ZyXEL

Firmware Release Note

ZyWALL 30W

Release 3.62(WN.0)

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

ZyXEL ZyWALL 30W Standard Version
Release 3.62(WN.0)
Release Note

Date: Feb, 26, 2004

Supported Platforms:

ZyXEL ZyWALL30W

Versions:

ZyNOS Version: V3.62(WN.0) | 02/26/2004
BootBase : V1.08 | 12/26/2003

Notes:

1. The setting of ignore triangle route is on in default ROM FILE. Triangle route network topology has potential security crisis. If you are not clear about it, please refer to Appendix for the triangle route issue.
2. 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.
3. 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.
4. When firewall turns from "off" to "on", the firewall initialization procedure will disconnect all connections running through the ZyWALL.
5. SUA/NAT address loopback feature was enabled on ZyWALL30W by default, however, if users do not need it, a C/I command "ip nat loopback off" could turn it off.
6. In WLAN configuration, a switch for enable / disable WLAN is added. The default value is "disable" since WLAN without any security setting is vulnerable. Please configure MAC filter, WEP and 802.1X when you enable WLAN feature.
7. ZyWALL A ----------NAT Router---------- ZyWALL B
   (WAN) (LAN)
   ZyWALL A has one VPN rule with NAT traversal on.
   ZyWALL B has two rules:
   Rule 1 is NAT traversal off, and wrong phase 2 SA parameters.
   Rule 2 is NAT traversal on, and other parameters are correct.
   When trigger VPN tunnel by ZyWALL A, tunnel will never be up.

Known Issues:

1. Sometimes on screen the “Local Area Connection” icon for UPnP disappears. The icon shows again when restarting PC.
2. The DHCP client in ZW LAN side may get an IP which is reserved by static DHCP. The situation will disappear if the client releases the IP and requests again.
3. eWC->WAN IP has bugs when WAN ISP is PPPoE or PPTP. Leaving some values in remote IP or remote masks for WAN IP and then switch to dynamic IP, ZyWALL cannot dial anymore.
4. If gateway in static route belongs to WAN interface and if WAN is PPPoE/PPTP encapsulation, 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.
5. When deleting a static route rule which its IP address = 0.0.0.0 and netmask = 0.0.0.0, the routing table's default route will be deleted.
6. Sometimes eWC→time zone page can’t be configured under IE 5.00.3315.
7. ZyWALL WLAN-802.1X can not connect with PC whose OS version is Windows XP SP1.
8. Sometimes message “SfsWriteFile: -1214” shows on screen after upgrade firmware to router.
9. When WAN is down, VPN tunnel will be fail with dial backup.

Restore to Factory Defaults Setting Requirement: No

Features:

Modifications in V3.62(WN.0) | 02/26/2004

1. Modify for formal release.

Modifications in V3.62(WN.0)b4 | 02/18/2004

1. [ENHANCEMENT] Remove CI command “ipsec config ike p1EncryKeyLen” because phase 1 AES just support key length with 128 bit.
2. [ENHANCEMENT] Add new CI command “ip arp period” to set up arp flash time.
3. [ENHANCEMENT] Add new CI command “ip arp force on|off”. When the user uses "ip arp force on", the age function of APR function will be disabled. That means even the ARP entry has been refered, the timer of it will not reset to 300 seconds, it will be still time out.
4. [BUG FIX] Symptom: IPSEC NAT Traversal doesn’t work.

Condition: When NAT Traversal is on, VPN tunnel won't be up because Initiator's phase 2 Encapsulation will change during negotiation.

5. [BUG FIX] Symptom: IPSec rule jumping is fail with NAT traversal.
   Condition:
   Initiator ----------NAT Router ----------Responder
   (1) Initiator has one rule with NAT Traversal on.
   (2) Responder has two rules:
       - Rule 1: NAT Traversal is on, and phase 2 ID is wrong.
       - Rule 2: NAT Traversal is off, and phase 2 ID is correct.
       - All other parameters in rule 1 and rule 2 are correct.
   (3) Dial tunnel from initiator. Responder will use rule 1 to start negotiate.
   (4) In phase 2, since phase 2 ID is wrong, responder will swap to rule 2 and eventually tunnel will be up because system won't check NAT Traversal flag when swapping the rule.
6. [BUG FIX] Symptom: When initiator receives wrong phase 1 ID from responder, it will jump to another rule.
   Condition: During IKE negotiation in Main mode, if responder's "Local ID Content" mismatches initiator's "Peer ID Content", initiator will do rule swap and choose another rule to negotiate.
7. [BUG FIX] Symptom: Symptom: Packets will not go through ZyWALL.
   Condition:
   (1) There is heavy traffic through router.
   (2) Sometimes PC A send a DNS query to outside DNS server, but the reply packet will be forwarded to another PC.
8. [BUG FIX] Symptom: When the Ethernet chip VT6105 operates under Half Duplex mode, its TX functionality might hang permanently due to severe collisions.
   Condition:
   ZyWALL A----------10 M Hub ----------ZyWALL B----------PC
   (WAN) (LAN)
   (1) Generate lot of packets and send from PC to ZyWALL A through ZyWALL B.
   (2) After few minutes, ZyWALL A may permanently fail to transmit packets.

Modifications in V3.62(WN.0)b3 | 02/09/2004

1. [FEATURE CHANGE] Change NAT session number to 2048.
2. [FEATURE CHANGE] Change rule number in eWC→SUA/NAT→SUA Server to 30.
3. [BUG FIX] Symptom: eWC→SUA/NAT→SUA Server: rules can't be saved.
   Condition: When saving rules in eWC→SUA/NAT→SUA Server, in "Status" shows " End port must greater than Start port!" and rule can't be saved.
4. [BUG FIX] Symptom: There are many logs show on eWC→Log when firewall is on.
   Condition: When firewall is on, log "Unsupported/out-of-orderICMP:ICMP (type:11, code:0)" shows on log." shows on eWC→Log many times.
5. [BUG FIX] Symptom: X-Auth configuration check is always activated when configure VPN rule by GUI.

Condition: In eWC→VPN→Rule Setting: un-check "Enable Extended Authentication" and select "Client mode". When saving the rule, message "Both User Name and Password are required" shows on "Status" and rule can't be saved.

6. [BUG FIX] Symptom: System crashes after several days.
   Condition: When ZyReport is on, system may crashes with huge dump after several days.
7. [BUG FIX] Symptom: System may crash when use CI command "wlan active".
   Condition: Use CI command "wlan active X" in which X > 1, system will crash.
8. [BUG FIX] Symptom: ZyWALL can't establish VPN tunnel with SoftRemote.
   Condition: When ZyWALL set up a VPN tunnel with SoftRemote version 10.0, and activates X-Auth, tunnel can't be up.
9. [BUG FIX] Symptom: DDNS doesn't work.
   Condition: When set DDNS by check "Server Auto Detect", device can't update host name.

Modifications in V3.62(WN.0)b2 | 01/14/2004

1. [ENHANCEMENT] Content filter supports to block two kinds of special URL.
   (1) URL has the '@' sign. For example, http://zyxel@209.247.228.201
   (2) IP address is transferred to decimal. For example, http://209.247.228.201 ==> http://3522684105
2. [FEATURE CHANGE] In eWC→SUA/NAT→SUA Server: expend the number of rules from 11 to 29.
3. [BUG FIX] Symptom: Web help pages are not correct.
   Condition: Web help pages in Certificate, Content Filter, Firewall and NAT/SUA are not correct.
4. [BUG FIX] Symptom: Default certificate is wrong.
   Condition: In default certificate, the content includes product name which should be "ZyWALL 30 W". But ZyWALL 30 W's default certificate it is "ZyWALL 10 W".
5. [BUG FIX] Symptom: eWC→MY Certificate→Detail→ Certificate in PEM (Base-64) Encoded Format: the certificate will be fragmented.
   Condition:
   (1) eWC→MY Certificate→Detail→ Certificate in PEM (Base-64) Encoded Format: the certificate will be fragmented into 64 character per line.
   (2) eWC→Trust CAs→Detail and eWC→Trust Remote Hosts→Detail also have such problem.
6. [BUG FIX] Symptom: NAT session will be full even the number of session is not used.
   Condition: In some cases when NAT sessions are used, they won't be released.
7. [BUG FIX] Symptom: VPN tunnel can be up even PFS is not correct.
   Condition:
   (1) Initiator chooses "DH1" as PFS type in VPN rule.
   (2) Responder chooses "DH2" as PFS type in VPN rule.
   (3) Trigger the VPN tunnel and the tunnel can be up.
8. [BUG FIX] Symptom: "Peer ID Type" in Menu 27.1.1 doesn't work correctly.

Condition:
(1) Go to Menu 27.1.1, default setting in “Peer ID Type” is IP.
(2) In Menu 27.1.1, choose “Peer ID Type” as DNS.
(3) Go to Menu 27.1.1.1
(4) Go back to Menu 27.1.1, now “Peer ID Type” will become IP again.

Modifications in V3.62(WN.0)b1 | 12/31/2003

1. [ENHANCEMENT] Add new feature: X-Auth as the authentication method in VPN IKE phase.
2. [ENHANCEMENT] Support rule swapping by phase 1 ID (Local ID type / content and Peer ID type / content) in IPSec.
3. [ENHANCEMENT] Add HTTPS proxy server support.
4. [ENHANCEMENT] When restore default ROM file in SMT, system will ask users to reconfirm.
5. [ENHANCEMENT] Add new feature: PKI supported in VPN.
6. [ENHANCEMENT] Add new feature: WLAN 802.1X TLS/TTLS.
7. [ENHANCEMENT] Add new feature: SSH.
8. [ENHANCEMENT] Add new feature: Support new encryption algorithm AES in IPSec.
9. [ENHANCEMENT] Add new feature: Bandwidth Management Light.
10. [ENHANCHMENT] Add new eWC firewall rules storage space utilization status bar in summary page.
    Previous: We used firewall rule numbers to count the usage space, but the rule size is depended on content (like IP pairs and total service numbers). The rule size is different from rule to rule.
    Now: We ignored the counter of firewall rules and just care of the remained size we can use.
11. [ENHANCEMENT] Add more information in CI command "ipsec disp #rule". If the secure gateway of an IPSec rule is configured as domain name, this command will show both domain and actual IP resolved by system.
12. [ENHANCEMENT] Add new feature: In content filer, use Cerberian to replace Cybernot.
13. [ENHANCEMENT] Add new feature: DNS Server for IPSec VPN. Please refer to Appendix 6 for detail.
14. [ENHANCEMENT] Add CI command "ip dropIcmp [0|1]"(default value is 0) to setup the device to drop ICMP fragment packets.
15. [ENHANCEMENT] Add two new categories "TCP Reset" and "Packet Filter" in Centralized Log.
16.
17. [ENHANCEMENT] Separate DNS servers into system DNS servers & DNS servers assigned to LAN hosts. The system DNS servers are used by router and the DNS servers assigned to LAN hosts are for LAN hosts. There will be no embedded default DNS server for this design.
18. [ENHANCEMENT] Add CI command "sys upnp reserve [0|1]"(default value is 0) to

reserve UPnP NAT rules in flash after system boot up.

19. [ENHANCEMENT] Add UPnP "Ports" page to show the UPnP NAT ports.
20. [ENHANCEMENT] IPSec related logs are enhanced.
    (1) Add success log and error messages in IKE in centralize log .
    (2) Add new IPSec debug log method.
21. [ENHANCEMENT] Add dynamic local and dynamic remote in IKE/IPSec. There are two CI commands, "ipsec config dynamicLocal" and "ipsec config dynamicRemote", to configure these two features.
    (1) When dynamic local turns on, My IP Addr = 0.0.0.0, Local Addr Type = single, Local Addr Start = 0.0.0.0, ZyWALL will use WAN IP as local address.
    (2) When dynamic remote turns on, secure GW = domain name, Remote Addr Type = single, Remote Addr Start = 0.0.0.0, ZyWALL will use IP resolved from peer domain name as remote address.
22. [ENHANCEMENT] Add new category "PKI" in Centralized Log.
23. [ENHANCEMENT] Add Local ID Type, Local ID Content, Remote ID Type, and Remote ID Content check when using RSA signature in IKE.
    (1) When using RSA signature, we can not set Local ID Type and Local ID content from UI. The Local ID Type and Local ID content depends on the certificate we select.
    (2) When using RSA signature, we can set and check Remote ID Type and Remote ID Content. There are two type added, one is "Subject Name" and the other is "Don't Care". The "Subject Name" measn we will check peer ID content using peer's certificate subject name. And "Don't Care" means that we won't chech peer's ID content when we receive it.
24. [FEATURE CHANGE] Add a new item “CERTIFICATES” in panel, and remove certificate related subjects in VPN rule editing page.
25. [FEATURE CHANGE] Enlarge number of rules in eWC→SUA/NAT→SUA Server to 19.
26. [FEATURE CHANGE] In eWC->CONTENT FILTER->Categories, change the wording of button from "Registration and Reports" to "Register".
27. [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.
28. [BUG FIX] When setting SA lifetime less than 180 seconds, the rule still can be saved.
29. [BUG FIX] Symptom: Firewall policy log is not correct.
    Condition: In eWC→LOGS, if the firewall policy is WAN to WAN/ZyWALL, router will show “W to W/P” which should be “W to W/ZW”.
30. [BUG FIX] Symptom: eWC→VPN→SA Monitor: SA status is not correct.
    Condition: In eWC→VPN→SA Monitor, when phase 2 encryption is NULL, eWC→VPN→SA Monitor->IPSec Algorithm shows “ESP ???—SHA1” in which “???” should be “NULL”.
31. [BUG FIX] Symptom: Device reboots when WAN is up/down for several times.
    Condition: After up/down WAN for several times in SMT menu 24.1, system will

crash.

32. [BUG FIX] Symptom: System may crash or can't login by GUI when traffic is heavy in LAN.
    Condition: When traffic is heavy in LAN, we may not login system or system may crash.
33. [BUG FIX] Symptom: VPN tunnel can be up, but data can't transmit.
    Condition: ZyWALL 30 W can set up VPN tunnel with peer, but data can't be transmit through the tunnel.
34. [Bug FIX] Symptom: Modified wording in GUI and SMT.
    Condition: Modify following wording in GUI and SMT:
    (1) eWC→VPN→Rule Edit: Authentication Key is modified as Authentication Method.
    (2) In SMT 27.1.1.1, there are two selections in "Authentication method": Pre-shared Key and Certificate.
    (3) In SMT 27.1.1.1, change "PSK" field name to "Pre-shared Key".
    (4) eWC→Content Filter→Categories: Change "Enable Web Site Categories" to "Enable External Database Content Filtering".
    (5) eWC→Content Filter→Categories: Change "Matched Web Sites" to "Matched Web Pages".
    (6) eWC→Content Filter→Categories: Change "Unrated Web Sites" to "Unrated Web Pages".
35. [BUG FIX] Symptom: eWC→VPN→Rule Edit→Local: "Ending IP address / Subnet Mask" should be gray out when Local Address type is Single.
    Condition: eWC→VPN→Rule Edit→Local: "Ending IP address / Subnet Mask" is writable when choosing Local Address Type as Single Address.
36. [BUG FIX] Symptom: When using CI command ip nat iamt with wrong parse, the system will reboot.
37. [BUG FIX] Symptom: Upload ROM file or RAS fail when console is disconnected.
    Condition: When using GUI to upload ROM file or RAS, and he console is disconnected, system won't restart after ROM file or RAS is uploaded.
38. [BUG FIX] Symptom: For VPN SMT setting, phase 1 ID is not correct.
    Condition:
    (1) Set VPN ID type as IP then save
    (2) Change ID type as DNS → go to menu 27.1.1.1 → back to menu 27.1.1, we will find the ID will be changed to IP.
    (3) If we save the type as IP then try to clear content will fail.
39. [BUG FIX] Symptom: When client PC is Windows NT 4.0 or Linux, system may crash.
    Condition: When client PC's OS is NT 4.0 or Linux, and request IP from ZyWALL, ZyWALL may crash.
40. [BUG FIX] Symptom: In AUX mode router can't start normally when connect with USR modem in console.
    Condition: When connecting with USR modem by console, router won't be able to start up in AUX mode.
41. [BUG FIX] Symptom: User cannot set the static route rule in SMT 12.1.
    Condition:

(1) Enter SMT 12.1.
(2) Set destination IP address as 1.1.1.1, IP subnet mask as 255.255.0.0, and gateway IP address as 1.2.1.1

42. [BUG FIX] Symptom: NAT table is full.
Condition: NAT sometimes may be full and will cause system crash.

Modifications in V3.61(WN.2) | 09/24/2003

Modify for formal release.

Modifications in V3.61(WN.2)b3 | 09/03/2003

1. [BUG FIX] Symptom: Router doesn't restart after upload f/w or ROM file in AUX mode.
Condition:
(1) Switch to AUX mode.
(2) Disconnect router's console port.
(3) Upload f/w or ROM file by web.
(4) Router doesn't reboot unless router's console port is connected.

Modifications in V3.61(WN.2)b2 | 08/27/2003

1. [BUG FIX] Symptom: Router doesn't restart after upload f/w or ROM file.
Condition:
(1) Disconnect router's console port.
(2) Upload f/w or ROM file by web.
(3) Router doesn't reboot unless router's console port is connected.

Modifications in V3.61(WN.2)b1 | 08/14/2003

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] 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.
5. [FEATURE CHANGE] eWC→Firewall→Attack Alert: Change max incomplete TCP

number from 10 to 30.

6. [BUG FIX] Symptom: IPSec packets will use ZyWALL's LAN IP as source IP.
   Condition:
   (4) There is a full feature NAT rule to transffered WAN IP to a LAN IP.
   (5) ZyWALL plays as RESPONDER.
   (6) 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.
7. [BUG FIX] Symptom: Netmeeting causes system crashes.
8. [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 V3.61(WN.1) | 07/07/2003

1. Modify for formal release.
2. [FEATURE CHANGE] In default setting, change "TCP Maximum Incomplete" in eWC→Firewall→Attack Alert from 10 to 30.
3. [BUG FIX] Symptom: HTP test behavior is not correct.
   Condition: Some words get lost when doing HTP test.

Modifications in V3.61(WN.1)b1 | 06/24/2003

1. [BUG FIX] Symptom: VPN tunnel may be dropped.
   Condition: When setting phase 1 SA lifetime shorter than phase 2 SA lifetime, and PING from Responder, tunnel may fail during re-key.
2. [BUG FIX] Symptom: Tunnel will be dropped after phase 1 SA timeout.
   Condition: Set up a dynamic rule in which phase 1 SA life time is shorter than phase 2 SA life time. When the tunnel is up, after phase 1 SA timeout, the tunnel will be dropped, and the traffic will use the old IPSEC SA until it is timeout.
3. [BUG FIX] Symptom: Wireless station can't PING other machines in LAN when activate the Wireless.
   Condition: When the router is up with Wireless inactive, and then activate the WIRELESS, the station can't PING other PCs in LAN.

Modifications in V3.61(WN.0)b7 | 05/21/2003

1. [BUG FIX] Symptom: Web help pages are not correct.
   Condition: Following help pages are not correct.
   (1) eWC→LAN→IP Alias
   (2) eWC→REMOTE MGNT→DNS
   (3) eWC→REMOTE MGNT→FTP

(4) eWC→REMOTE MGNT→SNMP
(5) eWC→REMOTE MGNT→TELNET
(6) eWC→REMOTE MGNT→WWW
(7) eWC→SUA/NAT→Address Mapping
(8) eWC→FIREWALL→RULE CONFIGURATION
(9) eWC→FIREWALL→SOURCE ADDRESS
(10) eWC→FIREWALL→Custom Port
(11) eWC→VPN→Maunal Key
(12) eWC→CONTENT FILTER→Free.
(13) eWC→CONTENT FILTER→iCard

Modifications in V3.61(WN.0)b6 | 05/20/2003

1. [BUG FIX] Symptom: Telnet console hangs when changing router's LAN IP. Condition: When user telnets to router from the LAN side and changes the router's LAN IP, the telnet console will hang. And user cannot telnet to router until router timeout.
2. [BUG FIX] Symptom: 802.1X is not stable.
   Condition: When router is DHCP server, it will assign IP to station periodically and the WLAN connection up and down for every 5 seconds.
3. [BUG FIX] RADIUS is not stable.
   Condition: In some RADIUS software, our router can not access the RADIUS server. Sometimes router doesn't communicate with RADIUS server.
4. [BUG FIX] Symptom: CNM doesn't work.
5. [BUG FIX] WAN will drop when using PPTP in ADSL modem.
   Condition: WAN connection will drop in case of using PPTP for ADSL modem (Alcatel ANT1000, Alcatel SpeedTouch Home and Thomson SpeedTouch 510), especially if there is "high speed" on ADSL (512/256).
6. [BUG FIX] eWC→System→General→Administrator Inactivity Timer: When set up with some value, after reboot the value will be still 5.

Modifications in V3.61(WN.0)b5 | 05/09/2003

1. [FEATURE CHANGE] Custom port is expended as 30.
2. [BUG FIX] Symptom: Sometimes "Message" field of catalog "Access Control" log is blank.
   Condition: "Message" field of catalog "Access Control" log is blank randomly whatever Firewall enables or disables.
3. [BUG FIX] Symptom: PPPoE will be triggered by port 53.
4. [BUG FIX] Symptom: Add product name in page title
5. [BUG FIX] Symptom:UPnP problem:
   Condition: When UPnP is up:
   (1) Tere is no "Network gateway" in network connection.
   (2) While MSN is up, applications can not run successfully.
6. [BUG FIX] Web help pages are not ready:

(1) eWC→Firewall→Rule Configuration→Source IP Address & Destination IP Address
(2) eWC→Firewall→Rule Configuration→Custom Port.

7. [BUG FIX] Symptom: Enable both custom DNS will cause system crash.
8. [BUG FIX] Symptom: When dial backup is up, SMT menu 4 won't change related setting when changing encapsulation.

Modifications in V3.61(WN.0)b4 | 05/02/2003

1. [BUG FIX] Symptom: eWC→LOGS→Reports doesn't work.
2. [BUG FIX] Symptom: Web help pages are not correct
   (1) Help page for eWC→WAN→WAN IP.
   (2) Help page for eWC→LAN→LAN IP
3. [BUG FIX] Symptom: Message "Un-consistent SA Happens!!" shows on console when setting up a VPN tunnel or re-key.
4. [BUG FIX] Symptom: Telnet to machine will cause system crash when eWC→Remote management→TELNET→Secured Client IP Address is "Selected", and an IP address is inserted in the related field.
5. [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.
6. [BUG FIX] 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.

Modifications in V3.61(WN.0)b3 | 04/18/2003

1. [ENHANCEMENT] Add new web pages:
   (1) Add eWC→LOGS→Reports
   (2) Add eWC→MAINTENANCE→Restart
   (3) Add new first page.
2. [BUG FIX] Symptom: The page title should have product name, i.e., should be "ZyXEL ZyWALL 30W".
3. [BUG FIX] Symptom & Condition: If user turns on Firewall TCP reset mechanism (via CI command: "sys firewall tcprst"), log shows "Firewall sent TCP packet in response to DoS attack" when Firewall sends TCP RST to the sender. This wording is incorrect and replaces by "Access block, sent TCP RST".
4. [BUG FIX] Symptom: Web help pages are not ready.

5. [BUG FIX] Symptom: Default settings are not correct.
   (1) eWC→WAN→Route→Dial Backup: Priority should be 15
   (2) eWC→WIRELESS LAN→Wireless→Threshold should be 2432
6. [BUG FIX] Symptom: Sometimes Windows Messenger doesn't work through WAN to LAN.
   Condition: While initiating Windows Messenger APs from WAN to LAN, router can not send and receive packets when all Messenger APs are on.
7. [BUG FIX] Symptom: When VPN is on, SA monitor shows duplicate tunnel when re-keying.
8. [BUG FIX] Symptom: In SMT 15.1.1, "Type" shows "+" when there are more than 5 characters in this column.

Modifications in V3.61(WN.0)b2 | 03/25/2003

1. [BUG FIX] Symptom: Wireless 802.1X doesn't work.
2. [BUG FIX] Symptom: VPN tunnel establish fail
   Condition:
   (1) Secure gateway IP address is 0.0.0.0
   (2) Phase 1 peer ID type is IP, and peer ID content is empty or 0.0.0.0.
   (3) Tunnel can not establish when peer dialing in.
3. [BUG FIX] Symptom: eWC→Dial Back Up doesn't exist.
4. [BUG FIX] Symptom: System crashes during tunnel establishing.
   Condition: In aggressive mode, when PFS is DH 1 or DH 2, tunnel will not establish. If now watch dog is on, system will crash.

Modifications in V3.61(WN.0)b1 | 03/07/2003

1. First release.

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

New function

(1) You can change the server port.
(2) You can set the security IP address for each type of server.
(3) You can define the rule for server access. (WAN only/LAN only, None, ALL).
(4) The secure IP and port of the SNMP server is read only
(5) The port of the SNMP and DNS server is read only.
(6) The default server access of the SNMP and DNS is ALL.

Modification

(1) The default value for Server access rule is ALL.
(2) Under the default setting: You can setup the Menu 15 to forwarding the server to LAN IP address. Thus you can configure the router through the WAN and you don't need to modify the server management or filter.

```
                    Menu 24.11 - Remote Management Control

TELNET Server:      Port = 23           Access = ALL
                        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.

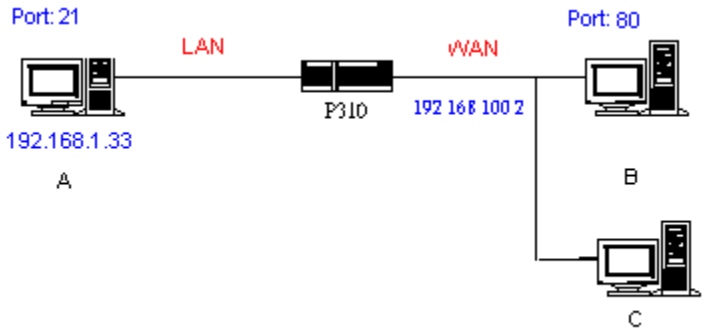
These triggered events can be timed so that they erase the port mapping as soon as they are done with the data transfer, so that the port mapping can be triggered by another Client computer. This gives the *illusion* that multiple computers can use the same port mapping at the same time, but the computers 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 Hard-coded packet filter for "NetBIOS over TCP/IP" (NBT)

The new set C/I commands is under "sys filter netbios" sub-command. Default values of any direction are “Forward”, and trigger dial is “Disabled”.

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

Example ouput:

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

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

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

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

Appendix 4 Traffic Redirect/Static Route Application Note

Why traffic redirect/static route be blocked by ZyWALL

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

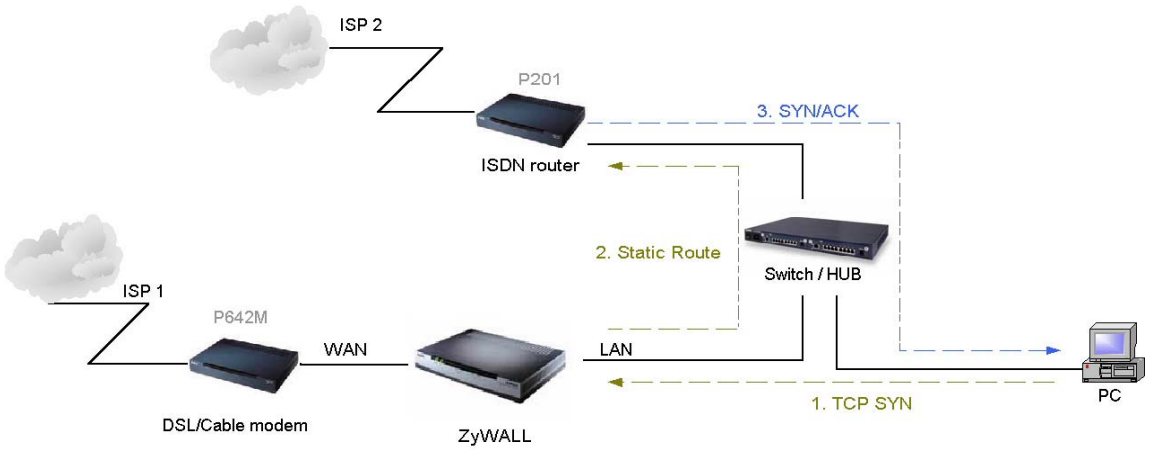


Figure 5-1 Triangle Route

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

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

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

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

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

That causes all of outgoing TCP traffics being reset!

How traffic redirect/static route works under protection - Solutions

(1) Gateway on alias IP network

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

normal function.

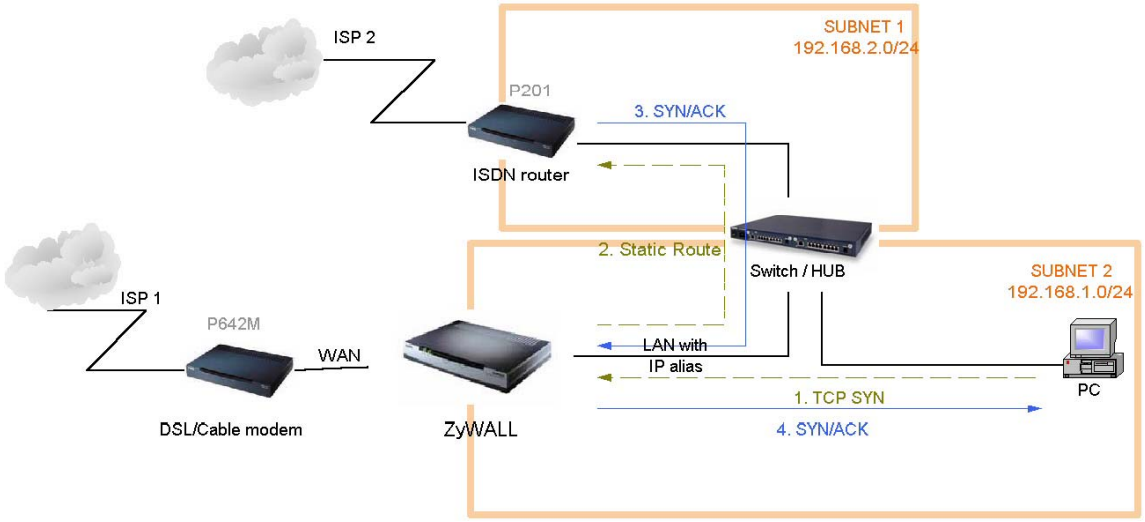


Figure 5-2 Gateway on alias IP network

(2) Gateway on WAN side

A working topology is suggested as below.

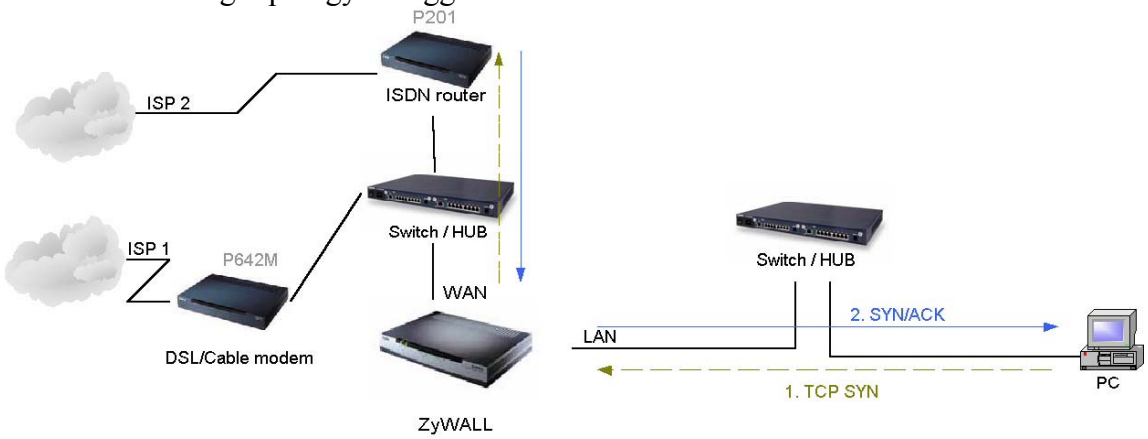


Figure 5-3 Gateway on WAN side

Appendix 5 IPSec FQDN support

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

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

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

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

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

We can put all combinations in to these two tables:

(Local ID Type is IP):

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

*Blank: User can leave this field as empty, doesn’t put anything here.
**Runtime status: During IKE negotiation, ZyWALL will use “My IP Addr” field as source IP of IKE packets, and put “Local ID Content” in the ID payload.

(Peer ID Type is IP):

Configuration		*Run-time check
Secure Gateway Addr	Peer ID Content	
0.0.0.0	blank	Just check ID types of incoming packet and machine’s peer ID type. If the peer’s ID is IP, then we accept it.
0.0.0.0	a.b.c.d	System checks both type and content

a.b.c.d	blank	1. System will check the ID type and the content. 2. The contents will match only if the ID content of coming packet is a.b.c.d because system will put Secure Gateway Address as Peer ID content.
a.b.c.d	e.f.g.h	1. System will check the ID type and the content. 2. The contents will match only if the ID content of coming packet is e.f.g.h.

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

Summary:

1. When Local ID Content is blank which means user doesn’t type anything here, during IKE negotiation, my ID content will be “My IP Addr” (if it’s not 0.0.0.0) or local’s WAN IP.
2. When “Peer ID Content” is not blank, ID of incoming packet has to match our setting. Or the connection request will be rejected.

When “Secure Gateway IP Addr” is 0.0.0.0 and “Peer ID Content” is blank, system can only check ID type. This is a kind of “dynamic rule” which means it accepts incoming request from any IP, and these requests’ ID type is IP. So if user put a such kind of rule in top of rule list, it may be matched first. To avoid this problem, we will enhance it in the future.

Appendix 6 DNS servers for IPSec VPN Note

DNS Domain Names

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

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

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

But the above are not enough for IPSec VPN applications.

How to access the private network by using domain names

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

ZyWALL DNS Servers for IPSec VPN

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

Annex A CI Command List

Last Updated: 2003/02/17

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

System Related Command Home

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

		mail		
			alertAddr [mail address]	send alerts to this mail address
			display	display mail setting
			logAddr [mail address]	send logs to this mail address
			schedule display	display mail schedule
			schedule hour [0-23]	hour time to send the logs
			schedule minute [0-59]	minute time to send the logs
			schedule policy [0:full/1:hourly/2:daily/3:weekly/4:none]	mail schedule policy
			schedule week [0:sun/1:mon/2:tue/3:wed/4:thu/5:fri/6:sat]	weekly time to send the logs
			server [domainName/IP]	mail server to send the logs
			subject [mail subject]	mail subject
		save		save the log setting buffer
		syslog		
			active [0:no/1:yes]	active to enable unix syslog
			display	display syslog setting
			facility [Local ID(1-7)]	log the messages to different files
			server [domainName/IP]	syslog server to send the logs
		updateSvrIP	<minute>	If there is one parameter <minute>, it will change the dns timer task timeout value. Otherwise, do dns resolve to find email log server and syslog server IP.
	pwderrtm		[minute]	Set or display the password error blocking timeout value.
	rn			
		load	<entry no.>	load remote node information
		disp	<entry no.>(0:working buffer)	display remote node information
		nat	<none|sua|full_feature>	config remote node nat
		nailup	<no|yes>	config remote node nailup
		mtu	<value>	set remote node mtu
		save	[entry no.]	save remote node information
	smt			not support in this product
	stdio		[minute]	change terminal timeout value
	time		[hour [min [sec]]]	display/set system time
	trcdisp			monitor packets
	trclog			
	trcpacket			
	syslog			
		server	[destIP]	set syslog server IP address
		facility	<FacilityNo>	set syslog facility
		type	[type]	set/display syslog type flag
		mode	[on|off]	set syslog mode
	version			display RAS code and driver version
	view		<filename>	view a text file
	wdog			
		switch	[on|off]	set on/off wdog
		cnt	[value]	display watchdog counts value: 0-34463
	romreset			restore default romfile
	server			
		access	<telnet|ftp|web|icmp|snmp|dns> <value>	set server access type
		load		load server information

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

Exit Command Home

Command				Description
exit				exit smt menu

Device Related Command Home

Command				Description
dev				
	channel			

		drop	<channel_name>	drop channel
	dial		<node#>	dial to remote node

Ethernet Related Command Home

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

POE Related Command Home

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

PPTP Related Command Home

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

Configuration Related Command Home

Command					Description
config					The parameters of config are listed below.
edit	firewall	active <yes|no>			Activate or deactivate the saved firewall settings
retrieve	firewall				Retrieve current saved firewall settings
save	firewall				Save the current firewall settings

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

			ut <seconds>		before it is terminated
			fin-wait-timeout <seconds>		Edit the wait time for FIN in concluding a TCP session before it is terminated
			tcp-idle-timeout <seconds>		Edit the timeout for an idle TCP session before it is terminated
			pnc <yes|no>		PNC is allowed when 'yes' is set even there is a rule to block PNC
			log <yes|no>		Switch on/off sending the log for matching the default permit
			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		
		server	<primary> [secondary] [third]	set dns server
		stats		
			clear	clear dns statistics
			disp	display dns statistics
	httpd			
		debug	[on|off]	set http debug flag
	icmp			
		status		display icmp statistic counter
		discovery	<iface> [on|off]	set icmp router discovery flag
	ifconfig		[iface] [ipaddr] [broadcast <addr> |mtu <value>|dynamic]	configure network interface
	ping		<hostid>	ping remote host
	route			
		status	[if]	display routing table
		add	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add route
		addiface	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add an entry to the routing table to iface
		addprivate	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add private route
		drop	<host addr> [/<bits>]	drop a route
	smtp			
	status			display ip statistic counters
	stroute			
		display	[rule # | buf]	display rule index or detail message in rule.
		load	<rule #>	load static route rule in buffer
		save		save rule from buffer to spt.
		config		
			name <site name>	set name for static route.
			destination <dest addr>[/<bits>] <gateway> [<metric>]	set static route destination address and gateway.

			mask <IP subnet mask>	set static route subnet mask.
			gateway <IP address>	set static route gateway address.
			metric <metric #>	set static route metric number.
			private <yes|no>	set private mode.
			active <yes|no>	set static route rule enable or disable.
	traceroute		<host> [ttl] [wait] [queries]	send probes to trace route of a remote host
	xparent			
		join	<iface1> [<iface2>]	join iface2 to iface1 group
		break	<iface>	break iface to leave ipxparent group
	ave			anti-virus enforce
	urlfilter			
		reginfo		
			display	display urlfilter registration information
			name	set urlfilter registration name
			eMail <size>	set urlfilter registration email addr
			country <size>	set urlfilter registration country
			clearAll	clear urlfilter register information
		category		
			display	display urlfilter category
			webFeature [block/nonblock] [activex/java/cookei/webproxy]	block or unblock webfeature
			logAndBlock [log/logAndBlock]	set log only or log and block
			blockCategory [block/nonblock] [all/type(1-14)]	block or unblock type
			timeOfDay [always/hh:mm] [hh:mm]	set block time
			clearAll	clear all category information
		listUpdate		
			display	display listupdate status
			actionFlags [yes/no]	set listupdate or not
			scheduleFlag [pending]	set schedule flag
			dayFlag [pending]	set day flag
			time [pending]	set time
			clearAll	clear all listupdate information
		exemptZone		
			display	display exemptzone information
			actionFlags [type(1-3)][enable/disable]	set action flags
			add [ip1] [ip2]	add exempt range
			delete [ip1] [ip2]	delete exempt range
			clearAll	clear exemptzone information
		customize		
			display	display customize action flags
			actionFlags [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
	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
			edit clear	clear one rule in the set
		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	lan	<on|off>	After a packet is IPSec processed and will be sent to LAN side, this switch is to control if this packet can be applied IPSec again.
				Remark: Command available since 3.50(WA.3)
		wan	<on|off>	After a packet is IPSec processed and will be sent to WAN side, this switch is to control if this packet can be applied IPSec again.
				Remark: Command available since 3.50(WA.3)
	show_runtime	sa		display runtime phase 1 and phase 2 SA information
		spd		When a dynamic rule accepts a request and a tunnel is established, a runtime SPD is created according to peer local IP address. This command is to show these runtime SPD.
	switch	<on|off>		As long as there exists one active IPSec rule, all packets will run into IPSec process to check SPD. This switch is to control if a packet should do this. If it is turned on, even there exists active IPSec rules, packets will not run IPSec process.
	timer	chk_my_ip	<1~3600>	- Adjust timer to check if WAN IP in menu is changed
				- Interval is in seconds
				- Default is 10 seconds
				- 0 is not a valid value
		chk_conn.	<0~255>	- Adjust auto-timer to check if any IPsec connection has no traffic for certain period. If yes, system will disconnect it.
				- Interval is in minutes
				- Default is 2 minuets
				- 0 means never timeout
		update_peer	<0~255>	- Adjust auto-timer to update IPSec rules which use domain name as the secure gateway IP.
				- Interval is in minutes
				- Default is 30 minutes
				- 0 means never update
				Remark: Command available since 3.50(WA.3)
	updatePeerIp			Force system to update IPSec rules which use domain name as the secure gateway IP right away.
				Remark: Command available since 3.50(WA.3)
	dial	<rule #>		Initiate IPSec rule <#> from ZyWALL box
				Remark: Command available since 3.50(WA.3)
	display	<rule #>		Display IPSec rule #
	remote	key	<string>	I add a secured remote access tunnel with pre-shared key. It is a dynamic rule with local: the route's WAN IP. The algorithms with it are fixed to phase1: DES+MD5, DH1 and SA lifetime 28800 seconds; phase2: DES+MD5, PFS off, no anti-replay and SA lifetime 28800 seconds. The length of pre-shared key is between 8 to 31 ASCII characters.
		switch	<on|off>	Activate or de-activate the secured remote access tunnel.
	keep_alive	<rule #>	<on|off>	Set ipsec keep_alive flag
	load	<rule #>		Load ipsec rule

	save			Save ipsec rules
	config	netbios	active <on|off>	Set netbios active flag
			group <group index1, group index2…>	Set netbios group
		name	<string>	Set rule name
		name	<string>	Set rule name
		keeyAlive	<Yes| No>	Set keep alive or not
		natTraversal	<Yes| No>	Enable NAT traversal or not.
		lcIdType	<0:IP | 1:DNS | 2:Email>	Set local ID type
		lcIdContent	<string>	Set local ID content
		myIpAddr	<IP address>	Set my IP address
		peerIdType	<0:IP | 1:DNS | 2:Email>	Set peer ID type
		peerIdContent	<string>	Set peer ID content
		secureGwAddr	<IP address | Domain name>	Set secure gateway address or domain name
		protocol	<1:ICMP | 6:TCP | 17:UDP>	Set protocol
		lcAddrType	<0:single | 1:range | 2:subnet>	Set local address type
		lcAddrStart	<IP>	Set local start address
		lcAddrEndMask	<IP>	Set local end address or mask
		lcPortStart	<port>	Set local start port
		lcPortEnd	<port>	Set local end port
		rmAddrType	<0:single | 1:range | 2:subnet>	Set remote address type
		rmAddrStart	<IP>	Set remote start address
		rmAddrEndMask	<IP>	Set remote end address or mask
		rmPortStart	<port>	Set remote start port
		rmPortEnd	<port>	Set remote end port
		antiReplay	<Yes | No>	Set anitreplay or not
		keyManage	<0:IKE | 1:Manual>	Set key manage
		ike	negotiationMode <0:Main | 1:Aggressive>	Set negotiation mode in phase 1 in IKE
			authMethod <0:PreSharedKey | 1:RSASignature	Set authentication method in phase 1 in IKE
			preShareKey <string>	Set pre shared key in phase 1 in IKE
			certFile <FILE>	Set certificate file if using RSA signature as authentication method.
			p1EncryAlgo <0:DES | 1:3DES>	Set encryption algorithm in phase 1 in IKE
			p1AuthAlgo <0:MD5 | 1:SHA1>	Set authentication algorithm in phase 1 in IKE
			p1SaLifeTime <seconds>	Set sa life time in phase 1 in IKE
			p1KeyGroup <0:DH1 | 1:DH2>	Set key group in phase 1 in IKE
			activeProtocol <0:AH | 1:ESP>	Set active protocol in phase 2 in IKE
			p2EncryAlgo <0:Null | 1:DES | 2:3DES>	Set encryption algorithm in phase 2 in IKE
			p2AuthAlgo <0:MD5 | 1:SHA1>	Set authentication algorithm in phase 2 in IKE
			p2SaLifeTime <seconds>	Set sa life time in phase 2 in IKE
		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. - Default value is “off” which means “no skip”.
	adjTcpMss		<off|auto|user defined value>	- After a tunnel is established, system will automatically adjust TCP MSS. - After all tunnels are drops, the MSS will adjust to the original value. - The default value is auto.

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

Wireless LAN Related Command Home

Command	Description

wlan	active			Display the current active status of WLAN, 0:inactive, 1:active
		0		Deactive WALN
		1		Active WLAN
	essid	<essid>		Give the ESSID of WALN. The default value is “Wireless”.
	chid	<channel id>		Give the channel id. The default value is 1.
	version			Display the primary/secondary version number of the WLAN card and the version number of tertiary firmware.
				.
	reset			Reset WLAN
	association			Display those WLAN stations associate to this device.
	tx			Only for EMI test
	rx			Only for EMI test
	basicrate			Display the current basic rate. The default value is 0x03
		<basic rate>		Set the basic rate. bit 0: 1M bps, bit 1: 2M bps, bit 2: 5.5M bps, bit 3: 11M bps
	txrate	<		Display the current data rate. The default value is 0x0f
		<tx rate>		Set the data rate. bit 0: 1M bps, bit 1: 2M bps, bit 2: 5.5M bps, bit 3: 11M bps.
	authen	<bit mask>		Set the authentication algorithm to use for authenticating the station. Bit 0: Open System. Bit 1: Shared Key.

Bridge Related Command

Home

Command				Description
bridge				
	cnt			related to bridge routing statistic table
		disp		display bridge route counter
		clear		clear bridge route counter
	stat			related to bridge packet statistic table
		disp		display bridge route packet counter
		clear		clear bridge route packet counter