ZyXEL

Firmware Release Note

ZyWALL 2WE

Release 3.62(WJ.0)

Date: **Feb, 24, 2004**
Author: **Neil Cheng**

ZyXEL ZyWALL 2WE Standard Version
Release 3.62(WJ.0)
Release Note

Date: Feb 24, 2004

Supported Platforms:

ZyXEL ZyWALL 2WE

Versions:

ZyNOS Version: V3.62(WJ.0) | 02/24/2004
BootBase : V1.05 | 01/05/2004

Notes:

1. **Restore to Factory Defaults Setting Requirement: No.**
2. When user upgrade firmware version to 3.62(WJ.0)b1. System may automatic change Bootbase version to 1.05. Please don't shut off the power when firmware upgrades proceeding.
3. The setting of ignore triangle route is on in default ROM FILE. Triangle route network topology has potential security crisis. If you are not clear about it, please refer to Appendix for the triangle route issue.
4. IKE process in phase 2 will check ID information between system and the peer. If you found that the IPSec connection is failed, please check your settings.
5. Using Web to configure VPN, the phase 1 algorithms have been fixed to DES + MD5. If other algorithms are preferred, please use ADVANCE page to configure them.
6. When firewall turns from "off" to "on", the firewall initialization procedure will disconnect all connections running through the ZyWALL.
7. SUA/NAT address loopback feature was enabled on ZyWALL by default; however, if users do not need it, a C/I command "ip nat loopback off" could turn it off.
8. 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.
9. When UPnP is on, and then reboot the router, Windows XP will not detect UPnP and refresh "My Network Places→Local Network". Plug in network wire again can solve this problem.

Known Issues:

---

1. Dial-backup can't work correctly when using USR modem.
2. If user connects WAN port and LAN port to same switch HUB simultaneously, packet routing may abnormal on ZyWALL 2.
3. eWC→WAN IP has bugs when WAN→ISP is PPPoE or PPTP. Leaving some values in remote IP or remote masks for WAN→IP and then switch to dynamic IP, ZyWALL cannot dial anymore.
4. Sometimes on screen the "Local Area Connection" icon for UPnP disappears. The icon shows again when restarting PC.
5. When you use MSN messenger, sometimes you fail to open special applications, such as whiteboard, file transfer and video etc. You have to wait more than 3 minutes and retry these applications.
6. Symptom: When turning on to many web sites at same time, it may cause content filter fail.

   Condition: When turning on browser to access a lot of websites (for example, 30 sites) at same time may cause content filter fail.
7. For ZyWALL 2/2WE, if you want to make two local stations can access the same remote private network, you can setup two IPSec rules for these two stations. But you should note that, these two IPSec rules must have the same security gateway, ID contents, IKE phase 1 parameters and Perfect Forward Secrecy.

Features:

Modifications in V 3.62(WJ.0) | 02/24/2003

Modify for formal release.

Modifications in V 3.62(WJ.0)b4 | 02/17/2004

1. [ENHANCEMENT] Add a new CI command "ip arp period" to change the ARP lifetime interval. The default ARP lifetime is 300 seconds, the user can use this CI to change ARP lifetime. Please note that this CI command will not change the lifetime of an existing ARP entry, but only for the newly created ARP entry. Please note also that it will not store the new ARP lifetime configuration into romfile.
2. [ENHANCEMENT] Add a CI command to switch the ARP attack:

   ip arp attpret <on|off>

   The default is "on" that means the router will avoid IP spoofing ARP attack by default. Users can use "ip arp attpret off" to make the router accept the different network ARP. To allow the DHCP client get the WAN IP address and gateway IP address which are in different networks, the router needs to accept the ARP from different networks.
3. [ENHANCEMENT] Add speed configuration CI commands to set WAN speed:

   ether edit speed <auto|10/half|10/full|100/half|100/full>

Note: Need to reset chip, so the connection will be broken.

4. [ENHANCEMENT] Add product name in eWC page title.
5. [FEATURE CHANGE] Modify wireless channel ID mapping with country code. Spain and France now used channel 1 to 13.
6. [ENHANCEMENT] Update eWC help pages on wireless and VPN.
7. [BUG FIX] Symptom: IPSec XAUTH cannot work with SoftRemote version 8.0.0
   Condition:
   1). Configure corresponding IPSec rule with XAUTH on SoftRemote and ZyWALL.
   2). Trigger SoftRemote IPSec rule.
   3). SoftRemote log shows "no proposal chosen" and connection fails.
8. [BUG FIX] Symptom: ZyWALL cannot establish IPSec connection to SSH Sentinel.
   Condition: When ZyWALL and Sentinel both enable XAUTH, the IKE negotiation will fail.
9. [BUG FIX] Symptom: IPsec NAT-Traversal can not work.
   Condition:
   1). Setup NAT-Traversal rule at Initiator and Responder, both sides are Tunnel encapsulation mode.
   2). Connect from Initiator side.
   3). Tunnel can not be established.
10. [BUG FIX] Symptom: IPSec rule swap 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.
11. [BUG FIX] Symptom: Rule swap failed when NAT-Traversal is on.
    Condition:
    1). Initiator setup one NAT-Traversal rule and transport encapsulation mode.
    2). Responder setup two NAT-Traversal rules, the first is tunnel mode, the second is transport mode.
    3). Initiator start to establish connection for the transport mode rule.
    4). IKE negotiation will fail.
12. [BUG FIX] Symptom: ICMP packet of NAT loopback will be blocked by Firewall.
    Condition:
    1). Enable Firewall.
    2). NAT default server is set to host A.
    3). Turn on NAT loopback.
    4). Host A pings router's WAN IP address.
    5). Host A does not receive echo reply packet and Firewall log shows "Land Attack".

Modifications in V 3.62(WJ.0)b3 | 02/09/2004

13. [BUG FIX] Symptom: Traceroute or PingPlotter are not able to discover ZyWALL's LAN interface.
    Condition:
    1). Running Traceroute or PingPlotter on desktop.
    2). Both applications can not discover ZyWALL's LAN interface.
    3). Firewall log shows "Unsupported/out-of-order ICMP: ICMP(type:11, code:0)".
14. [BUG FIX] Symptom: Wireless can’t work when user upgrade firmware from 3.60 to 3.62.
    Condition:
    1). Upgrade firmware to 3.62(WJ.0)b2.
    2). After system reboot, PC using wireless can’t get DHCP.
    3). Client PC can’t access internet through wireless via ZyWALL2WE.
15. [BUG FIX] Symptom: X-Auth behavior in VPN rule setting page isn't correct.
    Condition:
    1). eWC-->VPN-->Extended Authentication: Do not select "Enable Extended Authentication" (X-Auth is disabled).
    2). Select "Client mode" and keep "User name" and "Password" empty.
    3). VPN rule can't be saved and message "Both User Name and Password are required" shows on "Status".
16. [BUG FIX] Symptom: LAN host cannot access Internet.
    Condition: When one host continuously tries to setup a new connection, sometimes it fails and the host never can access Internet.
17. [BUG FIX] Symptom: System memory leak and eventually causing the reboot.
    Condition:
    1). Start collecting data in eWC->LOGS->Reports or using CI command "ip rpt start".
    2). Run for a very long time.
    3). System will run out of memory and become very unstable.
18. [ENHANCEMENT] Pause console display when the NAT session information fills a console screen.
19. [BUG FIX] Symptom: Bootbase auto convert failed with bootbase version 1.3
    Condition:
    1). Upgrade firmware on ZW2WE with bootbase version 1.3
    2). Bootbase convert will not be preformed.

Modifications in V 3.62(WJ.0)b2 | 01/29/2004

1. [BUG FIX]Symptom: When WAN encapsulation is PPPoE or PPTP, the DNS query initiated by router itself will fail to send.
   Condition:
   1). Set WAN encapsulation with PPPoE or PPTP.

2). Connect to a time server using domain name.
3). Time synchronization would fail as a result of domain name resolve failure.

2. [BUG FIX]Symptom: PC can't setup TCP connections via ZyWall to the internet when ZyWALL's WAN encapsulation is PPTP.
   Condition:
   1). Set WAN encapsulation with PPTP.
   2). Setup a TCP connection to the internet.
   For example: Use browser to create an HTTP connection.
   3). Browser won't retrieve any information because ZyWALL always resets TCP connections.

Modifications in V 3.62(WJ.0)b1 | 01/15/2004

3. [ENHANCEMENT] Add new feature: X-Auth as the authentication method in VPN IKE phase.
4. [ENHANCEMENT] Add new feature: Support new encryption algorithm AES in IPSec.
5. [ENHANCEMENT] Add new feature: Dial backup supported.
6. [ENHANCEMENT] Add new feature: Support Cerberian content filter.
7. [ENHANCEMENT] Add two new categories "TCP Reset", "Packet Filter" , "ICMP", "Remote Management", "CDR", "PPP" , "802.1X", "Wireless" in Centralized Log.
8. [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.
9. [ENHANCEMENT] Add UPnP "Ports" page to show the UPnP NAT ports.
10. [ENHANCEMENT] Add session manager to limit session number per host. Default setting is 256, user can modify this value with C/I command - "sys tos sessPerHost".
11. [ENHANCEMENT] Add NAT session limitation per host. Default setting is 256, user can modify this value with C/I command – "ip nat session".
12. [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.
13. [ENHANCHMENT] Modify and enhance firewall ACL schedule by rule.
    Before: Firewall ACL rule will active all day if we enable this rule.
    Now: We can assign which day(day of week) and time(time of day) that firewall ACL rule will active.
14. [ENHANCHMENT] On Maintenance page of DHCP Table, add "Reserve" checkbox to support static DHCP.
15. [ENHANCEMENT] Add system & LAN relative DNS CI commands.

16. [ENHANCEMENT] The GUIs of UPnP and HTTP are enhanced to inform users the relation between UPnP and HTTP.
17. [ENHANCEMENT] Add CI command "sys upnp reserve [0|1]"(default value is 0) to reserve UPnP NAT rules in flash after system boot up.
18. [ENHANCEMENT] In the past, when My IP Address is configured as 0.0.0.0 in IPSec rule, system will use the WAN's IP address as my IP address during IKE. Now it will use the IP of dial backup as my IP address when the WAN is disconnected. In the case of traffic redirect, it will use LAN IP as my IP address.
19. [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.
20. [FEATURE CHANGE] We change maximum Firewall custom port number from 10 to 30.
21. [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.
22. [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.

Modifications in V 3.60(WJ.3) | 10/03/2003

Modify for formal release.

Modifications in V 3.60(WJ.3)b2 | 09/24/2003

1. [BUG FIX] Symptom: Run ping plotter and it will show lots of packet lost errors.
   Condition: User Ping Plotter in local PC, and connect router to Internet. Ping Plotter will show packet lost error during running the program.
2. [BUG FIX] Symptom: Router sends DNS query even mail server or sys log server is empty.
   Condition: When sys log server or mail server is not given, system should not send DNS query but it did.

Modifications in V 3.60(WJ.3)b1 | 08/22/2003

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] [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:
   (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.
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 V 3.60(WJ.2)b1 | 05/23/2003

1. [BUG FIXED] Symptom: A special IPSec policy rule will make the ZyWALL can not establish the IPSec tunnel.
   Condition: (1) The security gateway is 0.0.0.0
   (2) The peer IP type is IP and the peer ID content is empty or “0.0.0.0”;
   (3) The ZyWALL can’t establish the IPSec tunnel when the peer site dial in.

2. [BUG FIXED] Under heavy traffic, sometime, ZyWALL’s firewall will make system crash.
3. [BUG FIXED] Symptom & Condition: Sometimes Enable/Disable traffic redirect when WAN encapsulation is PPPoE, system may crash.
4. [BUG FIXED] 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.
5. [BUG FIXED] 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).

CI command: "pptp enque <size>" to manually configure the maximum en-queue number. The default is 10.

6. [ENHANCEMENT] Enhance the WAN port configuration function so that user can configure the WAN port speed as Auto/10/100 Mbps and transmit mode as full or half duplex mode.

   CI Command: “ether edit load 2”
   “ether edit speed [*auto|100/full|100/half|10/full|10/half*]“
   “ether edit save”
7. [BUG FIXED] Symptom & Condition: The CNM feature doesn’t work, when we turn on the CNM encryption/decryption.

Modifications in V 3.60(WJ.1)b4 | 04/09/2003

8. [BUG FIXED] Symptom: WAN MAC address spoof has problem.
   Condition: When the user give ZW’s WAN a new MAC address and this address is also belong to a LAN station. This station can’t access the Internet any more, through the ZW device.

Modifications in V 3.60(WJ.1)b3 | 03/31/2003

9. [BUG FIXED] Symptom: Sometimes, IPSec re-key procedure failed.
   Condition: Under the heavy traffic situation, sometimes IPSec re-key failed.
10. [BUG FIXED] Symptom: Even though the IPSec policy is correct, the IKE phase 1 negotiation may failed.
   Condition 1: There are two IPSec polices with the same security gateway. ZyWALL sometimes can’t create the second IPSec tunnel .
   Condition 2: If ZyWALL didn’t send the DEL packet to info the security gateway to delete the IPSec tunnel(for example power off the device, or PPPoE drops…etc.), ZyWALL can’t re-create the tunnel.
11. [BUG FIXED] Symptom: It’s a compatibility problem with SonicWall.
   Condition 1: Can’t create the IPSec tunnel with a SonicWall security gateway, if the type of ID Content is FQDN.

Modifications in V 3.60(WJ.1)b2 | 03/21/2003

12. [BUG FIXED] Can’t save the IPSec Pre-Shared Key with the length over 16 octets, if

we use the hex-decimal format.

13. [ENHANCEMENT] Some fields checking and error messages for SMT and Web Telia Login setup.

Modifications in V 3.60(WJ.1)b1 | 03/12/2003

1. [BUG FIXED] Symptom: A special case will make the ZyWALL device to reboot.
   Condition:
   (2) Configure an IPSec Rule.
   (3) On the Logs Settings page, configure "Mail Server", "Mail Subject" and the mail address logs mails send to.
   (4) Still on the Logs Settings page, select IPSec and IKE alert.
   (5) Enter the CI command mode, and issue the CI command "ipsec dial #" to create the VPN tunnel.
   (6) After seeing the message "Press any key to return....", press the Enter key.
   (7) The ZyWALL crashs.
2. [BUG FIXED] Symptom & Condition: On Fireall --- Rule Config, can't setup to log firewall logs.
3. [BUG FIXED] The general user(not ZyWALL administrator), can directly retrieve ZyWALL rom file by using the rom-0 as the URL file, without password checking.
4. [ENHANCEMENT] Supports the hexdecimal format of IPSec Pre-Shared Key.
5. [ENHANCEMENT] Supports Telia login WAN access.
6. [ENHANCEMENT] Added a new CI commands to configure UDP port NAT timeout CI command: "ip nat timeout udp [port] <seconds>". For more details, please refer to CI command lists

Modifications in V 3.60(WJ.0)b9 | 2/21/2003

1. [BUG FIXED] Symptom & Condition: It's failed to restore default romfile by pressing reset button.
2. [BUG FIXED]Symptom: VPN setting causes system reboot.
   Condition: Step1. Build one VPN tunnel and set the secure gateway address by using IP address and establish the tunnel. Keep on pinging the client continuously
   Step2. Change the secure gateway address setting from IP to DNS and apply.
3. [BUG FIXED] Symptom:eWC, TimeZone page displays ERROR message.
   Condition: When we change System/Time Zone to none, an internally ERROR 1 will be displayed in the Status-Line.
4. [BUG FIXED] Symptom & Condition: In web, the page does not refresh when we change the time zone and apply.
5. [BUG FIX] Symptom & Condition: It's failed to restore default romfile by pressing reset button.

Modifications in V 3.60(WJ.0)b8

1. [BUG FIXED] Symptom: On eWC, the VPN host page appears again.
   Condition: This condition only occurs when the user enable the WLAN’s IEEE 802.1X feature.

Modifications in V 3.60(WJ.0)b7

2. [BUG FIXED] One special notebook PC(Dell Inspiron 8000) connect to ZyWALL’s console port and none of terminal program open the console port. In this situation, the ZyWALL device boots fialed.

Modifications in V 3.60(WJ.0)b6

3. [ENHANCEMENT] Add NAT traversal feature. This feature is supported only ESP tunnel and ESP transport when key management is IKE.
4. [ENHANCEMENT] Add the Full Feature NAT.
5. [FEATURE CHANGE] DHCP relay is not supported anymore.
6. [FEATURE CHANGE] The color of centralize Log GUI is defined. Black color is for normal log messages and red for alert log messages.
7. [FEATURE CHANGE] Remove VPN port restriction. Now LAN is a 4-port switch and all LAN’s hosts and WLAN can use VPN.
8. [FEATURE CHANGE] The number of VPN rules is changed to 2.
9. [FEATURE CHANGE] When phase 1 ID type is IP and content is blank or 0.0.0.0, ZyWALL will use WAN IP or Secure gateway address as content. In the previous design, only blank content will do.
10. [BUG FIX] Symptom & Condition: While NAT is enabled, remote device can not access router’s LAN IP through IPSec tunnel. In other words, remote management to the LAN IP over IPSec tunnel failed.
11. [BUG FIX] Symptom & Condition: When Traffic Redirect is active and change the WAN encapsulation to PPPoE or PPTP, and if idle time out the routing table will disorder.
12. [BUG FIX] Symptom & Condition: Removed wrong “DMZ” selection form all Remote Management pages.
13. [BUG FIX] Symptom & Condition: If the user didn’t load IPSec rule first before executing IPSec configuration CI command, “ipsec config netbios active <yes|no>” or “ipsec config netbios group <…>” , ZyWALL will crash.
14. [BUG FIX] Symptom: Can not change WAN MAC by web immediately:
    Condition: While we change WAN MAC by web, the MAC ca not change immediately till device reboot. But it is OK while we change by SMT menu.
15. [BUG FIX] Symptom: Receving hotmail mail will cause system crash.
    Condition: 1. Enable Block Cookies. 2. Receiving mail form hotmail causes system crash.
16. [BUG FIX] Symptom: System crashes when setting DHCP :

Condition: If we disable DHCP server and set a static DHCP entry, the ZyWALL crashes.

17. [BUG FIX] Symptom: The value for sys stdio can not be saved. :
    Condition: Under CI command, we enter “sys stdio 0”. The value becomes the default value after we relogin SMT.
18. [BUG FIX] Symptom: Traffic redirect check path is not up :
    Condition: While WAN link is fine and the traffic redirect check point is failed, it spends long time to activate traffic redirect. Under the situation, the metric of the route for traffic redirect sometimes changes frequently.
19. [BUG FIX] Symptom: Traffic Redirect can’t work on PPPoE connection.
    Condition: If the WAN side has a successful PPPoE connection, and the ZyWALL device would not check the checked site and update to correct the routing table.
20. [BUG FIX] Symptom: LAN LED light on, when setup the WAN.
    Condition: Using the eWC to setup WAN or using SMT 2 to setup the WAN's MAC address. All Ethernet LEDs will light on.
21. [BUG FIX] Symptom: Add, delete or refresh static route rule on SMT menu12 sometimes cause ZyWALL crash.
    Condition: Sometimes our action on menu12 with static route rule setup will cause ZyWALL crash.
22. [BUG FIX] Symptom: When "ipsec switch" is off, "ipsec dial" still works.
    Condition: If user uses command "ipsec switch off" to turn off IPSec, "dial" still works.
23. [BUG FIX] Symptom: When phase 1 ID type is IP, tunnel cannot be built.
    Condition:
    1. Set MyIP 0.0.0.0
    2. Set My ID Type as IP
    3. Leave My ID content blank
    4. During IKE, ZyWALL will use 0.0.0.0 as ID content. However it should be WAN IP.

Modifications in V 3.60(WJ.0)b5 | 12/11/2002

1. [BUG FIXED] The system crashes, if the user changes the console’s baud rate and presses any key by using a different data rate.
2. [BUG FIXED] The system crashes, if the user power off the PC which connect to the device’s console port.]
3. [Feature Enhancement] show the reason of forward/block by content filter feature in the centralized log message.
4. [Enhancement] Add a retype password confirmation mechanism for PPTP and PPPoE setup on SMT menu 4 and menu 11.
5. [BUG FIX] Menu 24.6 Restore occur system reboot
   Menu 24.6 Restore Configuration is Failed and Device will Hang then key any key Occur system reboot !
6. [BUG FIX] system reboot
   On F/W V3.60(WJ.0)b2, system reboot occurs. The Step: Into Web; VPN Host ;VPN Hosts IP Address or MAC address, if you change IP or MAC and Apply the ZW will

reboot!!

7. [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.
8. [BUG FIX] Symptom: Send email log will cause system to hang about 30 seconds.
   Condition: 1. Email server address is written in domain name. 2. The WAN network link can not connect to Internet when applying email log setting.
9. [BUG FIX] Symptom & condition: FQDN: When ID type is IP, VPN tunnel can not established if passing through another router with NAT.
10. [BUG FIX] Symptom & Condition: During IKE phase 1 negotiation, if ZyWALL receives a Notify DEL payload, it may crash.
11. [BUG FIX] Symptom: WAN side PC can not access the LAN port through VPN tunnel. Condition: With a VPN tunnel between two routers, the outer PC can not access the LAN port.
12. [BUG FIX] Symptom: VPN tunnel can not be established if ZyWALL sets phase 1 ID type as IP and wants to negotiate with another side by passing through a router with NAT.
    Condition: Take the figure below as the example:

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

    If ZyWALL A wants to build a VPN tunnel with ZyWALL B by passing through Router C with NAT, A can not see B and will set secure gateway as C. In our implementation system will set peer ID content as secure gateway address if peer ID type is IP. So A's peer ID content is C's WAN IP if A's peer ID type is IP. In this case, A and B will never negotiate successfully. To avoid this situation, now user can set ID content when ID type is IP. In this case, A will check the ID content what B is configured. However, user can leave the ID content is blank when ID type is IP. Please refer to appendix for the detail setting and system behavior.

Modifications in V 3.60(WJ.0)b4 | 11/29/2002

13. [BUG FIXED] HTP Program, LAN/WAL external loopback test fail.

Modifications in V 3.60(WJ.0)b3 | 11/29/2002

1. [ENHANCEMENT] Extended the bootbase to support a large 32K rom-file.
2. [BUG FIXED] VPN Port setup page causes the system crash
3. [BUG FIXED] SMT 24.6 can't restore rom file.
4. [BUG FIXED] Browse www.gamespy.com will causes the system crash

Modifications in V 3.60(WJ.0)b2 | 11/20/2002

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.

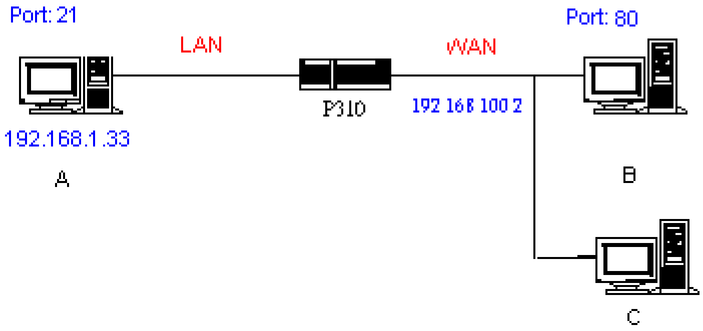
These triggered events can be timed so that they erase the port mapping as soon as they are done with the data transfer, so that the port mapping can be triggered by another Client computer. This gives the ***illusion*** that multiple computers can use the same port mapping at the same time, but the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

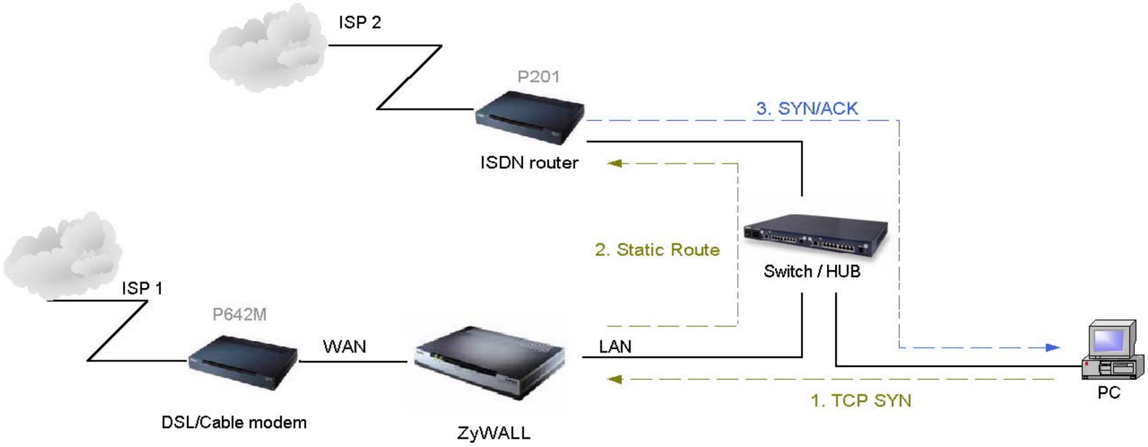


Figure 5-1 Triangle Route

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.

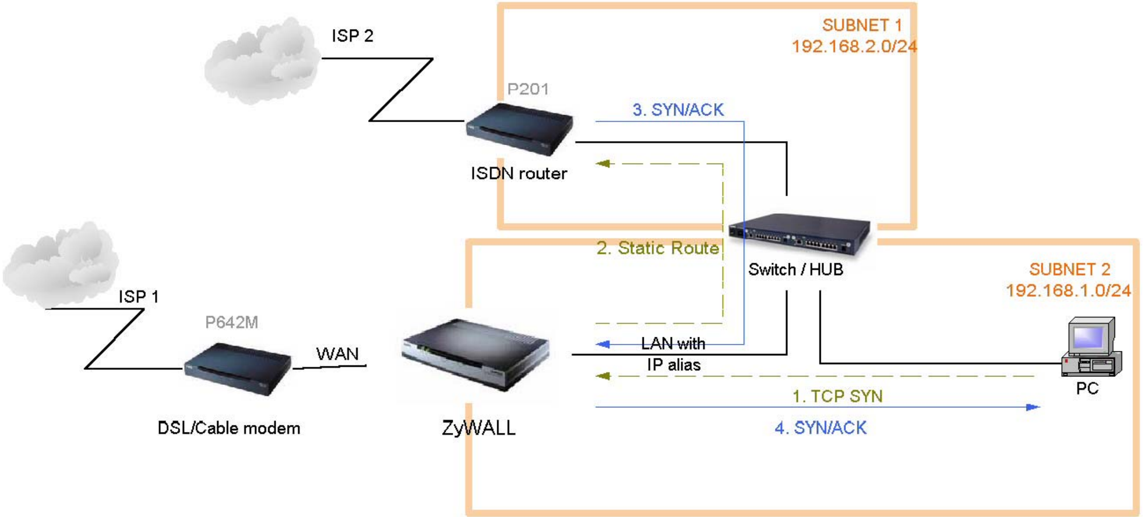


Figure 5-2 Gateway on alias IP network

(2) Gateway on WAN side

A working topology is suggested as below.

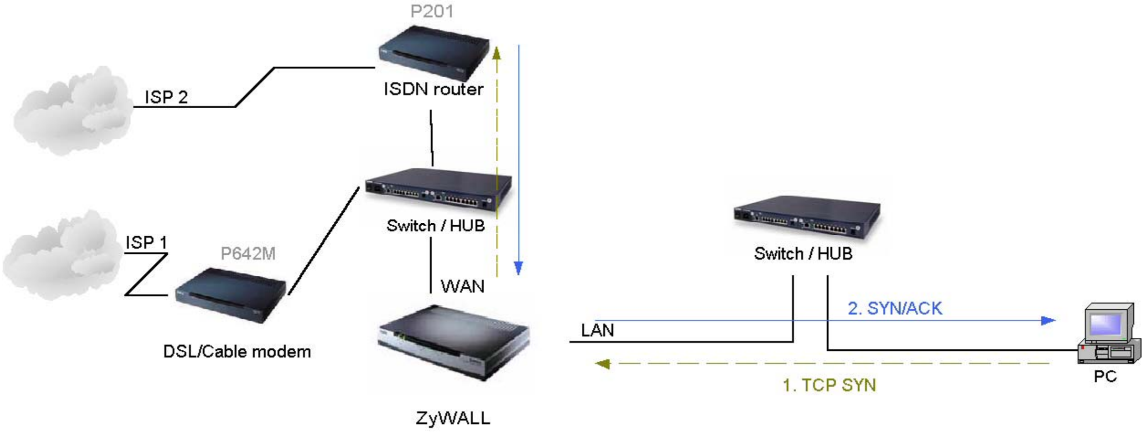


Figure 5-3 Gateway on WAN side

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

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
Configuration Related Command	IP Related Command	IPSec Related Command
Firewall Related Command	Wireless LAN 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
	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
	stdio		[second]	change terminal timeout value
	time		[hour [min [sec]]]	display/set system time
	trcdisp			monitor packets
	trclog			
	trcpacket			
	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
	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-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	Select and edit a destination address range of a

				address> <end ip address>	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		
		system		
			edit	edit system DNS status
			display	show system DNS status
		lan		
			edit	edit LAN DNS status
			display	show LAN DNS status
			clear	clear dns statistics
			disp	display dns statistics

		default	<ip>	Set default DNS server
	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
	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 [act(1-6)][enable/disable]	set action flags
			logFlags [type(1-3)][enable/disable]	set log flags
			add [string] [trust/untrust/keyword]	add url string
			delete [string] [trust/untrust/keyword]	delete url string
			clearAll	clear all information
		logDisplay		display cyber log
		ftplist		update cyber list data
		listServerIP	<ipaddr>	set list server ip
		listServerName	<name>	set list server name
	tredir			
		failcount	<count>	set tredir failcount
		partner	<ipaddr>	set tredir partner
		target	<ipaddr>	set tredir target
		timeout	<timeout>	set tredir timeout
		checktime	<period>	set tredir checktime
		active	<on|off>	set tredir active
		save		save tredir information
		disp		display tredir information
		debug	<value>	set tredir debug value
	nat			
		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
		timeout	udp [port] <seconds>	set the UDP port NAT timeout value

	igmp			
		debug	[level]	set igmp debug level
		forwardall	[on|off]	turn on/off igmp forward to all interfaces flag
		querier	[on|off]	turn on/off igmp stop query flag
		iface		
			<iface> grouptm <timeout>	set igmp group timeout
			<iface> interval <interval>	set igmp query interval
			<iface> join <group>	join a group on iface
			<iface> leave <group>	leave a group on iface
			<iface> query	send query on iface
			<iface> rsptime [time]	set igmp response time
			<iface> start	turn on of igmp on iface
			<iface> stop	turn off of igmp on iface
			<iface> ttl <threshold>	set ttl threshold
			<iface> v1compat [on|off]	turn on/off v1compat on iface
		robustness	<num>	set igmp robustness variable
		status		dump igmp status
	pr			

IPSec Related Command Home

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

		update_peer	<0~255>	- Adjust auto-timer to update IPSec rules which use domain name as the secure gateway IP.
				- Interval is in minutes
				- Default is 30 minutes
				- 0 means never update
				Remark: Command available since 3.50(WA.3)
	updatePeerIp			Force system to update IPSec rules which use domain name as the secure gateway IP right away.
				Remark: Command available since 3.50(WA.3)
	dial	<rule #>		Initiate IPSec rule <#> from ZyWALL box
				Remark: Command available since 3.50(WA.3)
	display	<rule #>		Display IPSec rule #
	remote	key	<string>	I add a secured remote access tunnel with pre-shared key. It is a dynamic rule with local: the route's WAN IP. The algorithms with it are fixed to phase1: DES+MD5, DH1 and SA lifetime 28800 seconds; phase2: DES+MD5, PFS off, no anti-replay and SA lifetime 28800 seconds. The length of pre-shared key is between 8 to 31 ASCII characters.
		switch	<on|off>	Activate or de-activate the secured remote access tunnel.
	keep_alive	<rule #>	<on|off>	Set ipsec keep_alive flag
	load	<rule #>		Load ipsec rule
	save			Save ipsec rules
	config	netbios	active <on|off>	Set netbios active flag
			group <group index1, group index2…>	Set netbios group

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.