Accessing www.hotmail.com/tw will cause system crash.
    Condition:
    (1) Enable Block Cookies.
    (2) Accessing website "www.hotmail.com/tw" and cause system crash.
27. [BUG FIX] Symptom & Condition: Alert mail cannot be sent when configuring only the "send alerts to" field and leaving the "send log to" field blank in Logs Setting page.

28. [BUG FIX] Symptom: The custom port is allowed to be deleted even though it is used by other firewall rules.
    Condition: Once it is deleted, the firewall will change to allow Any(TCP) and Any(UDP) and result in a security problem.
29. [BUG FIX] Symptom: When use CI (ip urlfilter category timeOfDay) command to configure the blocking time of content filter, the saved time is different from the input value.
    Condition: When the input time format is not the expected format hh:mm, the system will store wrong value.
30. [BUG FIX] Symptom & Condition: NAT router will create two session entries when building IPSEC tunnel.
31. [BUG FIX] Content filtering does not log information when blocking cookie.
32. [BUG FIX] Symptom&Condition: When setting the NAT address mapping rule and the start IP is greater than the end IP address, the configuration can be saved.
33. [BUG FIX] Symptom&Condition: When deleting a static route rule which its IP address = 0.0.0.0 and netmask = 0.0.0.0, the routing table's default route will be deleted.
34. [BUG FIX] Symptom: Configure the LAN IP on smt menu 3.2, the system doesn't save the configuration.
35. [BUG FIX]Symptom: Change country code will cause system crashes
    Condition:
        (1) Set country code as 219 by CI command "sys country 219".
        (2) Go to menu 3.5 (don't need to change setting).
        (3) Set country code as 233 by the same CI command in 1).
        (4) Go to menu 3.5 again, and system crashes.
36. [BUG FIX] Symptom & Condition: When enabling "Force UnAuthorized" for VPN port in GUI, all packets in all ports (LAN & WAN) will be dropped.
37. [BUG FIX] Symptom: Two IPSec hosts can establish IPSec connection when one uses main mode and the other chooses aggressive mode.
    Condition: When local and peer hosts use different IKE phase1 negotiation mode, they still can establish IPSec connection.
38. [BUG FIX] Protected "rom-0" file,when user no login.
39. [BUG FIX] Symptom: Content filter with keyword blocking and full path enabled will cause system crash.
    Condition:
        (1) Enable content filter.
        (2) Enable keyword blocking
        (3) Use CI command "ip urlfilter customize actionFlag act5 enable" to enable the full path check.
        (4) Connect to a website.
40. [BUG FIX] Symptom: Firewall logs duplicate ICMP type 3 code 3 which reply by itself.
41. [BUG FIX] Symptom: When our router exchange system information through NetBIOS, it may crash.
    Condition: When router send NetBIOS broadcast and found a new name needed to be added. The name list inital with NULL will cause adder function crash our ZyWALL.

42. [BUG FIX] Symptom: LAN LED light on, when setup the WAN.
    Condition: For the ZyWALL with ATAN8995L, using the eWC to setup WAN or using SMT 2 to setup the WAN's mac address. All ethernet LEDs will light on.
43. [BUG FIX] Symptom: ICMP packet with identifier zero will be droped by router.
    Condition: Send a ICMP ping packet with its identifier zero.
44. [BUG FIX] Symptom: Send email log will cause system to hang about 30 seconds.
    Condition:
    (1) Email server address is written in domain name.
    (2) The WAN network link can not connect to Internet when applying email log setting.
45. [BUG FIX] Symptom & Condition: During IKE phase 1 negotiation, if ZyWALL receives a Notify DEL payload, it may crash.
46. [BUG FIX] Symptom: The parsing string for keyword blocking is junk.
    Condition:
    (1) Use CI command "ip urlfilter customize actionFlag act5 enable" to enable the full path check.
    (2) Use browser to access the Internet.
47. [BUG FIX] Symptom: UPnP can't save Internet Gateway Services.
    Condition: When we add service in the Internet Gateway, the service can't be saved into the router.
48. [BUG FIX] Symptom: The keyword blocking does not work.
    Condition:
    (1) Use CI command "ip urlfilter customize actionFlag act5 enable" to enable the full path check.
    (2) Use browser to access the URL that set in the keyword blocking, the packets will be still allowed to pass.
49. [BUG FIX] Symptom: The static route rule can not be added into the static route table.
    Condition:
    (1) The WAN IP is dhcp client (dynamic IP address).
    (2) Use SMT menu 12 to add a static route rule. For example, dest IP= 192.168.111.0, mask=255.255.255.0, gw=172.21.3.1 which this gateway is the same domain as WAN IP address.
    (3) Use "ip route status" to see this static route rule is added into the table.
    (4) Reboot the router and show the table again to see whether the static route rule is added or not.
50. [BUG FIX] Symptom: Content filtering will block keyword that contains *.html.
51. [BUG FIX] Symptom & condition: FQDN: When ID type is IP, VPN tunnel can not established if passing through another router with NAT.
52. [BUG FIX] Symptom: The router will block the trusted domain URL.
    Condition:
    (1) Enable filter list customization & disable all web traffic except for trusted domains.
    (2) Add mypathways.deere.com in the trusted domain and go to this URL.
    (3) Login the page.
53. [BUG FIX] Symptom: Content filter will block the web site that matches the trusted

domain setting.
Condition: When a web site is both in the cybernot filter list and the trusted domain list, the content filter will block the web site.

54. [BUG FIX] Symptom: Add or delete or refresh static route rule on SMT menu12 sometimes cause ZyWALL crash.
    Condition: Sometimes our action on menu12 with static route rule setup will cause ZyWALL crash.
55. [BUG FIX] Symptom & Condition: If user didn't load ipsec rule first before executing IPSec configuration CI command, "ipsec config netbios active <yes|no>" or " ipsec config netbios group <…>", ZyWALL will crash.
56. [BUG FIX] Symptom: If firewall turns on, traffic redirect can not switch back the original Internet connection.
    Condition: This problem only happens when the traffic redirect gateway is not on WAN. If the default Internet connection fails, router will switch routing to traffic redirect gateway. When firewall turns on and the original connection recovers, the routing can not switch back.
57. [BUG FIX] Symptiom: When "ipsec switch" is off, "ipsec dial" still works.
    Condition: If user uses command "ipsec switch off" to turn off IPSec, "dial" still works.
58. [BUG FIX] Symptom: "Don't block Java/ActiveX/Cookies/Web Proxy to Trusted Domain sites" sometimes cannot work.
    Condition:
    (1) Enable Filter List Customization.
    (2) Enable "Don't block Java/ActiveX/Cookies/Web Proxy to Trusted Domain sites".
    (3) Add "dob.tnc.edu.tw" to trusted domain list
    (4) Connect to dob.tnc.edu.tw and choose one ActiveX example.
    (5) The example that contains ActiveX components should not be blocked by router but it still be blocked.
59. [BUG FIX] Symptom: Receving hotmail mail will cause system crash.
    Condition:
    (1) Enable Block Cookies.
    (2) Receiving hotmail mail and cause system crash.
60. [BUG FIX] Wording change for firewall log messages. Since our firewall log messages are logged packet direction with set number. This is hard to remember. So, we change the set number to a short message. For example: "set:1" will be "L to W" means packet from LAN to WAN. "set:9" will be "D to D/ZW" means packet from DMZ to DMZ/ZyWALL.
    Following is the reference table:
    set:1 -> L to W
    set:2 -> W to L
    set:3 -> D to L
    set:4 -> D to W
    set:5 -> W to D
    set:6 -> L to D
    set:7 -> L to L/ZW

set:8 -> W to W/ZW
set:9 -> D to D/ZW

61. [BUG FIX] Symptom: The PPPOE or PPTP address can be set within the range of LAN subnet.
    Condition: When using smt menu 4 or 11, choose the pppoe or pptp encapsulation, set the IP address

Modifications in V3.60(WH.2) | 3/31/2003

1. [BUG FIX] Symptom: eWC→WAN→Route: "Priorily" should be "Priority".

Modifications in V3.60(WH.2)b5 | 3/27/2003

1. [BUG FIX] Symptom: IPSec rekey procedure is not stable.
   Condition:
   (1) There exists an IPSec rule, it's Secure gateway address is domain name. And the phase 2 PFS is on, either DH1 or DH2.
   (2) Sometimes the IPSec rekey procedure will not work properly.
   (3) From the log, user will see ZyWALL only receives IKE packets but never responses.
2. [BUG FIX] Symptom: Old SA won't be deleted.
   Condition: When SA is renegotiated, it won't be deleted after one minute.

Modifications in V3.60(WH.2)b4 | 3/21/2003

1. [BUG FIX] Symptom: When VPN tunnel is up, and SMT→27.1.1.1→PHS is on (DH 1 or DH 2), users can not PING. through tunnel to peer.

Modifications in V3.60(WH.2)b3 | 3/20/2003

1. [BUG FIX] Sympton: Even the parameter is correct, negotiation for IKE phase 1 may fail.
   Condition: There are two types of conditions. 1) When two rules have same secure gateway address, sometimes the second tunnel cannot be established after the first one is built. 2) This situation also happens in rekey. If the initiator did not send DEL phase 1 information packet first and then start another phase 1 negotiation directly, this negotiation may fail.
2. [BUG FIX]Symptom: Sometimes IPSec rekey procedure failed.
   Condition: Under heavy traffic, sometimes IPSec rekey failed.
3. [BUG FIX]Symptom: VPN tunnel can not be established in aggressive mode.
4. [BUG FIX]Symptom: TELIA login problem:
   (3) In SMT, hint is not correct.

(4) The length of login name is inconsistent in SMT and GUI.
(5) In eWC, login server can input IP address.
(6) In SMT and eWC, users can set up WAN IP as static IP address which is not allowed.

Modifications in V3.60(WH.2)b2 | 3/18/2003

1. [BUG FIX] When user types the illegal value of the Telia server and relogin time, it will cause system reboot.

Modifications in V3.60(WH.2)b1 | 3/14/2003

1. [ENHANCEMENT] Support hexadecimal format of pre-shared key. Now pre-shared key starting with "0x" or "0X" will be treated as hexadecimal format.
2. [ENHANCEMENT] Support Telia login
3. [BUG FIX] Web URL can accept control characters <>.
4. [BUG FIX] User can download rom-0 through eWC without permission.

Modifications in V3.60(WH.1) | 3/14/2003

Modifications in V3.60(WH.1)b1 | 2/26/2003

1. [BUG FIX] Fix a security issue of web.
2. [BUG FIX] Symptom: VPN tunnel can not be established if ZyWALL sets phase 1 ID type as IP and wants to negotiate with another side by passing through a router with NAT.
   Condition: Take the figure below as the example:

   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 and will set secure gateway as C. In our implementation system will set peer ID content as secure gateway address if peer ID type is IP. So A's peer ID content is C's WAN IP if A's peer ID type is IP. In this case, A and B will never negotiate successfully. Now user can specify the ID content when ID type is IP. So user can set A's peer ID content as B's WAN IP and they can build tunnel successfully. For more detail, please refer to appendix 6.

Modifications in V3.60(WH.0) | 11/29/2002

1. [ENHANCEMENT] Add CI command for display categories. Now "sys logs disp CATEGORY" can show logs according to the CATEGORY field.
2. [ENHANCEMENT] Add new log category "ike" and four alerts: "access control", "block java etc", "ipsec", and "ike".
3. [ENHANCEMENT] The subject of email for the logs can be configure by CI command "sys logs mail subject.
4. [ENHANCEMENT] Add 802.1X access control on WLAN.
5. [ENHANCEMENT] Add more ID supported in IKE phase 1 authentication. Now ZyWALL10W supports ID-IP, ID-FQDN, ID-USER-FQDN.
6. [FEATURE CHANGE] In VPN configuration, local IP start field can accept 0.0.0.0.
7. [FEATURE CHANGE] The log of remote management is moved from error log to centralized log. Its category is "Access Control".
8. [FEATURE CHANGE] When WLAN is disable, the WLAN LED will be off.
9. [FEATURE CHANGE] Accept space character for ESSID in WLAN configuration.
10. [FEATURE CHANGE] The format of SYSLOG is changed. Source IP and destination IP are added.
11. [FEATURE CHANGE] After sending E-mail, the log will still remain.
12. [FEATURE CHANGE] Add a new CI command "clear" to clear a NAT entry. For example, "ip nat server edit 2 clear" can clear rule NAT rule number 2.
13. [FEATURE CHANGE] Add range check for Many-One-to-One. The number of local IP should be the same with Global IP.
14. [FEATURE CHANGE] In WLAN Setup, add feature to enable/disable WLAN.
15. [FEATURE CHANGE] Sometimes user will get some default policy log without set, because other processes like NAT drop these packets or bypass firewall. We replace the default policy description with its actual reason in centralize log.
16. [FEATURE CHANGE] Syslog adds source / destination IP address field.
17. [FEATURE CHANGE] Change the behavior of FQDN when ID type is DNS. Now ID and Address fields are independent.
18. [BUG FIX] After 34 item of email log will be garbage.
19. [BUG FIX] Fix a security issue related with port scan.
20. [BUG FIX] Fix a security issue related with smurf attack.
21. [BUG FIX] Symptom: System is not stable when domain names of mail server or syslog server are un-resolvable.
    Condition: When users set up mail server or syslog server address with domain name and then save the setting, system halts if that address is an illegal or un-resolvable domain name at that time when sending mail or syslog.
    [Note] Please refer to Appendix 5 for detail.
22. [BUG FIX] Symptom: System halts when both firewall and syslog turn on.
    Condition: When syslog server daemon stops or syslog server host does not exist, the syslog packets explode and firewall generates masses of ICMP packet logs. As a result, system hangs.
23. [BUG FIX] Symptom: Checkbox in eWC→UPnP is not correct.
    Condition: In eWC→UPnP, if selecting "Allow UPnP to pass through Firewall" checkbox and apply, then go to other page and return to eWC→UPnP again, the "Allow UPnP to pass through Firewall" checkbox is still unselected.

24. [BUG FIX] Symptom: When a PC traces route from LAN to WAN, ZyWALL is not visible in the tracing path with firewall on.
    Condition: Firewall blocks the time exceed ICMP packet and log message is "Unsupported/out-of-order ICMP".
25. [BUG FIX] Symptom: The content of web forward log message is junk.
    Condition: If user blocks the keyword "kimo" and access the web site that does not contain the keyword "kimo", the system will generate web forward log message.
27. [BUG FIX] Symptom: eWC→VPN→VPN configuration error message.
    Condition: While access eWC→VPN→"VPN Configuration", and then press "Go back" button, nothing happens and it shows "Please wait…" on "Status".
28. [BUG FIX] Symptom: Traffic redirect can not be set
    Condition: Can not set traffic redirect in SMT and will get message "Status =-121303 Duplicate IP address to other node's IP address" when saving rule in SMT 11.1.
29. [BUG FIX] Symptom: Can not change metrics in eWC→WAN→Route
    Condition: When press "Apply" in eWC→WAN→Route, nothing will be saved and message" Status =-121303 Duplicate IP address to other node's IP address" shows on SMT.
29 [BUG FIX] Symptom: System hangs when turning on/off Internet Gateway several times
    Condition: When UPnP is on, system will hang while turning on/off Internet Gateway several times.
30 [BUG FIX] Symptom: WLAN LED flickers when WLAN is non-active.
    Condition: WLAN LED flickers when WLAN card is inserted into router and not active.
31 [BUG FIX] Symptom: While access http://www.gamespy.com/articles/ and http://groups.yahoo.com system will crash.
    Condition: System crashes when access http://www.gamespy.com/articles/ or when survey/read the forums via http://groups.yahoo.com.
32 [BUG FIX] Symptom: The system will allow the packet with DF=1 and packet length > MTU to pass through the router without any error message returned to the sender.
    Condition: When the packet with its length larger than MTU but DF bit set, it is still allowed to pass through the router.
33 [BUG FIX] Symptom: Conflict check between multi-NAT configuration and VPN is not correct.
    Condition: When VPN local IP address is SUBNET, the conflict check with multi-NAT will reply incorrect result.
34 [BUG FIX] Symptom: VPN web page configuration is not correct.
    (1) If Edit VPN configuration choose "manual key", then it cannot be save. The error message "Manual My ID only can be IP" will be displayed.
    (2) If Edit VPN configuration choose "manual key", and ESP encryption algorithm choose "NULL", then press Apply. Edit the rule again, the authentication key cannot input anymore.
35. [BUG FIX] Symptom: SYSLOG entries truncated.
    Condition: When the entry length is larger than 64 bytes, it will be truncated.
36. [BUG FIX] Symptom: Telnet session issue when firmware uploaded.
    Condition: After firmware uploaded, system will reboot. However ZyWALL will not

disconnect the telnet session connecting to it. As a result, users have to disconnect the telnet session manually.

37. [BUG FIX] Symptom: UPnP sometimes cannot work. After ZyWALL's LAN IP is changed, sometimes PC with XP can not find ZyWALL
    Condition: After restoring default rom file and then change ZyWALL's LAN IP, PC with Windows XP can not find the router.
38. [BUG FIX] Symptom: eWC→SUA/NAT Address Mapping: rule can not be saved.
    Condition: When a rule is configured as type Many-to-one, it cannot be saved. Status will show: "IGA and ILA range does not match".
39. [BUG FIX] Symptom: High latency in PING across ZW 10 W.
    Condition: Under SUA, the latency of PING packets enlarges 30~40ms when they pass through ZyWALL10W.
40. [BUG FIX] Symptom: eWC bugs of WAN / LAN / SYSTEM / WIZARD.
    Conditions:
    (1) WAN IP: When changing WAN IP from static to dynamic, Gateway IP Address will be "0.0.0.0
    (2) Password: When entering wrong "Old Password ", the "Status" will show unreadable messages.
    (3) LAN→IP: The ZyWALL 10W will put the "IP Pool Starting Address" to "Primary DNS Server" and "Secondary DNS Server" field, if keep these two fields empty.
    (4) SYSTEM→TIME ZONE→"Maxico city" should be "Mexico city".
    (5) WIZARD: The example, "my_domain.com", is not correct because "_" is not valid in domain name.
    (6) eWC→WAN→Traffic redirect: The metric field cannot save correct value.
41. [BUG FIX] Symptom: eWC→Firewall bugs.
    Conditions:
    (1) WAN IP: When changing WAN IP from static to dynamic, Gateway IP Address will be "0.0.0.0
    (2) When configuring rules, modify "active" option and then change the protocol fields, the screen will refresh and then the active option status does not keep.
    (3) After configuring 10 rules, there will be a "go to rule" button. But the format is wrong.
    (4) The tags of summary and attack alert are too large.
    (5) When editing IP, the start IP can be larger than end IP, which is not correct.
    (6) Set more than 8 firewall rules in any direction, and then delete rules from bottom to top, somehow all exist rules will be empty.
    (7) Cannot insert rules more than 19.
    (8) When inserting a new rule for firewall between existing rules, and then cancel editing this rule, the sorting of other rules is incorrect.
42. [BUG FIX] Symptom: eWC→LOGS bugs.
    Conditions:
    (1) eWC→LOGS: If the user doesn't input email address in "Send alerts to:" then the ZyWALL won't send log mail.
    (2) Items in "Log" or "Send immediate alert" can be changed only once. After

applying, furthermore modification will not take changes. Only selecting other pages and com back can configure it again.

(3) When sorting by time, the order is not correct when multiple entries recorded within one seconds.

43. [BUG FIX] Symptom: Blocking time status is not correct for "ip url category disp".
    Condition: The blocking time format should be "hh:mm", but through the CI command it will show only integers.
44. [BUG FIX] Symptom: Xbox Live can't work through router.
    Condition: Xbox Live can not work through ZyWALL 10 W.
45. [BUG FIX] Symptom: ZyWALL10W can not block JAVA & Active-X components.
    Condition: When connecting to web site that has JAVA & Active-X components, the router can not block them by content filter.
46. [BUG FIX] Symptom: The content of the 128th email log is junk.
    Condition: The content of email log will be incorrect if each log is large.
47. [BUG FIX] Symptom: The system crashes when establishing IPSec connection.
    Condition: When local and peer machine use different phase 1 authentication algorithms in IKE, both systems crash.
48. [BUG FIX] Symptom: WAN side PC can ping ZyWALL's LAN IP
    Condition: When "SUA only" and "firewall off", outside PC can ping ZyWALL's LAN IP.
49. [BUG FIX] Symptom: The isolated DNS proxy server behinds firewall can not work.
    Condition: When the second or proxy DNS server behinds firewall and try to connect with public DNS server, the TCP 3-ways handshake fails.
50. [BUG FIX] Symptom: eWC→VPN-IKE: Sometimes "Secure Gateway Addr" is empty after saving the VPN rule.
    Condition: After saving one VPN rule at eWC, the secure gateway address disappears and tunnel can never be built.
51. [BUG FIX] Symptom: UPnP doesn't work
    Condition: Even the eWC showed UPnP in b4, it doesn't work.
52. [BUG FIX] Symptom: System reboots when transferring data on wireless and change wireless setting at same time.
    Condition: With Intersil 2.5/3.0 cards inserted, while data is transferring on wireless, changing wireless setting will cause router to reboot.
53. [BUG FIX] Symptom: eWC→ Wireless: while we select Radius, then wireless can not be select again.
    Condition: When click Radius tab from Wireless web, Wireless hyperlink disappeared.
54. [BUG FIX] Symptom: Wireless RADIUS issues:
    Condition:
    (1) Without WEP key: while 2nd time the same user login router again, authentication will be ignored and he can login directly.
    (2) With WEP key is used, users can not login.
55. [BUG FIX] Symptom: System reboots when running "sys log disp".
    Condition: With console port speed set to 9600, dump too much characters will reboot the system.
56. [BUG FIX] Symptom: FQDN doesn't work correctly when setting rule by web

Condition: When setting ID type as IP in web, corresponding content is always empty, and tunnel will never be built.

57. [BUG FIX] Symptom: Router learns illegal ARP packet.
    Condition: Router learns IP MAC addresses from wrong interface. For example, router may learn LAN IP Mac address from WAN. It causes some hosts can not connect to the router.
58. [BUG FIX] Symptom: When using Intersil 2.5/3.0 cards in ZyWALL10W, system may crash.
    Condition: During transmitting, save configuration in SMT will cause system to crash.
59. [BUG FIX] Symptom: Wireless Web error with RADIUS tag.

Condition: In eWC→ WIRELESSLAN, while we select Radius, then wireless can not be selected again.

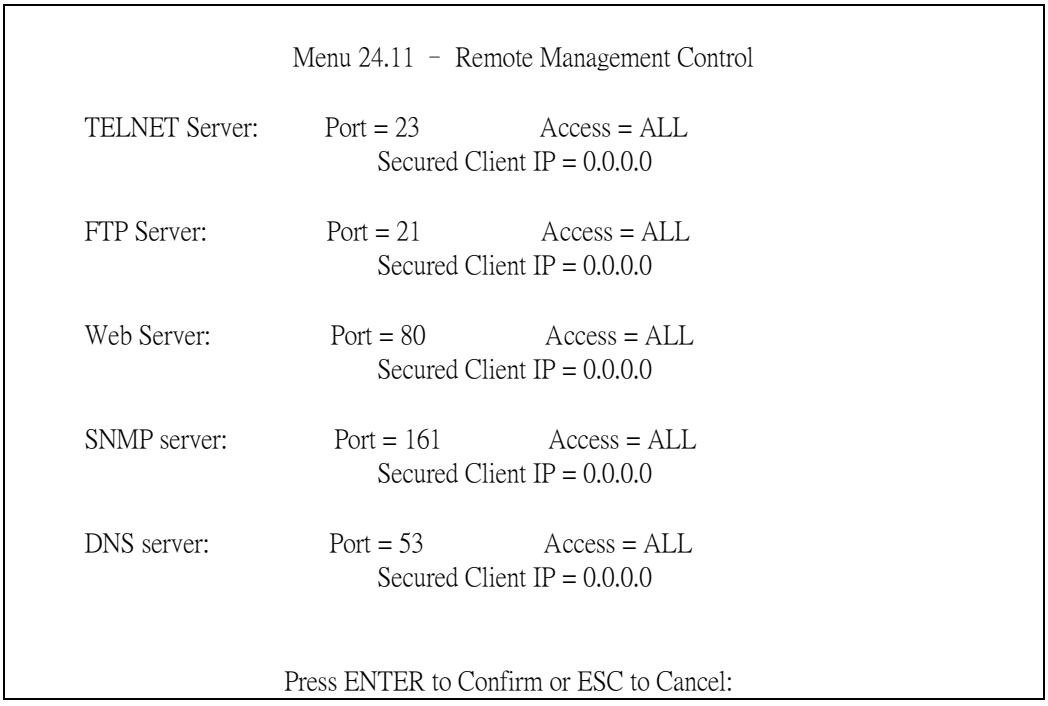
Appendix 1 Remote Management Enhancement (Add SNMP & DNS Control)

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.

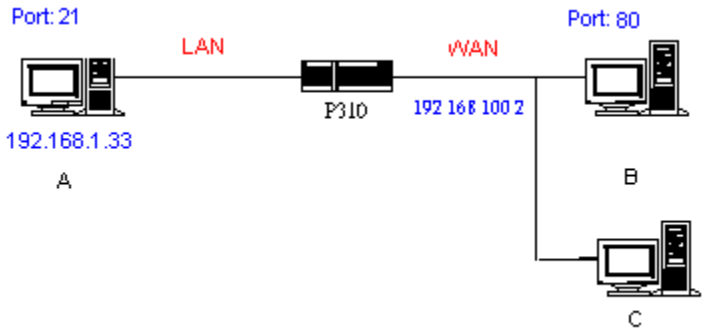
These triggered events can be timed so that they erase the port mapping as soon as they are done with the data transfer, so that the port mapping can be triggered by another Client computer. This gives the ***illusion*** that multiple computers can use the same port mapping at the same time, but the 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 "LAN to WAN" and "WAN to LAN" are "Block", "IPSec Packets" is "Forward" and trigger dial is "Disabled".

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

Example ouput:

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

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

Current filter types and their description are:

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

Example commands:
sys filter netbios config 0 on => block LAN to WAN NBT packets
sys filter netbios config 1 on => block WAN to LAN NBT packets
sys filter netbios config 6 on => block IPSec NBT packets
sys filter netbios config 7 off => disable trigger dail

Appendix 4 Traffic Redirect/Static Route Application Note

Why traffic redirect/static route be blocked by ZyWALL

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

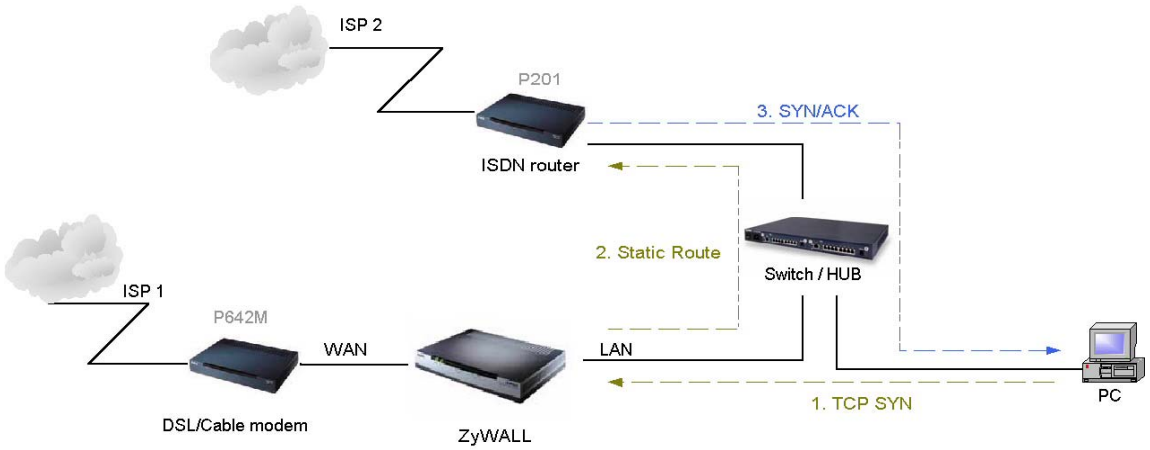


Figure 5-1 Triangle Route

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

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

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

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

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

That causes all of outgoing TCP traffics being reset!

How traffic redirect/static route works under protection – Solutions

(1) Gateway on alias IP network

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

normal function.

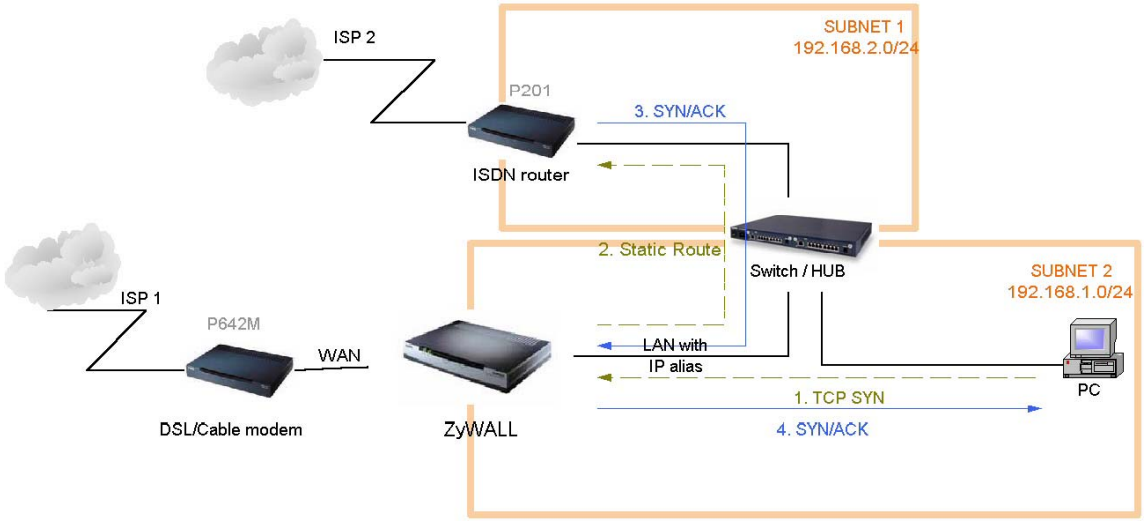


Figure 5-2 Gateway on alias IP network

(2) Gateway on WAN side

A working topology is suggested as below.

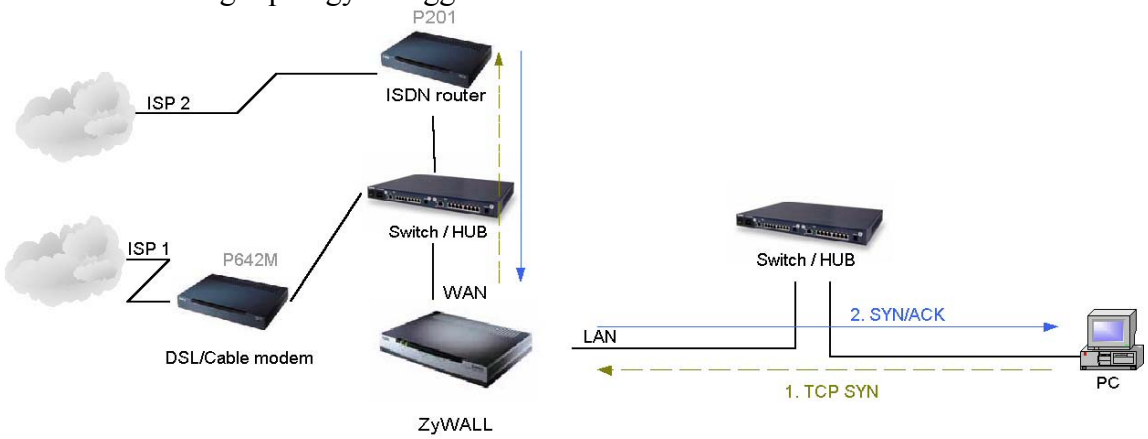


Figure 5-3 Gateway on WAN side

Appendix 5 Mail server setting causes system hang

Condition:

When users set up mail server or syslog server with domain name by CI command or set up in eWC→LOGS→Log Settings, system will resolve the server's domain name when users save the setting (or press "Apply" in eWC→LOGS→Log Settings). If the domain name for the mail server or syslog server can not be resolved (domain name is not correct, network is disconnected, etc.) at that time, system will halt if it sends logs or alert out.

Solution:

While saving the setting of mail server or syslog server address, if the server's address which is a domain name can not be resolved, system will not send alert or log out.

New CI command: *sys log resolve*

Purpose:

Force system to resolve syslog mail server address and mail server address.

Note:

This is a workaround version. During resolve, there will be no other DNS query packet can be processed.

Appendix 6 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 or 0.0.0.0	My WAN IP	My WAN IP
0.0.0.0	a.b.c.d (NOT 0.0.0.0)	My WAN IP	a.b.c.d
a.b.c.d (not 0.0.0.0)	*blank or 0.0.0.0	a.b.c.d	a.b.c.d
a.b.c.d (not 0.0.0.0)	e.f.g.h (NOT 0.0.0.0)	a.b.c.d	e.f.g.h

*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 or 0.0.0.0	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 (NOT 0.0.0.0)	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".

Appendix 7 DNS servers for IPSec VPN Note

DNS Domain Names

DNS (Domain Name System), a system for naming computers and network services that is organized into hierarchy of domain. DNS services provided by the DNS server can resolve the name to other information associated with the name, such as an IP address. The ZyWALL can be configured as a DHCP server. For most cases, your computer connected to the LAN of the ZyWALL can get IP settings (IP address, network mask, gateway address and DNS server address) from the ZyWALL DHCP server automatically.

There are three ways the ZyWALL's DHCP server assigns DNS servers addressed to its DHCP client computers.

(1) If the administrator has setup DNS servers on the ZyWALL's DHCP setting, the ZyWALL will tell the client those DNS server addresses.
(2) If the DNS server has not been setup on the ZyWALL DHCP server, but the ZyWALL has gotten the public DNS servers from the ISP; the ZyWALL will assign those public DNS servers address.
(3) The ZyWALL gives its own LAN IP address and acts as a DNS server proxy.

But the above are not enough for IPSec VPN applications.

How to access the private network by using domain names

On the IPSec VPN application, the user on the LAN of the ZyWALL, wants to access remote private networks. He must use the IP address to identify the remote site he wants to access. But at the modern intranet applications, we still want to have the DNS service for private network access. For example, there is a private Web server installed at the headquarters of your computer. You can access this Web server inside your company, or from your home by way of the ZyWALL's IPSec tunnel. The IP address of the private Web server is also private. You can't use the Internet public DNS servers to resolve those domain names that belong to your company's private network. You must setup those private DNS servers on your computer manually if you want to access the private network by using domain names.

ZyWALL DNS Servers for IPSec VPN

The ZyWALL has added DNS Server on each IPSec policy setup. When you setup the IPSec rule, you can give the DNS server if there exists a DNS Server that provides DNS service for this private network. The DHCP client (on ZyWALL's LAN) requests the IP information from your ZyWALL, the ZyWALL assigns additional DNS servers for IPSec VPN to the client, if the assigned IP address belongs to the range of local addresses of the IPSec rule.

Summary:

1. When Local ID Content is blank or 0.0.0.0, 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 or 0.0.0.0, 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 or 0.0.0.0, 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 such a kind of rule in top of rule list, it may be matched first. To avoid this problem, we will enhance it in the future.

Annex A CI Command List

Last Updated: 2002/11/26

Command Class List Table		
System Related Command	Exit Command	Device Related Command
Ethernet Related Command	POE Related Command	PPTP Related Command
Configuration Related Command	IP Related Command	IPSec Related Command
Firewall Related Command		

System Related Command Home

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

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

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

		save		save upnp information

Exit Command [Home]

Command				Description
exit				exit smt menu

Device Related Command [Home]

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

Ethernet Related Command [Home]

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

POE Related Command [Home]

Command				Description
poe				
	status		[ch_name]	see poe status
	dial		<node>	dial a remote node
	drop		<node>	drop a pppoe call
	ether		[rfc|3com]	set /display pppoe ether type

PPTP Related Command [Home]

Command				Description
pptp				
	dial		<rn-name>	dial a remote node
	drop		<rn-name>	drop a remote node call
	tunnel		<tunnel id>	display pptp tunnel information

Configuration Related Command Home

Command					Description
config					The parameters of config are listed below.
edit	firewall	active <yes|no>			Activate or deactivate the saved firewall settings
retrieve	firewall				Retrieve current saved firewall settings
save	firewall				Save the current firewall settings
display	firewall				Displays all the firewall settings
		set <set#>			Display current entries of a set configuration; including timeout values, name, default-permit, and number of rules in the set.
		set <set#>	rule <rule#>		Display current entries of a rule in a set.
		attack			Display all the attack alert settings in PNC
		e-mail			Display all the e-mail settings in PNC
		?			Display all the available sub commands
		e-mail	mail-server <mail server IP>		Edit the mail server IP to send the alert
			return-addr <e-mail address>		Edit the mail address for returning an email alert
			e-mail-to <e-mail address>		Edit the mail address to send the alert
			policy <full | hourly |daily | weekly>		Edit email schedule when log is full or per hour, day, week.
			day <sunday | monday | tuesday | wednesday | thursday | friday | saturday>		Edit the day to send the log when the email policy is set to Weekly
			hour <0~23>		Edit the hour to send the log when the email policy is set to daily or weekly
			minute <0~59>		Edit the minute to send to log when the email policy is set to daily or weekly
			Subject <mail subject>		Edit the email subject
		attack	send-alert <yes|no>		Activate or deactivate the firewall DoS attacks notification emails
			block <yes|no>		Yes: Block the traffic when exceeds the tcp-max-incomplete threshold
					No: Delete the oldest half-open session when exceeds the tcp-max-incomplete threshold
			block-minute <0~255>		Only valid when sets 'Block' to yes. The unit is minute
			minute-high <0~255>		The threshold to start to delete the old half-opened sessions to minute-low
			minute-low <0~255>		The threshold to stop deleting the old half-opened session
			max-incomplete-high <0~255>		The threshold to start to delete the old half-opened sessions to max-incomplete-low
			max-incomplete-low <0~255>		The threshold to stop deleting the half-opened session
			tcp-max-incompl		The threshold to start executing the block field

			ete <0~255>		
		set <set#>	name <desired name>		Edit the name for a set
			default-permit <forward|block>		Edit whether a packet is dropped or allowed when it does not match the default set
			icmp-timeout <seconds>		Edit the timeout for an idle ICMP session before it is terminated
			udp-idle-timeout <seconds>		Edit the timeout for an idle UDP session before it is terminated
			connection-timeout <seconds>		Edit the wait time for the SYN TCP sessions before it is terminated
			fin-wait-timeout <seconds>		Edit the wait time for FIN in concluding a TCP session before it is terminated
			tcp-idle-timeout <seconds>		Edit the timeout for an idle TCP session before it is terminated
			pnc <yes|no>		PNC is allowed when 'yes' is set even there is a rule to block PNC
			log <yes|no>		Switch on/off sending the log for matching the default permit
			rule <rule#>	permit <forward|block>	Edit whether a packet is dropped or allowed when it matches this rule
				active <yes|no>	Edit whether a rule is enabled or not
				protocol <0~255>	Edit the protocol number for a rule. 1=ICMP, 6=TCP, 17=UDP...
				log <none|match|not-match|both>	Sending a log for a rule when the packet none|matches|not match|both the rule
				alert <yes|no>	Activate or deactivate the notification when a DoS attack occurs or there is a violation of any alert settings. In case of such instances, the function will send an email to the SMTP destination address and log an alert.
				srcaddr-single <ip address>	Select and edit a source address of a packet which complies to this rule
				srcaddr-subnet <ip address> <subnet mask>	Select and edit a source address and subnet mask if a packet which complies to this rule.
				srcaddr-range <start ip address> <end ip address>	Select and edit a source address range of a packet which complies to this rule.
				destaddr-single <ip address>	Select and edit a destination address of a packet which complies to this rule
				destaddr-subnet <ip address> <subnet mask>	Select and edit a destination address and subnet mask if a packet which complies to this rule.
				destaddr-range <start ip address> <end ip address>	Select and edit a destination address range of a packet which complies to this rule.
				tcp destport-single <port#>	Select and edit the destination port of a packet which comply to this rule. For non-consecutive port numbers, the user may repeat this command line to enter the multiple port numbers.
				tcp destport-range <start port#> <end port#>	Select and edit a destination port range of a packet which comply to this rule.
				udp destport-single <port#>	Select and edit the destination port of a packet which comply to this rule. For non-consecutive port numbers, users may repeat this command line to enter the multiple port numbers.
				udp destport-range <start	Select and edit a destination port range of a

				port#> <end port#>	packet which comply to this rule.
				desport-custom <desired custom port name>	Type in the desired custom port name
delete	firewall	e-mail			Remove all email alert settings
		attack			Reset all alert settings to defaults
		set <set#>			Remove a specified set from the firewall configuration
		set <set#>	rule <rule#>		Remove a specified rule in a set from the firewall configuration
insert	firewall	e-mail			Insert email alert settings
		attack			Insert attack alert settings
		set <set#>			Insert a specified rule set to the firewall configuration
		set <set#>	rule <rule#>		Insert a specified rule in a set to the firewall configuration
cli					Display the choices of command list.
debug	<1|0>				Turn on|off trace for firewall debug information.

IP Related Command Home

Command				Description
ip				
	address		[addr]	display host ip address
	alias		<iface>	alias iface
	aliasdis		<0|1>	disable alias
	arp			
		status	<iface>	display ip arp status
	dhcp		<iface>	
		client		
			release	release DHCP client IP
			renew	renew DHCP client IP
		status	[option]	show dhcp status
	dns			
		query		
		server	<primary> [secondary] [third]	set dns server
		stats		
			clear	clear dns statistics
			disp	display dns statistics
	httpd			
	icmp			
		status		display icmp statistic counter
		discovery	<iface> [on|off]	set icmp router discovery flag
	ifconfig		[iface] [ipaddr] [broadcast <addr> |mtu <value>|dynamic]	configure network interface
	ping		<hostid>	ping remote host
	route			
		status	[if]	display routing table
		add	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add route
		addiface	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add an entry to the routing table to iface
		addprivate	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add private route
		drop	<host addr> [/<bits>]	drop a route
	smtp			

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

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

			<iface> v1compat [on|off]	turn on/off v1compat on iface
		robustness	<num>	set igmp robustness variable
		status		dump igmp status
	pr			

IPSec Related Command Home

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

				pre-shared key. It is a dynamic rule with local: the route's WAN IP. The algorithms with it are fixed to phase1: DES+MD5, DH1 and SA lifetime 28800 seconds; phase2: DES+MD5, PFS off, no anti-replay and SA lifetime 28800 seconds. The length of pre-shared key is between 8 to 31 ASCII characters.
		switch	<on|off>	Activate or de-activate the secured remote access tunnel.
	keep_alive	<rule #>	<on|off>	Set ipsec keep_alive flag
	load	<rule #>		Load ipsec rule
	save			Save ipsec rules
	config	netbios	active <on|off>	Set netbios active flag
			group <group index1, group index2…>	Set netbios group
		name	<string>	Set rule name
		name	<string>	Set rule name
		keeyAlive	<Yes| No>	Set keep alive or not
		lcIdType	<0:IP | 1:DNS | 2:Email>	Set local ID type
		lcIdContent	<string>	Set local ID content
		myIpAddr	<IP address>	Set my IP address
		peerIdType	<0:IP | 1:DNS | 2:Email>	Set peer ID type
		peerIdContent	<string>	Set peer ID content
		secureGwAddr	<IP address | Domain name>	Set secure gateway address or domain name
		protocol	<1:ICMP | 6:TCP | 17:UDP>	Set protocol
		lcAddrType	<0:single | 1:range | 2:subnet>	Set local address type
		lcAddrStart	<IP>	Set local start address
		lcAddrEndMask	<IP>	Set local end address or mask
		lcPortStart	<port>	Set local start port
		lcPortEnd	<port>	Set local end port
		rmAddrType	<0:single | 1:range | 2:subnet>	Set remote address type
		rmAddrStart	<IP>	Set remote start address
		rmAddrEndMask	<IP>	Set remote end address or mask
		rmPortStart	<port>	Set remote start port
		rmPortEnd	<port>	Set remote end port
		antiReplay	<Yes | No>	Set anitreplay or not
		keyManage	<0:IKE | 1:Manual>	Set key manage
		ike	negotiationMode <0:Main | 1:Aggressive>	Set negotiation mode in phase 1 in IKE
			preShareKey <string>	Set pre shared key in phase 1 in IKE
			p1EncryAlgo <0:DES | 1:3DES>	Set encryption algorithm in phase 1 in IKE
			p1AuthAlgo <0:MD5 | 1:SHA1>	Set authentication algorithm in phase 1 in IKE
			p1SaLifeTime <seconds>	Set sa life time in phase 1 in IKE
			p1KeyGroup <0:DH1 | 1:DH2>	Set key group in phase 1 in IKE
			activeProtocol <0:AH | 1:ESP>	Set active protocol in phase 2 in IKE
			p2EncryAlgo <0:Null | 1:DES | 2:3DES>	Set encryption algorithm in phase 2 in IKE
			p2AuthAlgo <0:MD5 | 1:SHA1>	Set authentication algorithm in phase 2 in IKE
			p2SaLifeTime <seconds>	Set sa life time in phase 2 in IKE
			encap <0:Tunnel | 1:Transport>	set encapsulation in phase 2 in IKE
			pfs <0:None | 1:DH1 | 2:DH2>	set pfs in phase 2 in IKE
		manual	activeProtocol <0:AH | 1:ESP>	Set active protocol in manual
		manual ah	encap <0:Tunnel | 1:Transport>	Set encapsulation in ah in manual

			spi <decimal>	Set spi in ah in manual
			authAlgo <0:MD5 | 1:SHA1>	Set authentication algorithm in ah in manual
			authKey <string>	Set authentication key in ah in manual
		manual esp	encap <0:Tunnel | 1:Transport>	Set encapsulation in esp in manual
			spi <decimal>	Set spi in esp in manual
			encryAlgo <0:Null | 1:DES | 2:3DES>	Set encryption algorithm in esp in manual
			encryKey <string>	Set encryption key in esp in manual
			authAlgo <0:MD5 | 1:SHA1>	Set authentication algorithm in esp in manual
			authKey < string>	Set authentication key in esp in manual

Firewall Related Command Home

Command				Description
sys	Firewall			
		acl		
			disp	Display specific ACL set # rule #, or all ACLs.
		active	<yes|no>	Active firewall or deactivate firewall
		clear		Clear firewall log
		cnt		
			disp	Display firewall log type and count.
			clear	Clear firewall log count.
		disp		Display firewall log
		online		Set firewall log online.
		pktdump		Dump the 64 bytes of dropped packet by firewall
		update		Update firewall
		dynamicrule		
		tcprst		
			rst	Set TCP reset sending on/off.
			rst113	Set TCP reset sending for port 113 on/off.
			display	Display TCP reset sending setting.
		icmp		
		dos		
			smtp	Set SMTP DoS defender on/off
			display	Display SMTP DoS defender setting.
			ignore	Set if firewall ignore DoS in lan/wan/dmz/wlan
		ignore		
			dos	Set if firewall ignore DoS in lan/wan/dmz/wlan

tria Set
ngle if
fire
wall
ign
ore
tria
ngle
rout
e in
lan/
wan

/dm
z/wl
an