ZyXEL

Firmware Release Note

ZyWALL 100

Release 3.52(WB.2)

Date: **Sep 30, 2003**
Author: **Jason Chiang**

ZyXEL ZyWALL 100 Standard Version
Release 3.52(WB.2)
Release Note

Date: Sep 30, 2003

Supported Platforms:

ZyXEL ZyWALL 100

Versions:

ZyNOS F/W Version: V3.52(WB.2) | 09/30/2003
BootBase : V1.04 | 09/11/2001 15:20:23

Notes:

1. Restore to Factory Defaults Setting Requirement: No
2. When users want to insert a firewall rule with a specific rule number, users may need to select the rule number and re-key a new one. Then users press insert to insert the rule with a specific rule number.
3. The setting of ignore triangle route is on in default ROM FILE. If you only update the firmware from older than 3.50(WB.5)b5, please type “sys firewall ignore triangle all on” in SMT24.8 to bypass firewall check of triangle route traffic. Triangle route network topology has potential security crisis. If you are not clear about it, please refer to Appendix 5 for the triangle route issue.
4. MAC address needs colons to separate each byte.
5. 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.
6. 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.
7. When firewall turns from "off" to "on", the firewall initialization procedure will disconnect all connections running through the ZyWALL.
8. SUA/NAT address loopback feature was enabled on ZyWALL 100 by default; however, if users do not need it, a C/I command "ip nat loopback off" could turn it off.
9. Although there are 120 IPSec SAs can be configured, only 100 of them can be activated concurrently.
10. To achieve higher throughput on routing/encrypting/decrypting/NATing/…, a trade-off may sometimes suffer administrator from slower response user interface.
11. It is a trade-off that if users (from LAN/DMZ) want to access servers (in LAN/DMZ) via global IP addresses (in NAT/SUA case), throughput would suffer from a user-friendly yet redundant translation of IP address.

12. 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.
13. ZyWALL 100 support ZyAIR 100/B100/B101 wireless LAN PC Card.

Known Issues:

1. Some wireless card can not login through 802.1x under Windows XP.
2. Do not support previous devices with serial number from 212001903 to 212001922, and 212304985 to 212305064. The system will hang up in these devices.
3. Symptom: After system boot up, static route cannot set into routing table.
   Condition: If gateway in static route belongs to WAN interface, static route node will not add in routing table and have no function after ZyWALL reboot. So, users need to reactive static route rule to enable this function.
4. L2TP VPN is not ready yet.
5. Symptom: ZyWALL WLAN-802.1X can not connect with PC whose OS version is Windows XP SP1.
   Condition: Since ZyWALL doesn't support TLS and there is no MD5 supported in Windows XP SP1, ZyWALL can not connect with the PC which has upgraded to Windows XP SP1.
6. When Peer ID content is blank when its ID type is IP and the secure gateway address is 0.0.0.0, the rule will be chosen when incoming packets' ID type is IP. This is because ZyWALL only check ID type when this rule's ID content is blank and ID type is IP. We will modify it in the future.
7. When WAN is static IP assigned by user, disable WAN remote node in SMT 11.1 will not deactivate WAN traffic.

Features:

Modifications in V 3.52(WB.2) | 9/30/2003

1. Modify for formal release.

Modifications in V 3.52(WB.2)b1 | 8/21/2003

1. [FEATURE CHANGE] Do not check protocol and port information during IKE phase 1 negotiation.
2. [FEATURE CHANGE] In previous design in traffic redirect, system checks traffic in all ways periodically. Now router checks backup route only when WAN is disconnected.
3. [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.
4. [FEATURE CHANGE] [FEATURE CHANGE] eWC→Firewall→Attack Alert: Change max incomplete TCP number from 10 to 30.
5. [BUG FIX] Symptom: IPSec packets will use ZyWALL's LAN IP as source IP.
   Condition:
   (1) There is a full feature NAT rule to transffered 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.
6. [BUG FIX] Symptom: Netmeeting causes system crashes.
7. [BUG FIX] Symptom: Sometimes system may crash when the client on LAN tries to send PPTP packets.
   Condition: PC(PPTP dial) -> ZyWALL -> ISP(PPTP Server)
   ZyWALL will do the PPTP pass through, but sometimes system may crash.

Modifications in V 3.52(WB.1) | 6/2/2003

Modifications in V 3.52(WB.1)b3 | 5/30/2003

1. [BUG FIX] Symptom & Condition: Sometimes ZyWALL may fail to parse the response from a DNS server.
2. [BUG FIX] Symptom & Condition: Users can not upgrade firmware through CNM.

Modifications in V 3.52(WB.1)b2 | 5/27/2003

Modifications in V 3.52(WB.1)b1 | 5/21/2003

1. [BUG FIX] Symptom & 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).
2. [BUG FIX] Symptom: After firmware upgrade, VPN rules cannot work.
   Condition: After firmware upgraded from 3.50 to 3.52, the VPN rules cannot work anymore. The only solution is to save these rules again.
3. [BUG FIX] Symptom: When changing Menu 4 "Encapsulation", the other items do not change immediately
   Condition:
   1) Configure the remote node 2 in the SMT11.
   2) Change the Encapsulation type in the SMT4.
   3) The "Service Type", "My Login", "My Password" will not change immediately.
4. [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.
5. [ENHANCEMENT] Support Vantage 1.0.

Modifications in V 3.52(WB.0) | 5/12/2003

Modifications in V 3.52(WB.0)b8 | 5/5/2003

1. [BUG FIX] Symptom: After phase 2 rekey, dynamic rule cannot pass traffic anymore.
   Condition:
   1) 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.
   2) After the phase 2 rekey, traffic cannot pass this tunnel anymore.
2. [BUG FIX] Symptom: When ‘keep alive’ flag turns on, disconnection in SA monitor didn't work correctly.
   Condition:
   1) Turn on keep alive flag.
   2) Use SA monitor to disconnect the tunnel.
   3) The tunnel will not be disconnected properly. There will be still tunnels showed on SA monitor.
3. [BUG FIX] Symptom & Condition: A NULL domain name is queried continuously when email log server or syslog server is not set.
4. [BUG FIX] Symptom: LAN side PC can’t access internet by default setting in SMT.
   Condition: The wrong default value of dial backup setting cause LAN side PC can’t

access internet.

5. [BUG FIX] Symptom & Condition: Setting dial backup through eWC, dial backup can't work.

Modifications in V 3.52(WB.0)b7 | 4/29/2003

1. [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.
2. [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.
3. [BUG FIX] Symptom: Dial backup eWC page will save setting even user do not apply anything.
   Condition: When user browse eWC dial backup page and leave this page without any setting applied. This page still save some setting in ROM file.
4. [BUG FIX] Symptom & Condition: SA monitor always show only one tunnel message even there are more than one tunnel existing in ZyWALL.
5. [BUG FIX] Symptom & Condition: System hangs up when LAN side client send file to WLAN client.
6. [BUG FIX] Symptom & Condition: Change dial backup setting except password in eWC page will save the wrong password in ROM file.
7. [BUG FIX] Symptom & Condition: Email log messages cannot be sent when the log schedule is changed from "HOURLY" to "NONE" and then changed back to "HOURLY" again.

Modifications in V 3.52(WB.0)b6 | 4/21/2003

1. [FEATURE CHANGE] In the past, after phase 2 rekey, responder still use old phase 2 SA to transmit packets for a certain period and then started use the new phase 2 SA. Now responder will use new phase 2 SA after rekey immediately.
2. [BUG FIX] Symptom: After rekey, VPN connection will fail to transmit traffic.
   Condition:
   1). When our NAT device is between two VPN routers and these two VPN routers enable NAT-traversal feature.
   2). After rekey process, the IPSec connection between these two VPN routers will be disconnected.
3. [BUG FIX] Symptom & Condition: Sometimes Enable/Disable traffic redirect when WAN encapsulation is PPPoE, system may crash.
4. [BUG FIX] Symptom & Condition: Under heavy traffic, firewall sometime has

inexplicable crash.

5. [BUG FIX] Symptom: After Unplug/Plug the WAN cable, PPPoE can't dial out anymore.
   Condition: When users unplug the wan cable, the PPPoE connection will be dropped. But after the cable plug into WAN port again. PPPoE can't dial out anymore.
6. [BUG FIX] Symptom & Condition: When viewing the "MAINTENANCE->VIEW LOG" Web page, the content loading time takes very long.
7. [BUG FIX] Symptom: ID type for VPN can not be changed from DNS or Email to IP.
   Condition: We can not change VPN ID type from DNS or E-mail to IP and will get error message - “Local ID content should be IP format”.
8. [BUG FIX] Symptom & Condition: Use wireless LAN and dial backup at same time will hang up our system.
9. [BUG FIX] Symptom & Condition: Using software - “ping plotter”, packets will lose in our system.

Modifications in V 3.52(WB.0)b5 | 3/28/2003

1. [NEW FEATURE] Add auto reload mechanism on eWC when you reset system setting back to factory default on eWC.
2. [NEW FEATURE] On Maintenance DHCP Table page, add "Reserve" checkbox to support reserve function. If the checkbox is checked, the IP-MAC pair is added into Static DHCP Table after clicking the "Apply" button.
3. [ENHANCEMENT] Support sorting display for IP address in DHCP Table.
4. [ENHANCEMENT]
   1). Add eWC wizard WAN IP check – WAN IP address can’t set with in LAN subnet.
   2). Add eWC wizard telia service check – relogin value, WAN IP assignment and telia login server should be domain name.
5. [ENHANCEMENT] Support hexadecimal format of pre-shared key. Now pre-shared key starting with "0x" or "0X" will be treated as hexadecimal format.
   Note: If old configuration with leading "0x" or "0X" will also be treated as hexadecimal input when save it again.
6. [ENHANCEMENT] When the checkbox "Enable Filter List Customization" is disabled, also disable the checkboxes "Disable all web traffic except for trusted domains" and "Don't block Java/ActiveX/Cookies/Web Proxy to trusted domain sites".
7. [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.
8. [FEATURE CHANGE] Remove "view error log" selection in smt24.3 "System Maintenance - Log and Trace".

9. [FEATURE CHANGE] Hide error log messages and error log CI command in both centralized log case and non centralized log case.
10. [FEATURE CHANGE] Explain and separate the log "Firewall sent TCP reset packets".
    New logs will be showed below:
    1). Under SYN flood attack, sent TCP RST.
    2). Exceed TCP MAX incomplete, sent TCP RST.
    3). Peer TCP out-of-state, sent TCP RST.
    4). Firewall session time out, sent TCP RST.
    5). Exceed MAX incomplete, sent TCP RST.
11. [FEATURE CHANGE] On WAN IP and Wizard page, when under Ethernet mode, the wording "Remote IP Address" is changed to "Gateway IP Address".
12. [BUG FIX] Symptom: PPTP connection is not stable.
    Condition: If encapsulation is PPTP, system can't dial out anymore after the line is dropped or disconnected once.
13. [BUG FIX] Symptom: Save Telia login service under static IP address assignment will show roadrunner error message.
    Condition: Telia login only work when WAN IP is assigned with dynamic IP. If save this service with static IP, the error message is not correct.
14. [BUG FIX] Symptom: Firewall blocked AH packet, no matter what the firewall configured.
    Condition: When one VPN security gateway locates on WAN and the other locates on LAN, AH packets were blocked by firewall even the setting is forward.
15. [BUG FIX] Symptom: 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 re-key. If the initiator did not send DEL phase 1 information packet first and then start another phase 1 negotiation directly, this negotiation may fail.
16. [BUG FIX] Symptom: Sometimes IPSec rekey procedure failed.
    Condition: Under heavy traffic, sometimes IPSec rekey failed.
17. [BUG FIX] Symptom & Condition: When the user types the illegal value of the Telia server and relogin time, the system reboots.
18. [BUG FIX] Symptom & Condition: The NAT session per host value is zero when the WAN port is not connected to Internet.
19. [BUG FIX]Symptom: Java applet, ActiveX, Cookie can't log twice continuously.
    Condition:
    1). Enable logging restricted web features in log setting page.
    2). Access some web sites that contain Java applet, ActiveX, Cookie twice continuously.
    3). Go to "View log" page and will see that there is only one blocking message in the log page.
20. [BUG FIX] Symptom: In SMT11.3, the WAN IP check criteria are not correct when encapsulation is PPTP or PPPoE.

Condition:
Before: When checking WAN IP address is on LAN subnet or not, system used "remote IP address " as the WAN IP value.
Now: System uses "My WAN address" as the WAN IP value for checking.

21. [BUG FIX] Symptom & Condition: Using "MG-SOFT MIB Browser" to get SNMP information twice will cause router to crash.
22. [BUG FIX] Symptom: Local and peer content can't change when ID type is IP with CI command.
    Condition: "ipsec config lcIdContent" and "ipsec config peerIdcontent" can't change the value when ID type is IP.
23. [BUG FIX] Symptom & condition: When user configure the VPN negotiation mode setting in Web, the setting won't changed in Web configuration.
24. [BUG FIX] Symptom & condition: When user configures the daylight saving setting in SMT, the setting won't be affected in Web configuration.
25. [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.
26. [BUG FIX] Symptom & Condition: Disable or delete dial backup remote node will not delete the routing table used by Backup ISP.
27. [BUG FIX] Fix two vulnerabilities in eWC.

Modifications in V 3.52(WB.0)b4 | 2/26/2003

1. [ENHANCEMENT] Add product name on eWC page title.
2. [ENHANCEMENT] Add service type - Telia login.
3. [ENHANCEMENT] Check Point UDP port 2746 timeout value enlarge support.
   NOTE: Use CI command "ip nat timeout udp [port] <seconds>" to change the timeout value.
4. [FEATURE CHANGE] Email log and alert can be sending by setting only "send log" or "send alert" Email address.
5. [FEATURE CHANGE] Dial backup default setting will enable SUA only now.
6. [FEATURE CHANGE] Change the mechanism of initial contact in reboot detection (original: tunnel-based, now: machine-based).
   NOTE:
   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.
7. [FEATURE CHANGE] 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.
   NOTE:
   1. Please use "ipsec swSkipOverlapIp <on|off>" to control this behavior.
   2. The default setting of swSkipOverlapIp is "off".
8. [BUG FIX] Symptom: Configure the LAN IP on SMT menu 3.2, the system doesn't save the configuration.

Condition:
1. Set WAN IP to 192.168.2.1.
2. Set WAN IP to dynamic IP.
3. Set LAN IP to 192.168.2.1.
4. The system doesn't save the configuration of step 3.

9. [BUG FIX] Symptom: NAT rule save the wrong configuration.
   Condition: When setting the NAT address mapping rule and the start IP is greater than the end IP address, the configuration can be saved.
10. [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.
11. [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.
12. [BUG FIX] Symptom: ZyWALL 100 reboot when delete remote node.
    Condition:
    1. Enable dial backup.
    2. Drop WAN port and let dial backup active.
    3. Disable dial backup in SMT menu2 and delete dial backup remote node in SMT menu11.
13. [BUG FIX] Symptom: Change wireless country code from 219 to 233 will cause ZyWALL reboot.
    Condition: After changing country code from 213 to 233 while wireless is enabled and WEP enabled will reboot our ZyWALL.
14. [BUG FIX] Symptom: Incorrect hint messages on SMT of menu 11.1.
    Condition: The hint message on SMT of menu 11.1 is not correct when encapsulation is PPTP. The hint messages of "My IP Addr" and "My IP Mask" is wrong.
15. [BUG FIX] Symptom & Condition: ZyWALL crashes when receiving an unexpected RIP packet.
16. [BUG FIX] Symptom: Dial backup eWC wording is not consistency with others.
    Condition: RIP direction wording case under dial backup page is not consistency with other pages.
17. [BUG FIX] Symptom: eWC – Daylights saving can't save when end date is smaller than start date.
    Condition: Saving Daylights when end date is smaller than start date, status will show "Start month is greater then end month" and can't be saved.
18. [BUG FIX] Symptom: Insert a new firewall rule and cancel it will get abnormal index number.
    Condition: If we insert a new firewall rule before rule 2 and cancel this new rule. Original rule will move to index 3 and is not the original index number.
19. [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.

Modifications in V 3.52(WB.0)b3 | 1/20/2003

1. [ENHANCEMENT] Extended Wireless local user database from 10 to 32.
2. [ENHANCEMENT] Add system restart button in eWC, which is in "MAINTENANCE – Configuration ". We will change it as a single page isolated with configuration in the next release.
3. [FEATURE CHANGE] Concurrent NAT session number enlarges to 4096.
4. [FEATURE CHANGE] For firewall default setting, we remove the hint message in eWC with NetBIOS from WAN to DMZ, and add the hint message in eWC with NetBIOS from DMZ to LAN.
5. [FEATURE CHANGE] Combine eWC Dial Backup pages in WAN. Now we have one Dial Backup tag in eWC WAN page.
6. [BUG FIX] Symptom: Ethernet WAN IP can't be changed from static to dynamic in eWC.
   Condition: When Ethernet WAN IP changes to static, it can't be changed to dynamic again in eWC.
7. [BUG FIX] Symptom: Enable WEP encryption and 802.1x will cause authentication failed.
   Condition: Both WEP and 802.1x are enabled will cause authentication failed.
8. [BUG FIX] Symptom: ZyAIR 100 V2.0 can't work.
   Condition: ZyAIR 100 V2.0 Wireless LAN PC card can't be recognized by ZW100.
9. [BUG FIX] Symptom: We can not build VPN connection with others ZyWALL series while VPN ID type is IP address.
   Condition: Bulid VPN connection with VPN ID type is IP address and leave content with blank and set My IP addr to 0.0.0.0 can't build tunnel between two ZyWALLs.
   Note: please reference the appendix 8 to get IPSec FQDN support.
10. [BUG FIX] Symptom: Changing PPPoE WAN IP causes our ZyWALL crash.
    Condition: While PPPoE dial fail and change WAN IP form static IP to dynamic IP cause ZyWALL crash.
11. [BUG FIX] Symptom: Enable cookie and receive F through web will crash our ZyWALL.
    Condition: Receiving hotmail through http://www.hotmail.com will cause ZyWALL reboot.
12. [BUG FIX] Symptom: When use CI (ip urlfilter category timeOfDay) command to configure the blocking time of content filter, the saved time value is wrong
    Condition: When the input time format is not the expected format hh:mm, the system will store wrong value. Now, time formats like "hh:mm", "h:mm", "hh:m" or "h:m" are acceptable.

Modifications in V 3.52(WB.0)b2 | 12/31/2002

1. [ENHANCEMENT] Add centralized logs for phase 1 ID (FQDN).
2. [ENHANCEMENT] 802.1x is supported for wireless LAN.
3. [ENHANCEMENT] Centralize Log is completed.
4. [ENHANCEMENT] ACL rule number is extended to 400.
5. [ENHANCEMENT] Static route rule number is extended to 50.
6. [ENHANCEMENT] Add ZyReport to collect traffic Statistics.
7. [ENHANCEMENT] Add IPSec NAT traversal support. It only supports ESP tunnel and ESP transport when key management is IKE. No manual key support for IPSec NAT traversal.
8. [ENHANCEMENT] Add CI commands to configure IPSec rules. Please refer CI command list.
9. [ENHANCEMENT] Add CI commands to configure static route rules. Through these commands, users can set / modify static route rules.
10. [ENHANCEMENT] Add a Go to page in eWC→ VPN.
11. [ENHANCEMENT] The subject of email for the logs can be configured by CI command "sys logs mail subject".
12. [ENHANCEMENT] Add Administrator Inactivity Timer. Let users can specify ZyWALL management session (either via the web configuration or SMT) idle timeout value.
13. [ENHANCEMENT] Show the reason of forward/block by content filter in the centralized log message.
14. [ENHANCEMENT] Add a retype password confirmation mechanism for PPTP and PPPoE setup in SMT menu 4 and 11.
15. [ENHANCEMENT] Add full path + file name check for keyword blocking.
16. [ENHANCEMENT] The system can send an alert mail of “Access Control”, “Blocked JAVA etc”, “IPSec”, and “IKE” categories.
17. [ENHANCEMENT] Add new centralized log category – IKE. And add CI command “sys logs category ike” to set it, “sys logs display ike” to display it.
18. [ENHANCEMENT] Add a protection mechanism for password check. When users enter wrong password three times, the system will block users trying to log in for the minutes that user defined. The blocking time will be set by CI command.
    NOTE: Use CI command "sys pwderrtm [minutes]" to set this timeout value.
    System will not perform this check when timeout value is empty.
19. [ENHANCEMENT] Add more ID supported in IKE phase 1 authentication. Now ZyWALL100 supports ID-IP, ID-FQDN, ID-USER-FQDN. All contents of these ID types can be set. During authentication, both peers’ ID content should match each other, or the connection may be rejected.
20. [ENHANCEMENT] Modified "ip dhcp enif0 server dnsorder" CI command. Through this command, users can assign DNS order.
21. [ENHANCEMENT] Add Nailed-Up connection settings for PPPOE & PPTP of eWC.
22. [ENANCEMENT] DDNS enhancement. In previous firmware, ZyWALL will provide its WAN IP to DDNS server, even if it’s a private IP. Now a user can specify the public IP by himself, or let the DDNS detect a proper global IP for ZyWALL.
23. [ENHANCEMENT] Add a new centralize log message - NAT session table is full. When NAT session table is full, there will be a log in Centralized log. Its category is

"System Maintenance".

24. [ENHANCEMENT] In "ip nat iface" CI command, system will parse ESP packets in NAT table list.
25. [ENHANCEMENT] When system updates its time or assign an IP to a host, there will be a log in Centralized log. The category is "System Maintenance".
26. [ENHANCEMENT] When the user login to the router (SMT, FTP, TELNET, or WEB), there will be a log in Centralized log. The category is "System Maintenance".
27. [ENHANCEMENT] In CI command "sys logs display", add a category filter to display only the specified category. For example, "sys logs display access" to display the access category only.
28. [FEATURE CHANGE] Wording change for firewall log messages. For example: "set:1" will be "L to W" means packet from LAN to WAN.
29. [FEATURE CHANGE] The log of remote management is moved from error log to centralized log.
30. [FEATURE CHANGE] In VPN configuration, local / remote IP start field can accept 0.0.0.0.
31. [FEATURE CHANGE] Make hard-coded NetBIOS CI commands visible by users.
32. [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.
33. [FEATURE CHANGE] Remove default port definition for AIM, ICQ and MSN messenger in firewall.
34. [FEATURE CHANGE] In firewall log, use "CHECK NEXT RULE" instead of blank left when a rule log setting is "not match".
35. [FEATURE CHANGE] Modify the firmware upload successful page.
36. [FEATURE CHANGE] If eWC:LAN→Pool Size sets to 0, it must show warning message on status.
37. [FEATURE CHANGE] Hard-coded Netbios filters are modified. Now WAN-to-LAN, LAN-to-WAN, WAN-to-DMZ, DMZ-to-WAN, DMZ-to-LAN and LAN-to-DMZ are independent. Add corresponding pages in eWC: WAN / LAN / DMZ / VPN. Please refer to appendix 4.
38. [FEATURE CHANGE] Default values of hard-coded Netbios filters are changed. They are LAN to WAN: block; LAN to DMZ: block; WAN to LAN: block; WAN to DMZ: block; DMZ to WAN: block; DMZ to LAN: block; IPSec: Forward; Trigger dial: Disable.
39. [FEATURE CHANGE] The default value of resolving IPSec peer's DNS is changed from 30 min to 15 min.
40. [FEATURE CHANGE] Log settings of default policy are changed. For those default policies are "forward", there will be no logs. On the other hand, for those default policies are "block", there will be logs.
41. [FEATURE CHANGE] Log schedule in Centralized log is default to "NONE".
42. [FEATURE CHANGE] Default value of remote management is changed to "ALL".
43. [FEATURE CHANGE] IPSec idle timeout value is changed back to 2 min.
44. [BUG FIX] Symptom: Receving hotmail mail will cause system crash.
    Condition: 1. Enable Block Cookies

2. Receving hotmail mail and cause system crash.

45. [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.
46. [BUG FIX] Content Filter does not block cookies.
47. [BUG FIX] NetBIOS packet crash the router when firewall is enabled.
48. [BUG FIX] Fix a security issue related with IP stack.
49. [BUG FIX] Symptom: Ftp remote management can't work over IPSec tunnel, even if access=ALL.
    Condition: Control channel can be opened over tunnel, but data channel is failed.
50. [BUG FIX] Symptom: Send an email log with more than 34 logs will cause system crash.
    Condition: In logs->view log in the WEB menu, when the number of logs is more than 34, press "Email Log Now" will cause system crash.
51. [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 host can not connect to the router.
52. [BUG FIX] Symptom: Under VPN channel, when sending out large file, the system will crash.
    Condition: When continuously sending large packet and the data packet size is over certain size (say 1450), then the system will eventually crash.
53. [BUG FIX] Symptom: Denied Access Message is too small.
    Condition: The "Denied Access Message" of content filter Full path should extend to all web pages.
54. [BUG FIX] Symptom: “Deleting” function for a NAT set is not complete.
    Condition: Create a rule in menu 15.1.1 in NAT full feature mode then delete the set that contains the rule. Using CI command "ip nat lookup #setnum" will see the deleted set with no rules in it.
55. [BUG FIX] Symptom: Delete an NAT set or that contains an active rule or modify the rule and ping outside host will cause system crashed.
    Condition: Create a rule in menu 15.1.1 in NAT full feature mode and ping outside host, then delete the set that contains the rule and ping it again.
56. [BUG FIX] Symptom: In centralized log, the format of IKE packets is incorrect.
    Condition: During IKE process, ZyWALL will record all payload types of both sent and received packets. However in centralized log, all these payload information is lost.
57. [BUG FIX] Symptom: CI command "ip dns server" is hidden.
    Condition: Entering the following ci command "ip dns", the server command which should be opened is hidden.

58. [BUG FIX] Symptom: Default DNS server can't work.
    Condition: When a user set a static IP on wan and set DHCP = none on LAN setup, the default DNS server can't work and there is no way to set the default DNS server IP.
    Note: A new CI command "ip dns default <ip>" is used to change the default DNS server IP.
59. [BUG FIX] Symptom: Using ci command to set content filter registration will cause system crash.
    Condition: Enter the following four content filter registration ci commands "ip urlfilter reginfo name/eMail/country/clearall" will cause system crashed.
60. [BUG FIX] Symptom: Using ci command to set content filter block time of day will set wrong time value in ROM.
    Condition: Enter ci command "ip urlfilter category timeOfDay" will set wrong value of begin time and end time into ROM.
61. [BUG FIX] Symptom: content filtering doesn't apply after VPN
    Condition: ZyWALL supports a special application:
    ZW(branch)=====VPN=====ZW(HQ)------>Internet
    Internet access from branch office must go out through the VPN tunnel. Thus HQ can control the traffic from / to the branch office. However, content filter setting in HQ cannot control the traffic from branch through the VPN tunnel.
62. [BUG FIX] Symptom: IKE process does not check encapsulation.
    Condition: During IKE negotiation, responder only accepts initiator's encapsulation setting and do not compare the value with its own setting.
63. [BUG FIX] Symptom: CI command "ipsec switch on/off" did not work.
    Condition: CI command "ipsec switch on/off" cannot change the switch state.
64. [BUG FIX] Symptom: When “sys firewall dos ignore lan on”, traceroute failed.
    Condition: When “sys firewall dos ignore lan on”, there will no hop information showed.
65. [BUG FIX] Symptom: SMT menu 24.2.1 will not show correct system name.
    Condition: Once the user configures the system and domain name in SMT menu 1, SMT menu 24.1 will show the string which joins system name and domain, but SMT menu 24.2.1 just display the system name.
66. [BUG FIX] Symptom: When our router exchanges 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 initials with NULL will cause adder function crash our ZyWALL.
67. [BUG FIX] Symptom: Content filtering will block keyword that contains *.html.
    Condition: Use "ip urlfilter customize actionFlag act5 enable" to enable the full path setting. Then add “.html” for keyword blocking. Content filtering will block website that contains *.html.
68. [BUG FIX] Symptom: The keyword blocking does not work.
    Condition: Use browser to access the URL that set in the keyword blocking, the packets will be still allowed to pass after enable the full path check.
69. [BUG FIX] Symptom: Firewall logs duplicate ICMP type 3 code 3 which reply by itself.

Condition: When router receives a unknown UDP service packet, it reply ICMP port unreachable and firewall logs this packet twice.

70. [BUG FIX] Symptom & Condition: During IKE phase 1 negotiation, if ZyWALL receives a Notify DEL payload, it may crash. Reason & Solution: It's a NULL pointer problem which we should check if the DEL payload is sent to a valid SA.
71. [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.
72. [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.
73. [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 within the range of LAN subnet and then save the configuration.
74. [BUG FIX] Symptom: Content filter will block the web site that matches the trusted domain setting.
    Condition: When web site is both in the cybernot filter list and the trusted domain list, the content filter will block the web site.
75. [BUG FIX] Symptom: Can not download cybernot list.
    Condition: On the "Advanced"->"content filter"->"list update" web page, user presses "download now" to download the cybernot list.
76. [BUG FIX] Symptom: Weird ICMP packet logs are generated.
    Condition: When user sends a large echo packet through the firewall, there are many weird ICMP packet logs to be generated. Sometimes the type and code of that ICMP log show undefined number, and the message shows "Unsupported/out-of-order ICMP".
77. [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.
78. [BUG FIX] Fix a security issue related with smurf attack.
79. [BUG FIX] Symptom: The system will allow the packet with DF=1 and the 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.
80. [BUG FIX] Symptom: Firewall->Edit: The “Active” checkbox value will not be saved.
    Condition: If user clicks “SrcAdd” or “SrcEdit” button in Firewall Edit page to configure “Source Address” in one rule, then the value of “Active” checkbox will not be saved.
81. [BUG FIX] Symptom: Remote management to LAN IP over IPSec failed.

Condition: While NAT was enabled, remote device could not access router's LAN IP through IPSec tunnel. In other words, remote management to the LAN IP over IPSec tunnel failed.

82. [BUG FIX] Fix a security issue related with port scan.
83. [BUG FIX] Symptom: VPN web page configuration is not correct.
    Conditions:
    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.
84. [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".
85. [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.
86. [BUG FIX] Symptom: Some IKE INFO logs are treated as ALERT.
    Condition: IKE logs "RECV: [payload]" messages are marked as alert, but it should be INFO.
87. [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.
88. [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.
89. [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.
90. [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.
91. [BUG FIX] Symptom: PC can ping router's LAN IP.
    Condition: When "SUA only" and "firewall off", outside PC can ping router's LAN IP.
92. [BUG FIX] Symptom: ZyWALL 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.
93. [BUG FIX] Symptom: XBox Live can't work through router.
    Condition: Xbox Live can not work through ZyWALL.
94. [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.
95. [BUG FIX] Symptom: Email log can not be sent.

Condition: When alert address is not set in the “Log->Log settings->Send alerts to:” field in the GUI, press the “Email Log Now” button in the Log->View Log page will not email the logs.

96. [BUG FIX] Symptom: In centralized log, the format of IKE packets is incorrect. Condition: During IKE process, ZyWALL will record all payload types of both sent and received packets. However in centralized log, all these payload information is lost.

Modifications in V 3.52(WB.0)b1 | 08/26/2002

1. [NEW FEATURE] Support bandwidth management, please refer to Appendix 6.
2. [FEATURE ENHANCED] IPSec can keep tunnel alive if you switch the keep alive on. When it turns on, even no packets passed through the tunnel, ZyWALL will re-key automatically after SA lifetime times out. Please note that both peers have to switch on this feature, or one side may disconnect.
3. [NEW FEATURE] WLAN can bridge with LAN/DMZ by CI command. Please refer to Appendix 7.
4. [ENHANCEMENT] Add CNM support. CI command “cnm active 1” could be used to active this feature. The default is inactive. CI command “cnm managerIp xxx.xxx.xxx.xxx” is used to specify the IP address of the ZyXEL’s CNM management station. For details for CNM, please reference to the User Guide for CNM.
5. [ENHANCEMENT] Add Centralized LOG support. We added a new page “LOG” in eWC to combine all LOGs from firewall, content filter, IPSec and error log into the same format.
6. [FEATURE ENHANCED] SMT 11.1 add PPTP server netmask
7. [FEATURE ENHANCED] URL checking in content filter is enhanced. Now it can parse full URL path for blocking, and the URL checking can be case insensitive. We have added two CI commands to allow users to turn on these two features. They are “ip urlfilter customize actionFlags act5 enable / disable” and “ip urlfilter customize actionFlags act6 enable”.
   NOTE: Turns on these two features will enlarge search load during content filter process and throughput will be impacted. The default values of them are both “disable”.
8. [BUG FIXED] VPN dynamic rule is not stable. When a runtime rule conflicts with the other during IKE phase 2 negotiation, sometimes ZyWALL will crash.
9. [BUG FIXED] A large number of SNMP packets sending to the ZyWALL will cause it reboot.
10. [BUG FIXED] Fix a vulnerability issue about TCP stack.
11. [BUG FIXED] Changing SNMP setting from eWC cause ZyWALL crash.
12. [BUG FIXED] Using Mozilla, 0.0.0.0 only shows dots in eWC of SUA/NAT address mapping.
13. [BUG FIXED] Setting Dial Timeout, Drop Timeout,and Call Back Delay in SMT 2.1 cause crash.
14. [BUG FIXED] Changing the Web access setting in SMT 24.11, the HTTPD data

crash error log isn't correct.

15. [BUG FIXED] Download CyberNOT list crash on passive mode.
16. [BUG FIXED] Port setting in VPN rule cannot work.
17. [FEATURE CHANGED] Wording changed for IPSec address configuration in SMT27.1, SMT27.1.1 and WEB→IPSec.
18. [FEATURE CHANGED] Triangle route network topology is allowed. We added the CI command to switch on/off firewall checking for triangle route, and this setting is saved in flash rom. It's "sys firewall ignore triangle all [on|off]". The default value is to ignore triangle route check.
19. [FEATURE CHANGED] WAN to LAN traffic is allowed in hard-coded netbios packet filter. We add one more CI command for users to control it. Please refer to appendix 4 for more information.
20. [BUG FIXED] No matter WAN IP and gateway in the same subnet or not, eWC always shows "Gateway must be on same subnet as this host".

Modifications in V 3.50(WB.5) | 06/18/2002

1. [BUG FIXED] Aggressive mode failed to work.
2. [BUG FIXED] Firewall blocks triangle-route reply packets which going through IP alias.
3. [BUG FIXED] IP checksum error causes that IGMP cannot work.
4. [BUG FIXED] Unexpected termination of the telnet session.
5. [FEATURE ENHANCED] Enhanced DoS ICMP handling.
6. [FEATURE ENHANCED] Added CI command "sys firewall ignore triangle <lan|dmz> [on|off]" to ignore triangle route problem. For example, user can bypass firewall checking on LAN by using "sys firewall ignore triangle lan on". Please note that the traffic DO NOT bypass DoS checking when you only use this command.
7. [FEATURE CHANGED] Accept peer's SA lifetime set to both SEC and KB.
8. [BUG FIXED] Use PPPoE / PPTP connection: after disconnection and then dial up again (Nail-up connection), if ZyWALL get new WAN IP, NAT mapping still used old IP address.
9. [BUG FIXED] Dynamic session does not found when NAT loopback.
10. [BUG FIXED] In virtue of port forwarding and NAT loopback, a server connects to itself through WAN IP. ZyWALL treats as "Land Attack".
11. [BUG FIXED] Use Netscape or Mozilla, eWC in Advance WAN page have square symbol.
12. [BUG FIXED] PFS writing error: "Perfect" instead of "Prefect".
13. [BUG FIXED] Use Mozilla, eWC in Wireless LAN page have square symbol.
14. [BUG FIXED] In WAN page, error message "Gateway must be on the same subnet" instead of "Fail to update due to internal error (-10)!"
15. [BUG FIXED] NetBIOS packets always trigger dial no matter "trigger dial" enabled or not.
16. [BUG FIXED] Hard coded netbios filters for IPSec didn't work. Even it is set to "Non-blocking", LAN-to-WAN filter will block netbios packets trying to pass IPSec tunnel.

17. [BUG FIXED] Runtime SPD should not be deleted when its SA lifetime remained.
18. [FEATURE CHANGED] When the DHCP server doesn't response in busy state, ZyWALL will do much more retransmit.

Modifications in V 3.50(WB.4) | 05/14/2002

1. [BUG FIXED] Dial-backup can not hang up ISDN-TA.
2. [BUG FIXED] race condition makes system crash
3. [BUG FIXED] Saving configuration in IPSec Web pages results crash
4. [BUG FIXED] Add then remove custom port results crash
5. [BUG FIXED] Saving configuration in Menu 11.1 results crash
6. [BUG FIXED] Using the Web configurator to inactivate the default route, fail to activate it again
7. [BUG FIXED] Custom Ports only works as a separate rule
8. [BUG FIXED] Static IP Web page only save the last 2 digits of the MAC address
9. [BUG FIXED] Sometimes firewall blocks ICMP packets without reason messages.
10. [FEATURE CHANGED] Idle timeout mechanism of IPSec is changed. Now if there is no outbound traffic and no inbound traffic, the tunnel will be "idle" and won't be deleted. Only when there is outbound traffic but no inbound traffic after the period set by idle timer period, the tunnel will be deleted.
11. [BUG FIXED] Trigger port Web pages fail to save configuration
12. [BUG FIXED] Content filter fail to "Log and Block"
13. [BUG FIXED] Unresolvable domain name result a "0.0.0.0" IP address
14. [BUG FIXED] RemoteManagement-FTP Web page provide invalid default value
15. [BUG FIXED] Menu 4 may show wrong message "Duplicate Static Route"
16. [FEATURE ENHANCED] When ZyWALL detected that its IP address is used by other host, it will alert an error message
17. [FEATURE ENHANCED] SMT menus now check IP address collision
18. [FEATURE ENHANCED] Add new Web pages WAN-ROUTE in WAN setup page
19. [FEATURE ENHANCED] Renew all of WAN help Web pages
20. [FEATURE ENHANCED] Add MISC tags at Remote Management Web pages
21. [FEATURE ENHANCED] Add netmask configuration for PPTP
22. [FEATURE CHANGED] Move Dial backup, Traffic Redirect pages into WAN Web pages
23. [FEATURE CHANGED] Move Trigger Port Web page into SUA/NAT Web pages
24. [BUG FIXED] Enable syslog client and firewall log may cause system hang on an infinite loop
25. [BUG FIXED] Wrong sub-ids in SNMP packets
26. [BUG FIXED] NAT many-one-to-one failed
27. [BUG FIXED] Dial backup Web pages may clear all settings without save them
28. [BUG FIXED] Incorrect label string "DMZ TCP/IP DMZ TCP/IP"
29. [FEATURE ENHANCED] Content Filter Web pages now has "Block Only" option.
30. [BUG FIXED] DHCP server does not provide DNS server.
31. [BUG FIXED] Content Filter doesn't work.
32. [BUG FIXED] Incorrect error log may crash system.
33. [BUG FIXED] Unexpected operations in Web GUI may leave zombie.
34. [BUG FIXED] Custom Port Web pages is still buggy.

35. [BUG FIXED] Firewall Web pages save wrong settings.
36. [NEW FEATURE] Add a new C/I command "sys firewall dos ignore <lan|wan|dmz> [on|off]". For example, user can bypass DoS attack checking on LAN by using "sys firewall dos ignore lan on"
37. [NEW FEATURE] Add a new C/I command "sys filter blockbc [on|off]". For example, user can block broadcast packets by using "sys filter blockbc on". Broadcast packets will be applied here are DHCP packets and RIP packets.
38. [FEATURE ENHANCED] C/I command set for NetBIOS over TCP/IP (NBT) is enhanced. Please refer to Appendix 4.
39. [FEATURE ENHANCED] C/I command, "ipsec display <rule index>" to display IPSec rules.
40. [FEATURE ENHANCED] C/I command, "ip nat incike <on|off>", to increase IKE source port. This is used in NAT pass-through.
41. [FEATURE ENHANCED] Remote Management Control mechanism now log "Access denied" messages into system log.
42. [FEATURE ENHANCED] Remote Management Control Web pages is ready.
43. [FEATURE ENHANCED] Static DHCP table Web pages is ready.
44. [FEATURE ENHANCED] Trigger Port Web pages is ready.
45. [FEATURE ENHANCED] Trafic Redirect Web pages is ready.
46. [FEATURE ENHANCED] Brand new Firewall Web pages is ready. There are 9 directional ACL sets; For packets originating from LAN to LAN(ZyWALL included)/WAN/DMZ, from WAN to LAN/WAN(ZyWALL included)/DMZ and from DMZ to LAN/WAN/DMZ(ZyWALL included).
47. [FEATURE CHANGED] Default ACL rules - "BOOTP client" and "IKE" pass through are moved from ACL set #2(WAN to LAN) to ACL set #8(WAN to WAN).
48. [FEATURE CHANGED] Dynamic rules will not conflict with static rules. Static rules have higher priority, and will be chose during runtime IKE procedure.
49. [FEATURE CHANGED] The repeated entries showed in VPN LOG are reduced.
50. [FEATURE CHANGED] Content filter and VPN Web pages are modified.
51. [FEATURE CHANGED] Wording consistency in Web GUI and SMT.
52. [BUG FIXED] Out-of-range error in Firewall Web pages.
53. [BUG FIXED] Custom Port Web pages is buggy.
54. [BUG FIXED] System crash after changing password.
55. [BUG FIXED] Fragmentation problems have been fixed, including teardrop, full feature NAT and ACL block.
56. [BUG FIXED] When ZyWALL as RESPONDER, it will accept all PFS setting from INITIATOR and does not check its own configuration.
57. [BUG FIXED] Notify message <No proposal chosen> has incorrect format.
58. [BUG FIXED] PFS mechanism has race condition. When two peers start to re-key simultaneously, sometimes one side will reject the connection.
59. [BUG FIXED] Packets to LAN should not match a rule whose remote IP range is "all".
60. [BUG FIXED] When rules configured as SUBNET, checking NAT full feature mapping with VPN failed.
61. [BUG FIXED] Web has wrong characters in ADVANCE page under Netscape 6.x.
62. [BUG FIXED] Enlarge memory parameters to assure there are enough memory for

system operation after VPN tunnels are built.

63. [BUG FIXED] After enable SUA, remote management to LAN IP via VPN tunnel failed.
64. [BUG FIXED] Connectivity Monitor may trigger PPTP dial by accident.
65. [FEATURE CHANGED] Missing Attack Atert and DoS Thresholds Web pages.
66. [BUG FIXED] Web GUI fail to setup Dial Backup, and make crash cycle.
67. [BUG FIXED] Incomplete function in Firewall Custom Port Web pages.
68. [BUG FIXED] Unfriendly operations in menu 15.3.
69. [BUG FIXED] Unfriendly operations in SUA/NAT Address Mapping Web pages.
70. [BUG FIXED] Log displaying mechanism may require additional keypress.
71. [FEATURE ENHANCED] Add new predefined service port AUTH, SYSLOG, and NEW-ICQ into Firewall Web pages.
72. [BUG FIXED] Dial-backup route may lost data, which makes FTP or HTTP fail sometimes.
73. [FEATURE ENHANCED] Add "Hide ESSID" in menu 3.5.
74. [BUG FIXED] Missing default setting (IKE UDP packets pass firewall)
75. [FEATURE ENHANCED] Send IPSec VPN logs to syslog server.
76. [FEATURE ENHANCED] More friendly error messages when SMTP client failed to send e-mail.
77. [FEATURE ENHANCED] Add C/I command "ipsec dial <#rule>", which can be used to trigger IPSec tunnel establishment.
78. [BUG FIXED] menu 11 cannot delete Dial-backup remote node, a nonactive zombie still there.
79. [BUG FIXED] menu 27.1.1 may persist claiming address conflict even mis-configuration has been corrected.
80. [FEATURE CHANGED] Because NetBIOS over TCP/IP (NBT) packet filter is hard-coded now, the factory default filters in menu 21.1 are all removed.
81. [BUG FIXED] Using CLI or Web configurator to configure ACL rules may result inconsistency.
82. [BUG FIXED] Old ROMFILE may result crash.
83. [BUG FIXED] Fail to edit LAN⇔WAN ACL rules via Web configurator.
84. [BUG FIXED] Fail to probe ill-behavior analog modem or ISDN TA.
85. [FEATURE CHANGED] Wireless LAN is back online.
86. [BUG FIXED] menu 15.3 trigger port forward is ready.
87. [BUG FIXED] menu 12 support 12 static routes.
88. [FEATURE CHANGED] default metric value of traffic redirect and dial-backup is changed to 15.
89. [FEATURE CHANGED] When ZyWALL plays as RESPONDER, it will delay 10 packets to start initiating the re-key procedure, if the INITIATOR does not re-key during the period.
90. [BUG FIXED] Transmitting phase-2 DEL packets during the IKE procedure should wait until the IKE finished.
91. [BUG FIXED] Race condition in NAT module may result crash.
92. [BUG FIXED] Fail to route tunneled packets.
93. [BUG FIXED] Compatibility issue. Fail to drop analog modem/ISDN TA.
94. [BUG FIXED] Fail to detect PPTP connectivity failure.

95. [NEW FEATURE] NetBIOS over TCP/IP (NBT) packet filter is hard-coded now. A set of C/I command is available:
    95.1 To enable/disable triggering dial by NBT packets:
    95.2 sys filter trigdial [on/off] , default is off
    95.3 To block/forward NBT packets
    95.4 sys filter blocknb [on/off] , default is on
    95.5 To make changes permanent, please edit autoexec.net
96. [ENHANCEMENT] Support 12 static routes.
97. [ENHANCEMENT] Add 3rd DNS and WINS server for DHCP server option. We add two C/I commands, "ip dhcp <iface name> server <dns server>" and "ip dhcp <iface name> server <wins server>" to add server IP.
98. [ENHANCEMENT] Add a switch to control NAT IRC service turned on/off. We provide a new C/I command "ip nat service irc <on|off>" to control the service.
99. [ENHANCEMENT] VPN LOG will show detail notify message type.
100. [FEATURE CHANGED] IPSec-related C/I commands are visible.
101. [FEATURE CHANGED] When peer's ID is single for dynamic rule, SA monitor will show a single address.
102. [BUG FIXED] After long time test, IPSec process will cause system lack of memory.
103. [BUG FIXED] Phase 1 time out in dynamic rule will delete runtime SPD and then tunnel fails.
104. [BUG FIXED] Only local ID being the same with remote ID can dynamic rule work.
105. [BUG FIXED] Dynamic SPD will be deleted during re-key procedure and cause tunnel down.
106. [BUG FIXED] Re-key-procedure will use wrong SA lifetime value.
107. [BUG FIXED] Under PPPoE connection, tunnel is built but no traffic can pass through it.
108. [BUG FIXED] Web a SUA/NAT behavior is wrong.
109. [BUG FIXED] "ip nat reset enif1" don't work.
110. [BUG FIXED] Firewall will check back-record for the TRACEROUTE reply to port unreachable of ICMP at the end host.
111. [BUG FIXED] Static routed packets from LAN to LAN will be blocked by firewall.
112. [BUG FIXED] Solve the SNMPv1 vulnerability problem.
113. [BUG FIXED] After using SMT to change password, WEB login procedure will fail.
114. [FEATURE CHANGED] Phase 1 SA will time out. And its lifetime is independent from phase 2 SA lifetime.
115. [BUG FIXED] Remote management from web cannot use port other than 80.
116. [BUG FIXED] Sometimes packets cannot pass through tunnel built from dynamic rule.
117. [BUG FIXED] SUA/NAT configuration in WEB is incorrect.
118. [BUG FIXED] Routing cache calculation will overflow.
119. [ENHANCEMENT] After a packet is processed IPSec and going to be transmitted, it can be applied IPSec again. We provide C/I commands to control which destination side can be applied IPSec. They are "ipsec route wan / lan".
120. [ENHANCEMENT] Add IPSec parser in C/I command, "sys trcpacket parse".
121. [ENHANCEMENT] Add SNMP link UP / DOWN trap for channels.
122. [FEATURE CHANGE] IPSec related SMT and WEB wording changed.

123. [FEATURE CHANGED] IPSec MyIP and secure gateway address can be set to 0.0.0.0 at the same time.
124. [FEATURE CHANGED] IPSec support LAN IP as MyIP.
125. [FEATURE CHANGED] DHCP packets will not run into IPSec process.
126. [BUG FIXED] Manual key cannot swap from one rule to another, if these two rules have the same secure gateway.
127. [BUG FIXED] When two peers initiate connections at the same time in some special cases, the two peers will reject each other and on tunnel can be established.
128. [BUG FIXED] When building the tunnel, sometimes system will crash.
129. [BUG FIXED] Provide online help for IPSec ADVANCE page in WEB.
130. [ENHANCEMENT] Support phase 2 ID: SINGLE / RANGE / SUBNET.
131. [ENHANCEMENT] Support using domain name as secure gateway address. We will periodically update peer IP according to the domain name. We provide two new C/I commands: "ipsec timer update_peer" and "ipsec updatePeerIp". The former is to set the interval for updating, and the latter is to force system update right away.
132. [ENHANCEMENT] Different rules can connect to the same secure gateway. However, there are some criteria for these rules, please refer to Appendix 2.
133. [ENHANCEMENT] Multiple dynamic rules are supported. There is no ordering issue for these dynamic rules.
134. [ENHANCEMENT] Web configurator can modify phase 1 algorithms through ADVANCE page.
135. [ENHANCEMENT] Add two C/I commands : "ppp lcp echo time" and "ppp lcp echo retry" to control echo timer and retry counts. Set one of them to 0 will disable echo request.
136. [ENHANCEMENT] Add remote management for support SNMP and DNS.
137. [FEATURE CHANGE] C/I commands for ipsec such as "ipsec sa" and "ipsec sa_sdb_status" are removed. To show SA status, we provide C/I command "ipsec show_runtime sa".
138. [NEW FEATURE] Add SNMP and DNS access control. For more information, please refer to Appendix 1
139. [NEW FEATURE] Add Trigger Port support. For more information, please refer Appendix 2.
140. [NEW FEATURE] Add a new C/I command:
141. ip aliasdis [on/off], , enable/disable routing between alias.
142. [ENHANCEMENT] Add Custom, Static DDNS domain name support.
143. [BUG FIXED] PPPOE cannot re-connect if previous disconnection time took too long
144. [NEW FEATURE] Add Internet Connectivity Monitor, Traffic Redirect and Dial-backup feature. For more information, please refer to Appendix 3.
145. [BUG FIXED] eWc spoof the fake LAN MAC address fail.
146. [ENHANCEMENT] Add SNMP linkup and linkdown trap of enet0, enet1, poe0, pns0 channel.
147. [BUG FIXED] Menu 22 SNMP trap configurations need to reboot system to become effective.
148. [ENHANCEMENT] Change eWC help pages format.
149. [ENHANCEMENT] Add C/I command to support the remote node option setting

feature:

149.1 sys rn load <entry no.> , load instruction
149.2 sys rn disp <entry no.> , display instruction (0:working buffer)
149.3 sys rn nat <none|sua|full_feature> , NAT setting instruction.
149.4 sys rn nailup <no|yes> , Enable/Disable NAIL-UP feature.
149.5 sys rn save <entry no.> , save instruction.

150. [BUG FIXED] Bug fix for multi-IPSEC Pass through problem
151. [BUG FIXED] Fix DHCP duplicated entries bug.
152. [BUG FIXED] Fix DNS server IP address runtime value will be cleaned.

Modifications in V 3.50(WB.3) | 01/22/2002

1. [BUG FIXED] PCI bus broken master at A0-AA/AB/AC board.
2. [ENHANCEMENT] RTL8139C(+) driver throughput.
3. [ENHANCEMENT] RTL8139C(+) driver stability.
4. [BUG FIXED] memory leak in IPSec VPN connections.
5. [ENHANCEMENT] RTL8139C(+) test OK in HTP.
6. [ENHANCEMENT] RTL8139C(+) Driver.

Modifications in V 3.50(WB.2) | 12/10/2001

1. [ENHANCEMENT] RTL8139C Driver reliability.

Modifications in V 3.50(WB.1) | 11/27/2001

1. [ENHANCEMENT] A connection from DMZ to the system's itself WAN address should be checked by firewall access control rule.
2. [FEATURE CHANGED] IPSec-VPN phase 1 SA algorithm was default to DES-MD5 via web configurator, user should change it via SMT if needed.

Modifications in V 3.50(WB.0) | 11/26/2001

1. [ENHANCEMENT] A connection from WAN to the system's itself DMZ address should be checked by firewall access control rule.
2. [BUG FIXED] SMT 24.11 fail to control connections from WAN using LAN/DMZ IP (or alias) addresses.
3. [BUG FIXED] System crash if time calibration fails.
4. [BUG FIXED] In web configurator DMZ pages, some default values mess-up.
5. [BUG FIXED] SMT 24.11 fail to control connections from WAN using LAN alias IP addresses.
6. [BUG FIXED] ICMP echo/reply message from WAN can pass through NAT/SUA if the destination address is an ILA.
7. [BUG FIXED] Firewall ACL will not apply to IPALIAS address.
8. [FEATURE CHANGED] Do not provide DHCP server on DMZ .
9. [BUG FIXED] C/I command "sys ddns disp" sometimes make crash.
10. [BUG FIXED] Setup DMZ via web configurator, then switch to SMT 5.2, an error message will claim missing required field.
11. [ENHANCEMENT] Support IP multicast on DMZ
12. [BUG FIXED] Alternative stress test by Smartbit 2000 make MAC chip block
13. [BUG FIXED] With PPPoE/PPTP, connections from DMZ can not reach WAN.

14. [BUG FIXED] When an (via telnet/web) administrator doing something for a long time or waiting for interactive operation, an (via console) administrator would fail to kick out the former one gracefully but a system reset will be triggered. The following cases match the criterion:
    14.1 Waiting on SMT 24.10
    14.2 Waiting on log displaying
    14.3 Waiting on interaction operation, e.g. waiting for "Y" or "N"
15. [BUG FIXED] Fail to change default route in web configurator.
16. [BUG FIXED] Applying missing filter (set #3).
17. [BUG FIXED] SMT 24.11 fail to control connections from DMZ
18. [BUG FIXED] Fail to access FTP server from LAN to DMZ.
19. [BUG FIXED] Web configurator (VPN / Content filter) cannot be accessed by Netscape 4.78
20. [BUG FIXED] With PPPoE / PPTP configured, but no dial-up, system would crash after typing "ip ro st" in C/I command mode.
21. [BUG FIXED] DNS proxy can't get the address when the original DNS server failed.
22. [BUG FIXED] After PPTP connection built, system would crash.
23. [BUG FIXED] When SNMP query through the system, it would crash.
24. [BUG FIXED] In SMT 24.6, interrupt the upload procedure would cause system crashed.
25. [BUG FIXED] Content filter configuration behavior modified. Configuration changes will not be saved unless press the "apply" button. "Reset" button will clear all configuration changes and reload the page.
26. [FEATURE CHANGED] When system crashes, it will not stop in the screen. Instead after showing memory dump, system will reboot automatically.
27. [ENHANCEMENT] In firewall setup, IKE (UDP:500) is placed in standard protocol instead of custom port. Default romfile changed.
28. [ENHANCEMENT] VPN logs and debug messages were modified to be much readable.
29. [ENHANCEMENT] When dynamic WAN-IP changes, system will disconnect all VPN connections which MyIP is "0.0.0.0".
30. [ENHANCEMENT] When VPN connection has no traffic through it for a period, it will disconnect automatically.
31. [ENHANCEMENT] Add two new C/I commands in "ipsec timer" to configure VPN timers.
32. [BUG FIXED] When firewall turns off and SUA only, PC in the WAN side can ping PCs in the LAN side.
33. [BUG FIXED] with PPPoE connection, WAN-to-LAN ACL will not be applied. Even a packet is allowed to be transferred from WAN to LAN, firewall will block it.
34. [BUG FIXED] When the WAN side is using PPPoE connection and NAT turns off, firewall does not protect the LAN side.
35. [BUG FIXED] When SA time out and reconnect, sometimes system will not free corresponding memory correctly. After a long connection, system will be exhausted.
36. [FEATURE CHANGED] Web status after saving configuration has changed to "Configuration updated successfully".
37. [FEATURE CHANGED] Only the last rule can apply security gateway to "0.0.0.0".

38. [FEATURE CHANGED] Web (SUA/NAT) default DMZ server changes to default server.
39. [BUG FIXED] When remote IP is too long, SA monitor will show incorrect layout.
40. [BUG FIXED] When phase 2 SA life time out, sometimes there exists a phase 1 SA and no tunnel can be built.
41. [BUG FIXED] Using Web to upgrade firmware, system will reply "internal error".
42. [BUG FIXED] VPN timeout re-connection function is not robust.
43. When "SA Life time" is time out, sometimes the VPN tunnel cannot be re-established again.
44. [BUG FIXED] VPN tunnel cannot be established if WAN IP is static without default gateway configured.
45. When a ZyWALL 10 / P312 is configured as "static IP" but default gateway as "0.0.0.0", and the other ZyWALL 10 / P312 is placed in the same subnet, the VPN tunnel cannot be established between them.
46. [BUG FIXED] VPN tunnel cannot work with multi-NAT.
47. [BUG FIXED] Web (VPN) pages are not consistent with SMT. SMT27.xx have been modified, but not Web pages.
48. [BUG FIXED] Use Web setup VPN for manual mode, it can not work until save in SMT again
49. [BUG FIXED] Web (Firewall) will show error messages when try to access help pages, which are not available now.
50. [ENHANCEMENT] Manual key SA will runtime creates when traffic matches SPD.
51. [ENHANCEMENT] SA monitor will show manual key SA, and command to delete it is available.
52. [ENHANCEMENT] Idle timer also applies on manual key SA. When no traffic transmits through the SA, system will delete it.
53. [ENHANCEMENT] VPN LOG is totally revised. Now it will show all IKE packets information. Besides, It will show error messages to identify the reason why connection cannot be built.
54. [ENHANCEMENT] IKE process in phase 2 will check ID information between system and the peer. If they don't match, i.e. both sites have different local / remote Addr setting, system will reject the connection and log in the VPN LOG.
55. [ENHANCEMENT] Simultaneous SA check: All VPN rules can be set to "ACTIVE", but only 10 runtime SA can be established at the same time.
56. [FEATURE CHANGED] Default idle timer value is set to 1 minute.
57. [BUG FIXED] Web (Content filtera EXEMPT ZONE) Apply button didn't work.
58. [BUG FIXED] VPN connection cannot be re-built after dynamic WAN IP being changed.
59. When one ZyWALL / P312 has "Secure Gateway IP Addr" to be "0.0.0.0" and the other one has "My IP Addr" to be "0.0.0.0", as below.

    59.1 ZyWALL #1 (security gateway IP 0.0.0.0) ← ZyWALL #2 (my IP 0.0.0.0)

    59.2 If ZyWALL #2 has been configured as "dynamic WAN IP", the VPN tunnel between ZyWALL 1 and ZyWALL 2 can be established at the first time. However, if ZyWALL 2 has its WAN ip changed, the VPN tunnel cannot be

re-built again.

60. Fix:
61. For the role of ZyWALL2, it periodically checks WAN IP, as long as IP changes, system will auto-disconnect tunnel. This will be logs in VPN Logs.
62. For the role of ZyWALL1, it periodically checks if any runtime SA has no traffic for a long time. If a SA has no traffic through it in 3 minutes, system will disconnect the tunnel.
63. There are two new C/I commands to configure 1) and 2). They are "ipsec timer chk_my_ip" and "ipsec timer chk_conn"
64. For the role of ZyWALL1, security gateway IP setting to be 0.0.0.0 can receive multiple requests at the same time. Appendix 1 is a simple configuration example.
65. [BUG FIXED] Can not download Content filter list
66. [BUG FIXED] IPSec-VPN settings in SMT menu was not saved to ROM
67. [ENHANCEMENT] Re-program 93C46 AGAIN to enhance RTL8139C's reliability.
68. [ENHANCEMENT] Users from LAN/WAN/DMZ can not use the same IP address (the global IP address which was usually resolved from FQDN) to access servers in LAN/DMZ when NAT/SUA was enabled.
69. [ENHANCEMENT] Re-program 93C46 to enhance RTL8139C's reliability.
70. [ENHANCEMENT] FLASH programming procedure was improved that it runs triple speed on Intel J3A series.
71. [BUG FIXED] All known crash issues.
72. [INTERNAL] Throughput (routing only) is about 20Mbps.
73. [BUG FIXED] System crashed by unusual IKE message
74. [BUG FIXED] IPSec configuration bugs
75. [ENHANCEMENT] Re-program 93C46
76. [ENHANCEMENT] Speed up IPSec DES engine
77. [ENHANCEMENT] Speed up FLASH writing process.
78. [ENHANCEMENT] System stability enhanced
79. [ENHANCEMENT] Throughput enhanced
80. [BUG FIXED] IPSec rule name disappear
81. [BUG FIXED] Console login didn't kick out web configurator
82. [BUG FIXED] Debug messages removed
83. [ENHANCEMENT] System stability enhanced
84. [NEW FEATURE] SA monitor was added in Web Configurator
85. [BUG FIXED] SMT menu 27.x.x.x mess-up
86. [BUG FIXED] Setup IPSec (rule 9) to Manual mode, ZW100 crash
87. [BUG FIXED] Configure IPSec in Manual mode, when starting establish an SA, ZW100 crash
88. [BUG FIXED] Use Web Reset to default rom file, although ZW100 has reboot, but configuration still not change
89. [BUG FIXED] Can not use web restore backup configuration file
90. [BUG FIXED] Firewall block LAN to DMZ traffic
91. [BUG FIXED] In web configurator, restoring default ROMFILE make ZW100 crash
92. [BUG FIXED] After remote node was deleted from menu 11, accessing menu 5 make ZW100 crash
93. [INTERNAL] BootBase was extended to 128KB

94. [INTERNAL] ROMFILE was extended to 256KB
95. [BUG FIXED] Use FTP upgrade Firmware, ZW100 will crash
96. [BUG FIXED] Can not use Web configurator upgrade firmware
97. [BUG FIXED] Annoy debug messages
98. [BUG FIXED] Make an VPN connection with ZyWALL10, ZyWALL10 will crash
99. [BUG FIXED] PPTP can not dial up
100. [BUG FIXED] Access Internet(WWW), ZyWALL100 crash
101. [BUG FIXED] Change menu 4 to PPTP,ZW100 crash
102. [BUG FIXED] Can ping LAN PC from the PC behind DMZ port
103. [BUG FIXED] Menu 24.5/24.6 fail
104. [BUG FIXED] HTP test AUX port, LINK/ACT LEDs don't work
105. [BUG FIXED] Web configurator failed on VPN page
106. [NEW FEATURE] IP police routes can be applied to LAN port in menu 3.2
107. [BUG FIXED] HTP test failed on LAN/WAN/DMZ items
108. [ENHANCEMENT] Wireless LAN bridge was enhanced.
109. [NEW FEATURE] IPSec VPN support 120 SAs

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. (LAN only/WAN only/DMZ only, Disable, 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) We **removed** the default TEL_FTP_WEB filter in Menu 11.5.
(2) The default value for Server access rule is **ALL**.
(3) Under the default setting: You can setup the Menu 15 to forwarding the server to LAN IP address. Thus you can configure the router through the WAN and you don't need to modify the server management or filter.

```
          Menu 24.11 - Remote Management Control

    TELNET Server:    Port = 23       Access = ALL
                      Secured Client IP = 0.0.0.0

    FTP Server:       Port = 21       Access = ALL
                      Secured Client IP = 0.0.0.0

    Web Server:       Port = 80       Access = ALL
                      Secured Client IP = 0.0.0.0

    SNMP server:      Port = 161      Access = ALL
                      Secured Client IP = 0.0.0.0

    DNS server:       Port = 53       Access = ALL
                      Secured Client IP = 0.0.0.0


               Press ENTER to Confirm or ESC to Cancel:
```

Appendix 2 Trigger Port

Introduction

Some routers try to get around this "one port per customer" limitation by using "triggered" maps. Triggered maps work by having the router watch ***outgoing*** data for a specific port number and protocol. When the router finds a match, it remembers the IP address of the computer that sent the matching data. When the requested data wants to come back ***in*** through the firewall, the router uses the port mapping rules that are linked to the trigger, and the IP address of the computer that "pulled" the trigger, to get the data back to the proper computer.

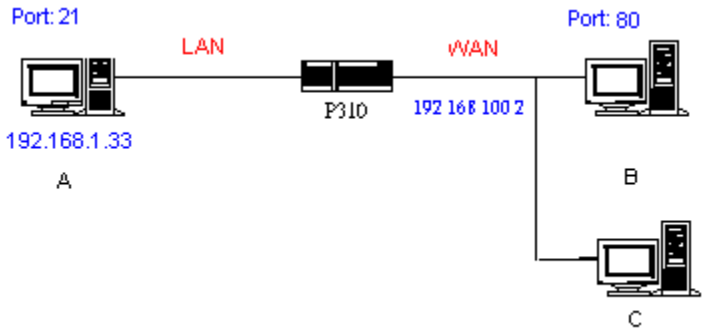
These triggered events can be timed so that they erase the port mapping as soon as they are done with the data transfer, so that the port mapping can be triggered by another Client computer. This gives the ***illusion*** that multiple computers can use the same port mapping at the same time, but the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

How to use it

Following table is a configuration table.

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

How it works



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

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

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

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

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

Notes

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

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

Appendix 3 Internet Connectivity Monitor, Traffic Redirect and Dial-Backup

Introduction

These features are used to keep Internet connectivity of the ZyWALL. The Connectivity Monitor is running at interval to detect if the ZyWALL can reach a desired host/address or the adjacent upstream gateway. Once the ZyWALL has detected the connectivity is broken, it tries to forward the traffic to another gateway that user has specified.

Menu 11.6 - Traffic Redirect Setup

```
              Menu 11.1 - Remote Node Profile

Rem Node Name= Normal_route   Route= IP
Active= Yes

Encapsulation= Ethernet       Edit IP= No
Service Type= Standard        Session Options:
Service Name= N/A             Edit Filter Sets= No
Outgoing:
  My Login= N/A               Edit Traffic Redirect= YES
  My Password= N/A
  Server IP= N/A

         Press ENTER to Confirm or ESC to Cancel:
```

```
            Menu 11.6 - Traffic Redirect Setup

          Active= No
          Configuration:
            Backup Gateway IP Address= 0.0.0.0
            Metric= 2
            Check WAN IP Address= 0.0.0.0
              Fail Tolerance= 0
              Period(sec)= 0
              Timeout(sec)= 0

         Press ENTER to Confirm or ESC to Cancel:
```

(1) Configure "Active" to "YES" if you want this feature work.
(2) "Backup Gateway". When the primary ISP or the check point is unreachable, traffic will be handed over to this backup gateway. [In IP address format]
(3) "Metric". Please reference section "**Metric**"
(4) "Check WAN IP Address". The Connectivity Monitor will probe the connectivity to a check-point. In general case, this check-point is the adjacent upstream gateway, which is typically assigned by ISP. However, if user desires to check a more significant point on the Internet, it can be specified here. A special case should be noticed that, even the ISP is online, this check-point maybe not reachable. The hand-over mechanism will function when the check-point failed. Leave it to 0.0.0.0, and the ZyWALL will take the upstream gateway as the default check-point.
(5) "Fail Tolerance" is the check failure upper limit. For example, if this value is 2. When ZyWALL failed to reach the check-point at the 3rd try, Connectivity Monitor will

invalidate the corresponding route and promote candidate to be the default route.

(6) "Period". The Connectivity Monitor will examine physical link signal and then probe the check-point at a interval of "period" seconds.

(7) "Timeout". The check-point is expected to response ZyWALL's probe within a reasonable time. After that, ZyWALL will log a failure. When the fail tolerance is exceeded, traffic will be handed over to the candidate route.

(8) The probing mechanism employs ICMP echo request/reply. Some hosts or routers on Internet may discard such packets.

Menu 2 - Dial-Backup Setup

```
                    Menu 2 - WAN Setup

               MAC Address:
                 Assigned By= Factory default
                 IP Address= N/A

               Dial-Backup:
                 Active= YES
                 Phone Number=
                 Port Speed= 115200
                 AT Command String:
                   Init= at&fs0=0
                 Edit Advanced Setup= No

          Press ENTER to Confirm or ESC to Cancel:
```

This menu setup the dial device, which is typically an analog modem or ISDN TA. To activate the dial device, please toggle "Avtive" to "YES".

Menu 11.1 - Backup ISP Setup

```
       Menu 11.1 - Remote Node Profile (Backup ISP)

Rem Node Name= Backup route  Edit PPP Options= No
Active= Yes                   Rem IP Addr= 0.0.0.0
                              Edit IP= YES
Outgoing:                     Edit Script Options= No
  My Login=
  My Password= ********       Telco Option:
  Authen= CHAP/PAP              Allocated Budget(min)= 0
  Pri Phone #= ?                Period(hr)= 0
  Sec Phone #=                   Nailed-Up Connection= No

                              Session Options:
                                Edit Filter Sets= No
                                Idle Timeout(sec)= 100

          Press ENTER to Confirm or ESC to Cancel:
```

A valid pair of login username and password is required. And the phone number of ISP is required. Leave "Rem IP Addr" to 0.0.0.0 makes ZyWALL try to get its IP

address from ISP.

```
        Menu 11.3 - Remote Node Network Layer Options

          Rem IP Addr= 0.0.0.0
          Rem Subnet Mask= 0.0.0.0
          My WAN Addr= 0.0.0.0

          Network Address Translation= SUA Only
          Metric= 2
          Private= No
          RIP Direction= Both
          Version= RIP-2B
          Multicast= None

            Enter here to CONFIRM or ESC to CANCEL:
```

Typically, "Network Address Translation" should be "SUA Only".

Metric

Once the traffic redirect and dial-backup mechanism were activated, ZyWALL will have 3 default routes to Internet. The first one is the normal route that designated by ISP or the static route mechanism; the second one is the traffic-redirect route (i.e. the backup gateway); the third one is the dial-backup route.

Customable metrics are provided in the menu 11.6 (Traffic Redirect) and menu 11.3 (Dial-backup) to determine the priority of the 3 default routes. For example, if the normal route has a metric "1" and traffic-redirect route has a metric "2" and dial-backup route has a metric "3", then the normal route is the first priority candidate to be the primary default route. If the normal route failed to get on Internet, the traffic-redirect route will be the successor. By the same theorem, dial-backup route is the successor after traffic-redirect route failed. For any two of the default routes match the same metric, a pre-defined priority is taken:

Normal route > Traffic-redirect route > Dial-backup route

For another example, if user want ZyWALL to use dial-backup route prior than traffic-redirect route or even the normal route, all need to do is to make metric of dial-backup route to be "1" and the others to be equal to "2" (or greater).

C/I commands

A set of C/I commands are provided.

(1) "ip tredir active [on/off]" to enable/disable traffic redirect.
(2) "ip tredir partner" IP address of the backup gateway.
(3) "ip tredir target" IP address of the check target.
(4) "ip tredir failcount" to setup fail tolerance.
(5) "ip tredir checktime" to setup checking period.
(6) "ip tredir timeout" to setup check timeout.
(7) "ip tredir disp" to show system value and run time value.
(8) "ip tredir save" will save the configuration.

Note

(1) Turn off "RIP" in SMT3.2 is recommended.
(2) When traffic redirect is turned on, and encapsulation type is PPPOE or PPTP, "Nail-UP" function in SMT11.1 will be enabled
(3) A useful WINDOWS commands "tracert" can be used to verify the packet routing.
(4) Connectivity Monitor can not be disabled. However, traffic redirect and dial-backup mechanism can be enabled/disabled independently.
(5) Because the primary ISP and the backup ISP may assign different WAN IP address to ZyWALL. When traffic have handed over from one ISP to the other, all exist connections may be forced to reconnect.

Appendix 4 Hard-coded packet filter for "NetBIOS over TCP/IP" (NBT)

Windows neighborhood by NetBIOS protocol is very convenient for sharing computers and Internet resources, but since it carries private data with plain text over the network, it is dangerous to use without any control. We designed a simple method to control the NetBIOS packet by ZyWALL series. By setting the filter flag, System administrator can easily control the NetBIOS packet. See the figure below.

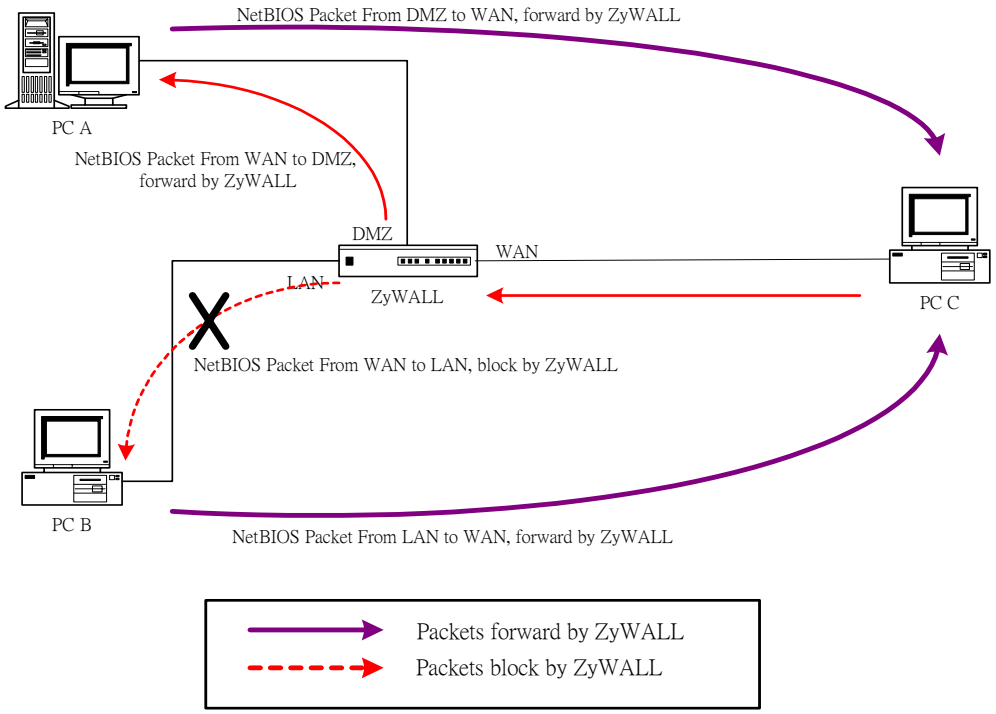


Fig 1. Using filter to block access from WAN to DMZ

PC A can find PC C, and PC B can find PC A, too. But, by the setting of NetBIOS filter, WAN to LAN NetBIOS packets will be blocked. So, PC C can find only PC A without PC B by windows neighborhood.

There are two situations we concerned about and the NetBIOS packet should be. We set the priority of VPN environment is higher than normal situation. So, packets encrypted by IPSec get top priority. See the following description.

- **Without VPN, IPSec unused and packets are not encrypted :**
  By ZyWALL 100, there are LAN port, WAN port and DMZ port on it. By configuration, we have six directions on it (LAN => WAN, LAN => DMZ, WAN => LAN, WAN => DMZ, DMZ => LAN and DMZ => WAN).See the figure below.

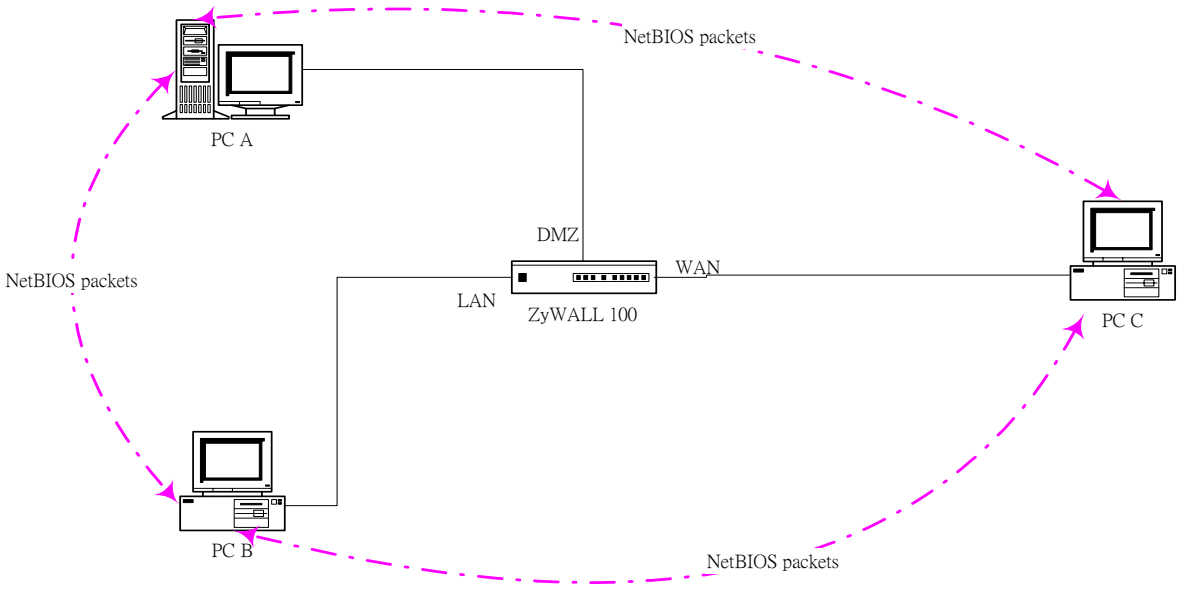


Fig 2. Without VPN, Using filter to block NetBIOS packet.

- **Using VPN, NetBIOS packets are encrypted by IPSec :**
  When VPN feature is enabled, all packets transmitted by tunnel are encrypted by IPSec. To conform the characteristic of VPN, we should ignore the setting of LAN, WAN and DMZ. If IPSec packets are defined to forward, we should pass the NetBios packets encrypted by IPSec. See the figure below

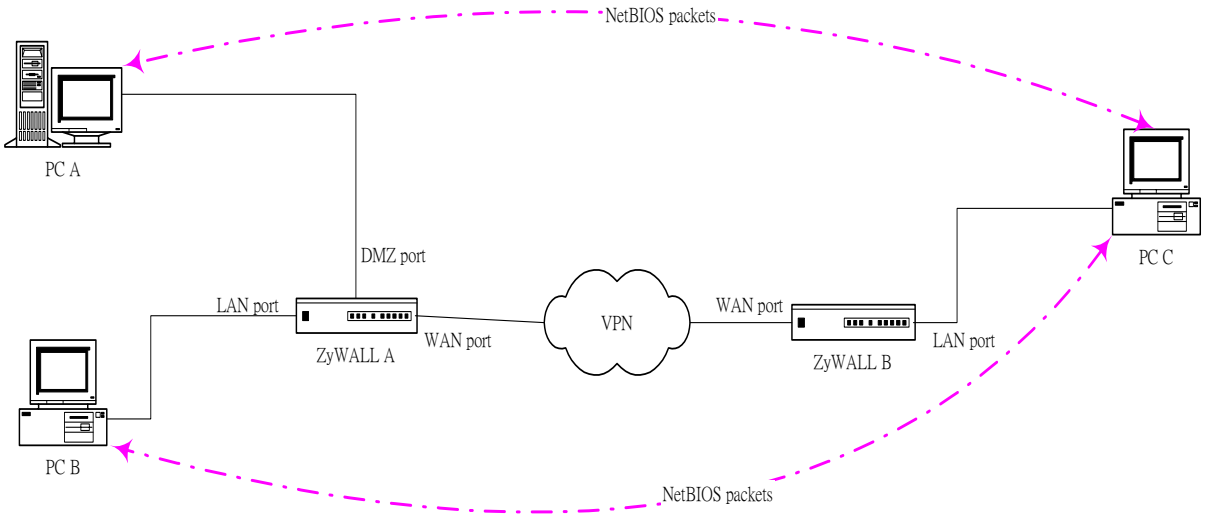


Fig 3 Using VPN connection between two ZyWALLs

- **User Interface Implementation :**
  1. Must provide user the ability to set the flag of forward/block NetBIOS packet with all directions(LAN => WAN , LAN => DMZ , WAN => LAN , WAN => DMZ , DMZ => LAN , DMZ => WAN).

2. Must provide user the ability to set IPsec packets forward/block.
3. Must provide user the ability to set Trigger Dial function enable/disable.

- **CI Commands :**
  In order to configure the NetBIOS filter, CI commands are enhanced for configure and display all status of NetBIOS filter. They are added under **sys filter netbios** category, and they are :

  1. **sys filter netbios disp**
     This function is used to display the NetBIOS filter status.
     Example output 1 : (without DMZ port supported)
     ========== NetBIOS Filter Status ==========

LAN to WAN:	Forward
WAN to LAN:	Forward
IPSec Packets:	Forward
Trigger Dial:	Disabled

     Example output 2 : (with DMZ port supported)
     ========== NetBIOS Filter Status ==========

LAN to WAN:	Forward
WAN to LAN:	Forward
LAN to DMZ:	Forward
WAN to DMZ:	Forward
DMZ to LAN:	Forward
DMZ to WAN:	Forward
IPSec Packets:	Forward
Trigger Dial:	Disabled

  2. **sys filter netbios config**
     For different products, CI commands help message may be different.
     Example 1 : (without DMZ port supported)

config <0:LAN to WAN, 1:WAN to LAN, 6:IPSec passthrough, 7:Trigger Dial> <on|off>

     Example 2 : (with DMZ port supported)

config <0:LAN to WAN, 1:WAN to LAN, 2:LAN to DMZ, 3:WAN to DMZ, 4:DMZ to LAN, 5:DMZ to WAN, 6:IPSec passthrough, 7:Trigger Dial> <on|off>

     This function is used to set the NetBIOS filter flag, the number of parameter accept just one configure. For example :
     Enable the function of "block packets" from WAN to LAN, use
     sys filter netbios config 1 on

The CI Commands can be summarized as the table shown below :

Root	Commands or Sub-directory	Commands or Sub-directory	Commands	Description
Sys	filter	Netbios		
			Disp	Display NetBIOS filter information.
			Config <0:LAN to WAN, 1:WAN to LAN, 2:LAN to DMZ, 3:WAN to DMZ, 4:DMZ to LAN, 5:DMZ to WAN, 6:IPSec pass through, 7:Trigger Dial> <on|off>	To set NetBIOS packets block/forward for all directions and IPSec packets pass through. For dial backup system function, index 7 is enable/disable Trigger Dial function.

Appendix 5 Traffic Redirect/Static Route/Policy Route Application Note

- **Why traffic redirect/static/policy route be blocked by ZyWALL**

ZyWALL is the ideal secure gateway for all data passing between the Internet and the LAN/DMZ. 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.

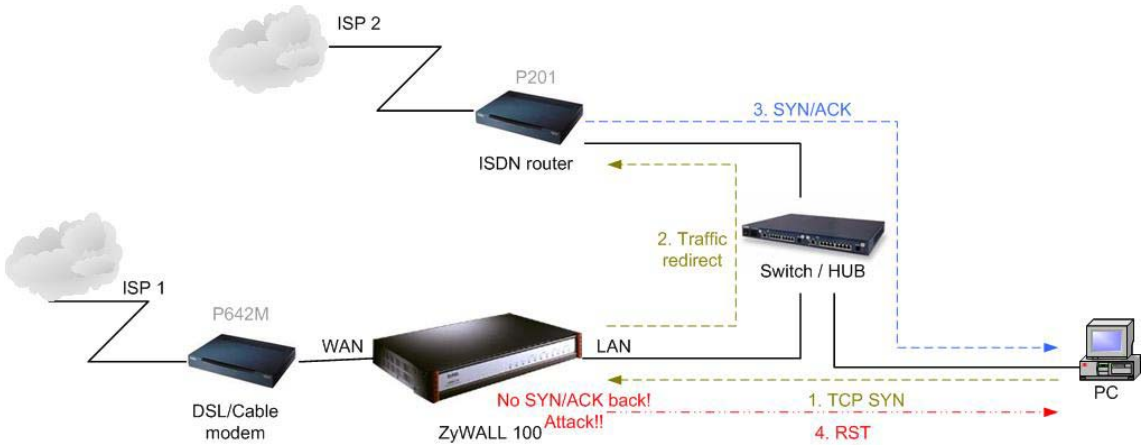


Figure 5-1 Triangle Route

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/policy 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.

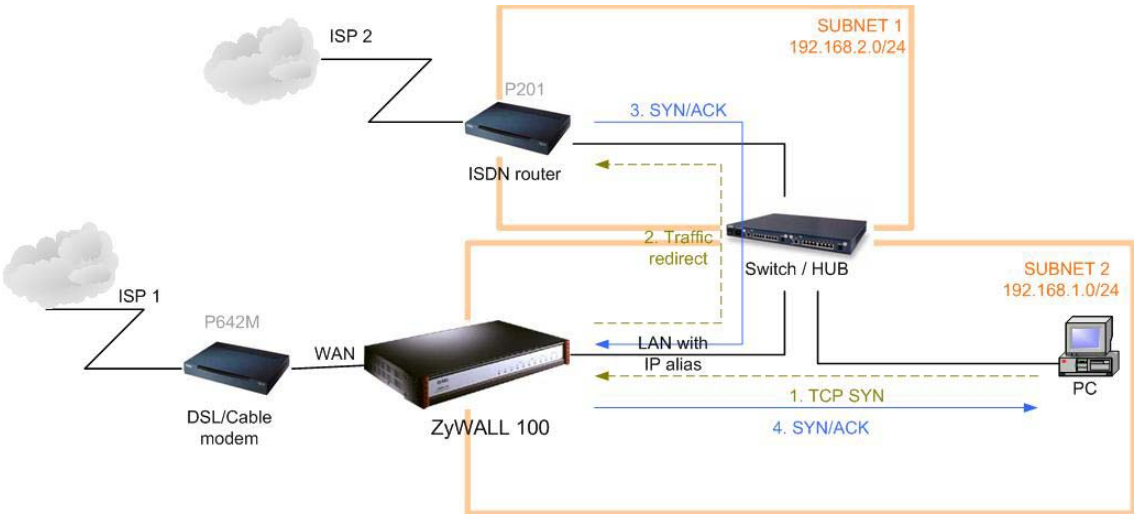


Figure 5-2 Gateway on alias IP network

(2) Gateway on WAN side

A working topology is suggested as below.

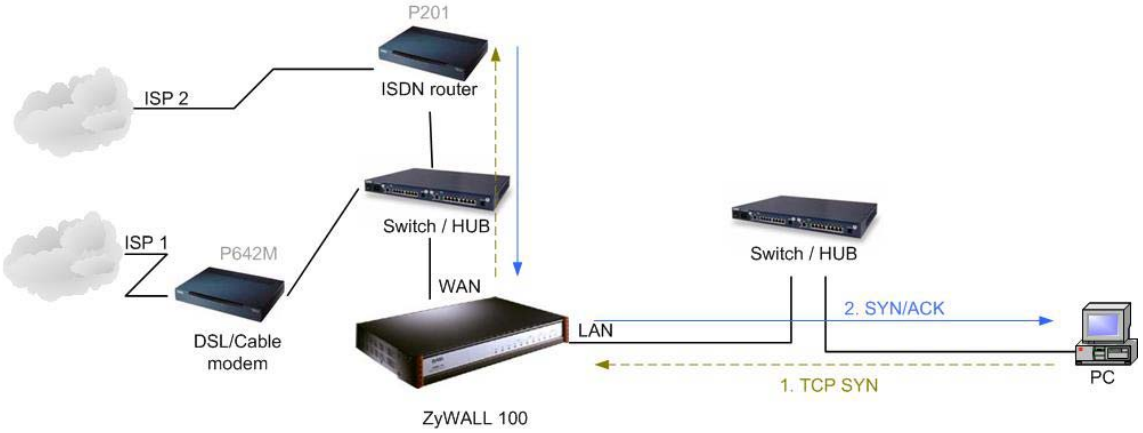


Figure 5-3 Gateway on WAN side

Appendix 6 WLAN can bridge with LAN/DMZ

The new C/I commands is "sys wlanbridge".

(1) ”sys wlanbridge” will display the syntax and which port is now bridged with WLAN.

(2) “sys wlanbridge lan/dmz” will set WLAN to bridge with LAN/DMZ. The setting will take effect after the system reboots.

Appendix 7 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”.

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

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

System Related Command Home

Command				Description
sys				
	adjtime			retrive date and time from Internet
			display	display cbuf static
	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]	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]	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		display all 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
	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]	
	rn			
		load	<entry no.>	load remote node information
		disp	<entry no.>(0:working buffer)	display remote node information
		nat	<none|sua|full_feature>	config remote node nat
		nailup	<no|yes>	config remote node nailup
		mtu	<value>	set remote node mtu
		save	[entry no.]	save remote node information
	smt			not support in this product
	stdio		[second]	change terminal timeout value
	time		[hour [min [sec]]]	display/set system time
	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

	wlanbridge	[lan|dmz]		set WLAN to bridge with LAN or DMZ.
	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		

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
		speed	<speed>	set ether data speed
		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

AUX Related Command Home

Command				Description
aux				
	atring		<device name>	Command the AT command to the device.
	cnt			
		disp	<device name>	display aux counter information
		clear	<device name>	clear aux counter information
	drop		<device name>	disconnect
	init		<device name>	initialize aux channel
	mstatus		<device name>	display modem last call status
	mtype		<device name>	display modem type

	netstat		<device name>	prints upper layer packet information
	rate		<device name>	show tx rx rate
	redirect		<device name>	invalid
	signal		<device name>	show aux signal

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
		attack	send-alert <yes|no>		Activate or deactivate the firewall DoS attacks notification emails
			block <yes|no>		Yes: Block the traffic when exceeds the tcp-max-incomplete threshold
					No: Delete the oldest half-open session when exceeds the tcp-max-incomplete threshold
			block-minute <0~255>		Only valid when sets 'Block' to yes. The unit is minute
			minute-high <0~255>		The threshold to start to delete the old half-opened sessions to minute-low
			minute-low <0~255>		The threshold to stop deleting the old half-opened session
			max-incomplete-high <0~255>		The threshold to start to delete the old half-opened sessions to max-incomplete-low
			max-incomplete-low <0~255>		The threshold to stop deleting the half-opened session

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

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

IP Related Command Home

Command				Description
ip				
	address		[addr]	display host ip address
	alias		<iface>	alias iface
	aliasdis		<0|1>	disable alias
	arp			
		status	<iface>	display ip arp status
	dhcp		<iface>	
		client		
			release	release DHCP client IP
			renew	renew DHCP client IP
		status	[option]	show dhcp status
	dns			
		query		
		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.
	udp			
		status		display udp status
	rip			
	sidepath			
		clear		clear side path
		disp		display side path
		set	<iface> <gateway>	set side path
	tcp			
		status	[tcb] [<interval>]	display TCP statistic counters
	telnet		<host> [port]	execute telnet clinet command
	tftp			
	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
	forceproxy		<display|set> [on|off] [servicePort] [proxyIp] [proxyport]	enable TCP forceproxy
	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 [filterList/disableAllExceptTrusted/ unblockRWFToTrusted/keywordBlo ck/fullPath/caseInsensitive/fileNam e][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
	rpt			
		start		start report
		stop		stop report
		url	[num]	top url hit list
		ip	[num]	top ip addr list
		srv	[num]	top service port list
	nat			
		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
		service		
			irc [on|off]	turn on/off irc flag
		resetport		reset all nat server table entries
		incikeport	[on|off]	turn on/off increase ike port flag
	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	dmz	<on|off>	After a packet is IPSec processed and will be sent to DMZ side, this switch is to control if this packet can be applied IPSec again.
				Remark: Only supported in ZyWALL100
		lan	<on|off>	After a packet is IPSec processed and will be sent to LAN side, this switch is to control if this packet can be applied IPSec again.
				Remark: Command available since 3.50(WA.3)
		wan	<on|off>	After a packet is IPSec processed and will be sent to WAN side, this switch is to control if this packet can be applied IPSec again.
				Remark: Command available since 3.50(WA.3)
	show_runtime	sa		display runtime phase 1 and phase 2 SA information
		spd		When a dynamic rule accepts a request and a tunnel is established, a runtime SPD is created according to peer local IP address. This command is to show these runtime SPD.
	switch	<on|off>		As long as there exists one active IPSec rule, all packets will run into IPSec process to check SPD. This switch is to control if a packet should do this. If it is turned on, even there exists active IPSec rules, packets will not run IPSec process.
	timer	chk_my_ip	<1~3600>	- Adjust timer to check if WAN IP in menu is

				changed
				- Interval is in seconds
				- Default is 10 seconds
				- 0 is not a valid value
		chk_conn.	<0~255>	- Adjust auto-timer to check if any IPsec connection has 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
		active	<Yes | No>	Set active or not
		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
	swSkipOverlapIp		<on|off>	When a VPN rule with remote range overlaps with local range, the switch decides if a local to local packet should apply this rule.

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
			triangle	Set if firewall ignore triangle route in lan/wan/dmz/wlan