ZyXEL

Firmware Release Note

ZyWALL 5

Release 3.62(XD.3)

Date: **Jan. 20, 2005**
Author: **Tim Tseng**
Project Leader: **Stanley Liu**

ZyXEL ZyWALL 5 Standard Version release 3.62(XD.3) Release Note

Date: Jan. 20, 2005

Supported Platforms:

ZyXEL ZyWALL 5

Versions:

ZyNOS Version: V3.62(XD.3) | 01/20/2005
Bootbase Version: V1.08 | 01/17/2005

Note:

1. Restore to Factory Defaults Setting Requirement: Yes.
2. The setting of ignore triangle route is on in default ROM FILE. Triangle route network topology has potential security crisis. If you are not clear about it, please refer to Appendix for the triangle route issue.
3. 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.
4. 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.
5. When firewall turns from "off" to "on", the firewall initialization procedure will disconnect all connections running through the ZyWALL.
6. 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.
7. 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.
8. 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.
9. The default port roles for LAN/DMZ setting is: port 1 to port 4 are all LAN ports.
10. In bridge mode, If LAN side DHCP clients want to get DHCP address from WAN side DHCP server, you may need to turn on the firewall rule for BOOT_CLIENT service type in WAN→LAN direction.

Known Issues:

1. If the metric of dial-backup is smaller (has higher priority) than the metric of Traffic-Redirect, Traffic-Redirect can't be triggered any more.

2. Sometimes on screen the "Local Area Connection" icon for UPnP disappears. The icon shows again when restarting PC.
3. 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..
4. On the SUA/ Address Mapping page, users can enter two or above same rules.
5. On the SUA/ Address Mapping Edit page, the user can give the same local IP and global IP.
6. SMT 15.1, if we try to edit the 11th rule then press ESC, the system returns some weird characters.
7. You must notice those metric values of WAN, Traffic-Redirect and Dial-backup. You should better give those values, Dial-backup > Traffic-Redirect > WAN. For example, WAN (1), Traffic-Redirect(14), Dial-backup(15).
8. Bandwidth Management doesn't work on wireless LAN.
9. Sometimes, modify an active IPSec rule(the VPN tunnel was created) will crash the system, if this tunnel is going the re-key process.
10. Symptom: LAN host can ping Internet while LAN host change cable from LAN port to DMZ port.
    Condition:
    (1) Host connect to LAN port and get DHCP address from router.
    (2) Unplug LAN host cable and plug it into DMZ port.
    (3) The host can still ping Internet using LAN DHCP address
    (4) The scenario will continue about 30secs.
11. The DMZ TxPkts counter increment at about 1 pkt/min even without any Ethernet cables ever connected.
12. At SMT24.1, the collisions for WAN, LAN and DMZ port are not really counted.
13. AES doesn't work with key length 192 and 256.
14. When device boots in Bridge Mode, some CI command error messages will be displayed on console. This is because some predefined CI commands in autoexec.net is forbidden to execute in Bridge Mode.
15. Under Bridge Mode, all LAN ports will behave as a hub, and all DMZ ports will also behave as another hub.
16. When perform SPT partial reset via Vantage, device wouldn't reset all system parameters.
17. Device can't delete address mapping via Vantage.
    (1) Let device register to Vantage.
    (2) Add 2 address-mapping rules via Vantage.
    (3) Delete 1 address-mapping rule via Vantage. The rule can't be deleted.
18. H.323 may not work with following scenario:
    PC1 ⟷ ZyWALL ⟷ internet ⟷ ZyWALL ⟷ PC2.
19. SIP P2002w Wify-Phone may not work with following scenario:
    PC1 ⟷ ZyWALL ⟷ internet ⟷ ZyWALL ⟷ PC2.

Features:

Modifications in V3.62(XD.3) | 01/20/2005
Modify for formal release

Modifications in V3.62(XD.3)b2 | 01/17/2005
1. [BUG FIX]
   Symptom: eWC-->LAN-->IP Alias has no conflict check
   Condition: In eWC-->LAN-->IP Alias, Alias 1 and Alias 2 should be in different subnet, but our system doesn't do such check.

Modifications in V3.62(XD.3)b1 | 01/11/2005
2. [ENHANCEMENT]
   Change keep alive behavior to nailed-up in IPSec.
3. [ENHANCEMENT]
   Modify CI command "ip arp add" from hidden to visible.
4. [ENHANCEMENT]
   Support for DNS queries from WAN to LAN internal DNS server.
5. [ENHANCEMENT]
   Add the switch of NAT AOL alg. "ip nat service aol [on|off]"
6. [ENHANCEMENT]
   Add "ip urlfilter webControl reginfo refresh" The CI command is to query whether device's external CF had been registered. If yes, write the original license key to flash.
7. [BUG FIX]
   Symptom: In GUI->AUTH SERVER->Local User Database, it cannot check the duplicate name.
   Condition:
   1. In eWC->AUTH SERVER->Local User Database.
   2. If two rows of data have the same username, the status bar does not show the warning message.
8. [BUG FIX]
   Symptom: Add Static route rule on WAN interface, after reboot system, the routing table not exist this rule.
   Condition:
   1. WAN1 (or WAN2) uses ethernet dynamic IP.
   2. Add a static route rule on WAN1 (or WAN2) interface and check this rule exist on routing table.
   3. Reboot system, this rule not exist on routing table.
9. [BUG FIX]
   Symptom: eWC-->LAN-->IP Alias has no conflict check
   Condition: In eWC-->LAN-->IP Alias, Alias 1 and Alias 2 should be in different subnet, but our system doesn't do such check.
10. [BUG FIX]
    Symptom: Possible NAT issue in combination with specific SUA entry.
    Condition:
    (1) Go to eWC>NAT Port Forwarding Page set a rule with port start from 10000 to

20000, inactive this rule.
(2) After some outbound traffic, use CI command “ip nat hashTable enif1” to check, the outgoing port incorrectly start from 20000

11. [BUG FIX]
    Symptom: If M-1 & 1-1 are using the same public IP address, it would cause some problem.
    Condition:
    (1) Go to eWC>NAT Address Mapping Page set M-1 NAT and 1-1 NAT with same global IP address.
    (2) The M-1 NAT entries will let the first 1-1 NAT connections fail.
12. [BUG FIX]
    Symptom: Content filtering cannot block keyword.
    Condition:
    1. Add keyword "pchome".
    2. enable keyword blocking.
    3. Connect to "www.google.com.tw" to search "pchome".\
    4. Click the first link "www.pchome.com.tw" in the search result page.
    5. The access will be blocked.
    6. Refresh the pae again.
    7. The web site "www.pchome.com.tw" can be accessed.
13. [BUG FIX]
    Symptom: Triangle routes via ZyWALL’s WAN ports will fail.
    Condition:
    1. Connect ZW70-WAN1 port to WAN.
    2. Setup a FTP server and a FTP Client on WAN.
    3. Enable triangle route.
    4. Setup a static route on FTP Client. Route the packets to FTP server using ZW70-WAN1 as GW.
    5. Use FTP Client to connect with FTP server. It will fail to establish the TCP connection.
14. [BUG FIX]
    Symptom: Router will crash under VPN stress test
    Condition:
    1. Use two ZW5 and configure 10 VPN rules.
    2. Use SmartBit build up 10 VPN tunnels and run stress test
    3. Router will crash after a long time
15. [BUG FIX]
    Symptom: Zywall will reboot.
    Condition: When using BT (Bitspirit) to download, the ZW5 will reboot itself sometimes.
16. [BUG FIX]
    Symptom: A firewall rule is created automatically after Click on Cancel button.
    Condition:
    (1) On GUI>FIREWALL>Summary, Click on "Insert" button to go to the firewall edit rule screen.
    (2) Click on "Add" to create Custom Port Service in Firewall.

(3) Delete the above created Custom Port Service.
(4) Click on Cancel button, back to summary page, a firewall rule is created automatically.

17. [BUG FIX]
    Symptom: Two ZyWALL 5 are connected with PPPoE, using AES for VPN connection, ftp failed. But DES, 3DES worked.
    Condition:
    Two ZyWALL 5 are connected with PPPoE, using AES for VPN connection, ftp failed. But DES, 3DES worked.
18. [BUG FIX]
    Symptom: Enter special url will cause device crash.
    Condition:
    1. Form LAN site, enter
    http://192.168.1.1/Forms/rpAuth_1?ZyXEL%20ZyWALL%20Series<script>top.location.pathname=%20""</script> on browser, the device will crash.
19. [BUG FIX]
    On eWC>REMOTE MGMT>CNM help page is missing.
20. [BUG FIX]
    Symptom: DHCP client does not work on beta user's environment.
    Condition: DHCP client not RFC 2131 on rebinding request, according to RFC it should be broadcast where our device is send unicast.
21. [BUG FIX]
    Symptom: Under the remote-access VPN scenario, the mobile user cannot access the internet via the VPN tunnel.
    Condition:
    1. Configure a dynamic IPSec rule on ZyWALL_a with Local Network as 0.0.0.0 ~255.255.255.255.
    2. Configure an IPSec rule on a mobile user to connect with ZyWALL_a.
    3. After a tunnel is established between ZyWALL_a and the mobile user, all the internet-bound traffic from the mobile user will be tunnelled to ZyWALL_a. ZyWALL_a should be able to route these traffics to the internet and then route the responses back to the tunnel. However, ZyWALL_a fails to do so.

Modifications in V 3.62(XD.2) | 09/24/2004
Modify for formal release.

Modifications in V3.62(XD.2)b3 | 09/21/2004

1. [BUG FIX]
   Symptom: LAN host will get wrong DNS server.
   Condition:
   1. Set SMT 3.2 DNS first DNS server as user defined 1.1.1.1. Others are none.
   2. Unplug WAN port and reboot.
   3. LAN host get IP address and DNS server and the DNS server is LAN IP.

Modifications in V3.62(XD.2)b2 | 09/17/2004

1. [BUG FIX]
   Symptom: LAN host ping device LAN IP a period time, then PPPoE/PPTP will be triggered dial.
   Condition:
   1. Set WAN 1 are PPPoE.
   2. LAN host ping device LAN IP a period time, then WAN 1 will be triggered dial.
2. [BUG FIX]
   Symptom: Firewall sends TCP RST after it blocks traffic period of time.
   Condition:
   1. Configure Firewall LAN to WAN blocked and enable log
   2. Generate one TCP SYN packet from LAN to WAN
   3. Firewall will block this packet and generate block log
   4. After period of time (30 seconds), Firewall log shows it sent TCP RST to both client and server side
3. [BUG FIX]
   Symptom: System has a lot of long timeout UDP sessions.
   Condition:
   1. Enable firewall.
   2. Display TOS sessions.
   3. A lot of long timeout UDP sessions.
4. [BUG FIX]
   Symptom: ZyWALL crashes very often in bridge mode.
   Condition:
   1. Switch to bridge mode.
   2. Enable Firewall.
   3. ZyWALL crashes very often.
5. [ENHANCEMENT] Enhance "cnm keepalive" ci command. Add "cnm keepalive 0" command to stop sending of keepalive packet to Vantage.
6. [BUG FIX] Symptom: Symptom: FTP from WAN to LAN does not work.
   Condition:
   1. Set a FTP server on a host in the LAN side and configure a default server to this host.
   2. Using FTP from WAN to the default server with port mode.
   3. After typing username and password, "ls" command does not work.
7. [BUG FIX] Symptom: LAN host will get wrong DNS server.
   Condition:
   1. Set SMT 3.2 DNS first DNS server as user defined 1.1.1.1. Others are none.
   2. Unplug WAN port and reboot.
   3. LAN host get IP address and DNS server and the DNS server is LAN IP.
8. [BUG FIX] Symptom: System Crash when change encryption key in Vantage.
   Condition:
   1. Device register to Vantage in router mode under DES and PPPoE.
   2. configuration>>general>>system change the original encryption key and apply
   3. Device receives data but soon the system crash.

9. [BUG FIX] Symptom: WAN Gateway will be reset to 0.0.0.0.
   Condition:
   1. In Vantage CNM add a device (the device have a static IP),when it register to Vantage. Vantage set default value to device.
   2. After the device reset, WAN Gateway will be reset to 0.0.0.0.
10. [BUG FIX] Symptom: CNM agent accepts wrong CI command ”cnm keepalive -323123122222222222222222”.
    Condition:
    1. In SMT 24.8, type ”cnm keep -323123122222222222222222”.
    2. The system accepts it and saves with the value.
11. [BUG FIX] Symptom: CNM agent accepts wrong CI command ”cnm encrymode 1231223”.
    Condition:
    1. In SMT 24.8, type ”cnm encrymode 1231223”.
    2. The system accepts it and read it as ”65535”.
12. [BUG FIX] Symptom: [Vantage] Configuration>>VPN: When delete a active VPN tunnel successfully. Device sends VPN tunnel status "Destroy" to vantage.
    Condition:
    1. Create and dial up a VPN tunnel via Vantage.
    2. Delete this active rule in Vantage.
    3. Vantage server will have exception.
13. [BUG FIX]
    Symptom: eWC will fill the "Connection ID/Name" field with "C:1" when the fetch data is empty.
    Condition:
    1. In eWC, set "Connection ID/Name" as empty in PPTP mode and apply it.
    2. Go go another page and go back the WAN page, the "Connection ID/Name" field is filled with "C:1" even we set the field as empty.

Modifications in V3.62(XD.2)b1 | 08/16/2004

1. [ENHANCEMENT]
   Add Unified ALG for SIP and H.323.
2. [ENHANCEMENT]
   Each unified ALG can be enabled/disabled. The default ALG setting for SIP and H.323 is disabled.
3. [ENHANCEMENT]
   Firewall can bypass AX.25 (protocol #93) & IPv6 (protocol #41) protocols.
4. [BUG FIX]
   Symptom: Bandwidth management with ALG_H.323 cause system crash.
   Condition:
   1. Create a class with a Service-H.323 filter in WAN1 interface.
   2. Unplug all WAN’s cable
   3. Lanch the ”Openphone” application that supports H.323 and make a call.
   4. Router crashes.
5. [BUG FIX]

Symptom: Router block trusted web content.
Condition:
1). In "eWC->CONTENT FILTER->General", enable content filter.
2). In "eWC->CONTENT FILTER->Customization", select check boxes of "Enable Web site customization" and "Disable all Web traffic except for trusted Web sites".
3). In "eWC->CONTENT FILTER->Customization", set "www.hellowork.go.jp" as trusted web site.
4). Open browser and access http://www.hellowork.go.jp/kensaku/servlet/kensaku?pageid=001
5). In the new page, select third and fourth radio bottom and click "search" bottom.
6). In the new page, click "next page" bottom.
7). The new page will be blocked.

6. [BUG FIX]
Symptom: External Content Filtering cannot block the URL belonging to restricted category.
Condition:
1). In "eWC->CONTENT FILTER->Customization", unselect "Enable Web site customization".
2). Add a URL to "trusted web sites".
3). In "eWC->CONTENT FILTER-Customization>, select "Block Web sites which contain these keywords".
4). In "eWC->CONTENT FILTER->Categories", select the category which the URL belongs to.
5). Access the trusted URL.
6). The URL will not be blocked.
7. [BUG FIX]
Symptom: System crash by memory leak.
Condition:
1). Enable bandwidth management.
2). Into eWC->Bandwidth Management->Monitor and wait for a period time.
3). System crash by memory leak.
8. [BUG FIX]
Symptom: Remote node CI command crashes.
Condition:
1). Goto SMT 24.8
2). Load dial backup remote node to working buffer.
3). Type CI command "sys rn accessblock 0".
4). Save this remote.
5). System crashes.
9. [BUG FIX]
Symptom: System crash when someone want to configure NAT mapping rules.
Condition:
1. Use the terminal program to login the console.
2. Enter SMT 15, NAT Setup
3. Select 1 to enter SMT 15.1, Address Mapping Sets.
4. The system crash
10. [BUG FIX]

Symptom: eWC>NAT>ADDRESS MAPPING edit page leaks memory.
Condition:
1. Log on to eWC.
2. Go to eWC>NAT>ADDRESS MAPPING edit page, and then click Cancel.
3. Repeat Step 2 for several times.
4. Check system memory info by the CI command: system memu ms You will observe abnormal increases of memory sections, indicating memory leaks.

11. [BUG FIX]
    Symptom: Trigger port will disappear after system reboot.
    Condition:
    1. Configure Trigger port rule.
    2. System reboot.
    3. The configured Trigger port rule disappear.
12. [BUG FIX]
    Symptom: The system might crash when enabling IPSec.
    Condition: During IKE negotiation the system might crash.
13. [BUG FIX]
    Symptom: MSN Messenger's "Ask for Remote Assistance" function causes system crash.
    Condition:
    1. Enable UPnP.
    2. Set PC(A) and router(B) in intranet and PC(C) connects to LAN port of router(B).
    3. Test MSN Messenger's "Ask for Remote Assistance" function from PC(A) to PC(C).
    4. After PC(C) accepts the PC(A) request by "Ask for Remote Assistance" then the device will crash.
14. [BUG FIX]
    Symptom: System out of memory.
    Condition:
    1. Let the ZyWALL be a DNS proxy for LAN hosts.
    2. Do a lot of DNS inverse queries by running IPScan tool continuously from LAN host.
    3. After a long time, the ZyWALL will out of memory.
15. [FEATURE CHANGE]
    Change UPnP device name for ZyWALL35 and ZyWALL5
    WAS: "ZyXEL ZyWALL 35 Internet Security Gateway"
    IS: "ZyXEL ZyWALL 35 Internet Security Appliance"
16. [BUG FIX]
    Symptom: Packets cannot pass through NAT router to LAN hosts.
    Condition:
    1. NAT default server is on
    2. Procotol of the packet is not TCP, UDP, ICMP, ESP, GRE.
    3. Packets from WAN to router.
    4. Packets cannot pass through NAT router to LAN hosts (NAT default server)
17. Symptom: External Content filtering cannot register.
    Condition:
    1. In "eWC->content filter->categories", click "register" to connect to ZSSW.
    2. Do the registration on ZSSW.
    3. The registration will fail in the final step.
18. [ENHANCEMENT]
    External content filtering support full URL checking.

Was: External content filtering only take domain name or IP address of URL into category checking.
Is: External content filtering put entire URL into category checking.

19. [ENHANCEMENT]
    CI command to turn off triangle route log, multicast log and broadcast log.
    1. Add CI commands:
    a. "sys logs switch".
    b. "sys logs switch display".
    c. Triangle route log switch: "sys logs switch bmlog <0:no|1:yes>"
    d. Broadcast/Multicast log switch: "sys logs switch trilog <0:no|1:yes>".
20. [BUG FIX]
    Symptom: System time problem.
    Condition:
    1. enter SMT24.10, configure time server.
    2. open daylight saving, configure the start time and end time so that current time is within the daylight saving time.
    3. after writing to rom file, router ask you to calibrate the system clock, answer yes.
    4. If system failed to connect time server, system time will add one hour, every time you enter smt 24.1,system time add 1 hour automatically.
21. [FEATURE CHANGE]
    Change external content filtering message on centralized log and blocked page for some error events.
22. [BUG FIX]
    Symptom: Router will crash.
    Condition: When user continuously accesses eWC and press "Apply" button, sometimes router will crash.
23. [BUG FIX]
    Symptom: The system crashes after it receives a url that contains more than three "/"s behind the ip address (or domain name).
24. [BUG FIX]
    Symptom: Sometimes when connect to router by TCP, FTP or HTTP will fail.
    Condition:
    1. One user connects to router by FTP, TELNET or HTTP.
    2. In TCP handshake, client doesn't receive SYN ACK. i.e., router is in SYN RECEIVE state.
    3. Client timeout and send RESET to router.
    4. Related socket in router is still alive and other users can't login router until this socket timeout.
25. [BUG FIX]
    Symptom: eWC spelling error: eWC->Firewall→Default Rule: Allow Asymetrical should be “Asymmetric”
26. [BUG FIX]
    Symptom: System out of memory and reboot when firewall enable.
    Condition:
    1. Enable firewall, then generate traffic.
    2. The memory will slowly leak until it uses up all the memory, then reboot.
27. [BUG FIX]
    Symptom: Generate a lot of TCP port 80 sessions to ZyWALL will cause device to hang and reboot by hardware watchdog.
    Condition:

1. Use session.exe to generate a lot of TCP port 80 sessions to ZyWALL's LAN or WAN interface
2. After several hundreds of sessions are established, the ZyWALL will hang and finally reboot.

28. [ENHANCEMENT]
    1. Support user config for SIP session timeout value.
    2. Support SIP SDP multiple RTP port.
    3. Delete unused ALG type.
    4. Command for ALG enable/disable and sip timeout.
29. [BUG FIX]
    Symptom: Sometimes the ZyWALL reboots by software watchdog.
    Condition:
    1.Put the ZyWALL on the network for a long time.
    2.Sometimes the ZyWALL will reboot by software watchdog.
30. [BUG FIX]
    Symptom: XAUTH with rule swap doesn't work.
    Condition:
    1. In initiator, set up a VPN rule with XAUTH in client mode.
    2. In responder, there are three VPN rules:
    a. Rule 1 is XAUTH off.
    b. Rule 2 is XAUTH with client mode.
    c. Rule 3 is XAUTH with server mode (this rule corresponds to client rule).
    3. Dial from initiator, and the tunnel will never be up.
31. [BUG FIX]
    Symptom: Content filter timeout problem.
    Condition:
    1. A router is register the content filter (CF) server.
    2. Enable the CF feature.
    3. Enable the external database content filtering.
    4. The router log often record "Waiting content filter server (server name) timeout!".
    5. A PC in lan fetch web from internet often hang for a while.

Modifications in V3.62(XD.1) | 06/25/2004

1. Formal release.

Modifications in V3.62(XD.1)b1 | 06/16/2004

1. [ENHANCEMENT] Suppout Vantage CNM 2.0 (Vantage Centralized Network Management).

Modifications in V3.62(XD.0) | 05/18/2004

1. Formal release.

Modifications in V3.62(XD.0)b5 | 05/14/2004

1. [BUG FIX] Symptom: The ZyWALL might crash or hang when users browse eWC→Firewall→Rule Summary.
   Condition:
   (1) Log on to eWC.
   (2) Browse Ewc→Firewall→Rule Summary
   (3) The ZyWALL might crash or hang.

Modifications in V3.62(XD.0)b4 | 04/27/2004

1. [FEATURE CHANGE]
   Remove Policy Route feature from ZyWALL 5 because Policy Route is not defined in product specification.
2. [FEATURE CHANGE]
   Maximum concurrent VPN tunnel number is changed from 5 to 10.
3. [FEATURE CHANGE]
   The following default settings is changed:
   (1) eWC→Firewall→Anti-Probing
   WAS: Anti-Probing Respond Ping to LAN
   IS: Anti-Probing Response Ping to LAN&WAN&DMZ
   (2) eWC→Firewall→Threshold
   WAS: TCP Maximum Incomplete Sessions = 10
   IS: TCP Maximum Incomplete Sessions = 30
   (3) eWC→WAN→Route
   WAS: WAN Priority = 2
   IS: WAN Priority = 1
4. [BUG FIX]
   Symptom: External Content Filtering cannot be registered.
   Condition:
   (1) In eWC→CONTENT FILTER→Categories", click "register" to connect to ZSSW.
   (2) Do the registration on ZSSW.
   (3) Browser display "Please wait....." and the page of "Register successfully" does not appear.
5. [BUG FIX]
   Symptom: Traffic Redirect does not work.
   Condition:

   Internet ------- Router A ------ ZyWALL ----- gateway B ----- Internet
   WAN LAN
   (1) Let ZyWALL WAN port connect to another router A and A is connected to Internet.
   (2) Setup Traffic Redirect to backup gateway B located at LAN side.
   (3) Disconnect the connection between router A and Internet.
   (4) The ZyWALL can not do Traffic Redirect to gateway B located at LAN side.
6. [BUG FIX]

CI command “ip igmp” is lost.

7. [BUG FIX]
   Symptom: The behavior in priority-based Bandwidth Management is not correct.
   Condition:
   (1) In eWC→BW MGMT→Summary, activates WAN1 root class with Speed = 1500 kbps and Scheduler = Priority-Based
   (2) In eWC→BW MGMT→Class Setup, Adds two sub-classes under WAN1 root class. Where WAN1-1 : Bandwidth Budget = 200, Priority = 7(higher than WAN1-2), and “Borrow bandwidth from parent class” is selected; WAN1-2 : Bandwidth Budget = 500, Priority = 1, “Borrow bandwidth from parent class” is also selected.
   (3) First generates traffic that satisfies WAN1-2 class, users will find WAN1-2 borrow the whole available bandwidth from parent, and the traffic is bound at about 1500kbps.
   (4) Then generates traffic that satisfies WAN1-1 class. Users will find WAN1-1 can not borrow bandwidth from parent class and bandwidth is bound at about 200kbps even though WAN1-1 has higher priority than WAN1-2.
8. [BUG FIX]
   Symptom: In eWC→MAINTENANCE→General, set a number which is bigger than 1000 for Administrator Inactivity Timer. The label string 'Administrator Inactivity Timer' will disappear.
   Condition:
   (1) Go to eWC→MAINTENANCE→General, set a number which is bigger than 1000 for Administrator Inactivity Timer.
   (2) Click 'Apply'.
   (3) The label string 'Administrator Inactivity Timer' will disappear.
9. [BUG FIX]
   Symptom: ZyWALL ping sometimes fails.
   Condition:
   (1) Turn on Firewall.
   (2) Go to SMT 24.8
   (3) Ping to exist host, but it sometimes fails.
10. [BUG FIX]
    Symptom: In SMT 3.2, the subnet of ZyWALL LAN IP can be different from the subnet of DHCP client ip and ZyWALL LAN IP can be set within DHCP Client IP pool range.
    Condition:
    First case:
    (1) Go to SMT 3.2
    (2) Set DHCP client IP Starting address to be 192.168.2.3
    (3) Set LAN IP Address to be 192.168.1.1, then confirm to save.
    (4) These setting can be saved and no error message.
    Second case:
    (1) In SMT 3.2, set DHCP client ip Starting address to be 192.168.1.3
    (2) Set Size of Client IP Pool to be 10
    (3) Set LAN IP Address to be 192.168.1.3, then confirm to save.
    (4) These setting can be saved and no error message.
11. [BUG FIX]

Symptom: Remote access control cannot work properly.
Condition:
(1) Turn on bridge mode
(2) Configure telnet server access control from WAN only by SMT 24.11
(3) Telnet to device via WAN side
(4) The telnet connection fails.

12. [BUG FIX]
    Symptom: System crashes.
    Condition: Configure device by eWC sometimes cause crash.
13. [BUG FIX]
    Symptom: In bridge mode ZyWALL at eWC→Bridge, Bridge IP address settings can not be saved successfully.
    Condition:
    (1) Switch the ZyWALL to bridge mode.
    (2) Go to eWC→Bridge page.
    (3) Change "IP Address", "IP Subnet Mask", or "Gateway IP Address" then click "Apply"
    (4) Status shows "Configuration updated successfully" but the changes was not really saved.
14. [BUG FIX]
    Symptom: In SMT 24.11, the setting of DNS Service is displayed under bridge mode
    Condition:
    (1) Go to SMT 1, change Device Mode to bridge mode.
    (2) After reboot, go to SMT 24.11, DNS Service incorrectly appear.

Modifications in V3.62(XD.0)b3 | 04/04/2004

1. [BUG FIX]
   Symptom: CI command error, ZyWALL will show some CI commands which don't belong to current command set.
   Condition:
   (1) Go to SMT 24.8, CI command mode.
   (2) Type "ip dns system", ZyWALL will correctly print two available commands, "edit" and "display".
   (3) Type "ip dns sys", ZyWALL will unexpectedly print nine available commands instead of two. Those extra seven commands are not under "ip dns system".
2. [BUG FIX]
   Symptom: DHCP client cannot get address from router.
   Condition:
   (1) In eWC→LAN→LAN, configure router as a DHCP server and set IP pool starting address as 192.168.1.33.
   (2) In eWC→LAN→Static DHCP, configure all rules in static DHCP table and the IP addresses are 192.168.1.33~192.168.1.40.
   (3) Use a PC which MAC address is not in the static DHCP table to get a IP address from router.

(4) The PC cannot get the IP address.

3. [BUG FIX]
   Symptom: The ZyWALL will reset the current eWC HTTP session even when the LAN IP configuration is not successfully changed. Under this situation, users have to re-log in the ZyWALL.
   Condition:
   (1) Log in ZyWALL eWC, and go to eWC→LAN.
   (2) Deliberately configure the LAN IP address as within the WAN subnet.
   (3) Click Apply, then the status will show an error message indicating address conflict.
   (4) The ZyWALL will then automatically break the current eWC HTTP session. To access the ZyWALL, users have to log in again.
4. [BUG FIX]
   Symptom: Router will crash when entering SMT menu 3.5
   Condition:
   (1) Insert WLAN card.
   (2) In CI command, enter "wlan active 11" instead of "wlan active 1" to activate WLAN on router.
   (3) Enter SMT 3.5, router will crash.
5. [ENHANCEMENT]
   Supports Vantage CNM 2.0(Vantage Centralized Network Management)
6. [BUG FIX]
   Symptom: The Content Filtering blocks cookies even if it is not in the blocked schedule.
   Condition:
   (1) In eWC→CONTENT FILTER→General, select "Block Cookies".
   (2) In eWC→CONTENT FILTER→General, set "Schedule to Block" with a time period NOT including the current time.
   (3) Access a web site which contains cookies.
   (4) The cookies will be blocked by the Content Filtering.
7. [BUG FIX]
   Symptom: WAN status in SMT 24.1 shows wrong information in bridge mode.
   Condition:
   (1) Configure Internet access as PPTP or PPPoE encapsulation in router mode.
   (2) Switch ZyWALL to bridge mode.
   (3) WAN status in SMT 24.1 shows idle and IP address is "0.0.0.0".
8. [BUG FIX]
   Symptom: Device cannot transfer Ethernet frame in bridge mode.
   Condition:
   (1) ZyWALL enables bridge mode.
   (2) The Internet connection is under DMZ port.
   (3) Plug Ethernet cable between one host and ZyWALL DMZ port.
   (4) This host starts to transfer packets to Internet.
   (5) Unplug the Ethernet cable from DMZ port and plug in LAN port.
   (6) This host cannot transfer packets to Internet anymore.
9. [BUG FIX]
   Symptom: PPPoE connection sometimes fails in France.
   Condition: Since France Telecom changes their core network setup to BRAS,

ZyWALL PPPoE connection on authentication phase most of the time fails.

10. [ENHANCEMENT]
    Updates help pages for ZyWALL 5.
11. [BUG FIX]
    Symptom: On the eWC→WIZARD→Internet Access page, the System DNS Servers configuration is not available when the ZyWALL is not a DHCP server for its LAN hosts.
    Condition:
    (1) Log onto eWC, and go to eWC→LAN. Uncheck the "DHCP Server" option to stop ZyWALL from being a DHCP server to its LAN hosts.
    (2) Go to eWC→HOME→WIZARD→Internet Access. The System DNS Servers configuration is not available in the wizard.
12. [ENHANCEMENT]
    The ZyWALL 5 Firewall GUI are enhanced as follows.
    (1) On eWC→Firewall→Rule Summary→Edit Rule, a basic sanity check on the firewall rule is performed.
    (2) On eWC→Firewall→Rule Summary→Edit Rule, the selected service for a new rule is empty by default.
    (3) On eWC→Firewall→Rule Summary→Edit Rule, the useless headers "####### Source IP Address #######" and "#### Destination IP Address #####" are removed.
    (4). On eWC→Firewall→Rule Summary→Edit Rule, when a specific address is added to the Source/Destination Address list, the "Any" address will automatically be deleted.
    (5) On eWC→Firewall→Rule Summary→Edit Rule, the firewall action radio buttons are replaced by a dropdown list.
    (6) On eWC→Firewall→Threshold, the "Cancel" button is replaced by "Reset" button.
    (7) On eWC→Firewall→Deafult Rule, the wording "Default Rule Settings" is replaced by "Deafult Rule Setup".
    (8) On eWC→Firewall→Anti-Probing, the wording "Anti-Probing Settings" is replaced by "Anti-Probing Setup".
    (9) "ACCESS POLICY" is renamed as "FIREWALL".
    (10) "CUSTOM PORT" is renamed as "CUSTOM SERVICE".
    (11) Users can expand or collapse "Source Address", "Destination Address" and "Service Type" drop down lists by clicking the [+]/[-] icon at the beginning of each rule in Firewall Rule Summary Table.

Modifications in V3.62(XD.0)b2 | 03/26/2004

1. [BUG FIX]
   Symptom: In eWC→FIREWALL→ACCESS POLICY→EDIT RULE, Action for Matched Packets can't be saved correctly.
   Condition:
   (1) Go to eWC→FIREWALL→ACCESS POLICY→EDIT RULE
   (2) Choose the type of Action for Matched Packets as Block, and then click Apply.
   (3) Leave this page and then re-enter this page again, Action for Matched Packets always shows Forward.

2. [ENHANCEMENT]
   Supports Intel TE28F640 J3C120 Flash ROM.

Modifications in V3.62(XD.0)b1 | 03/11/2004
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.

Note

(1) DNS Service is not available in Bridge Mode.

```
                Menu 24.11 - Remote Management Control

TELNET Server:     Port = 23         Access = ALL
                   Secure Client IP = 0.0.0.0
FTP Server:        Port = 21         Access = ALL
                   Secure Client IP = 0.0.0.0
SSH Server:        Certificate = auto_generated_self_signed_cert
                   Port = 22         Access = ALL
                   Secure Client IP = 0.0.0.0
HTTPS Server:      Certificate = auto_generated_self_signed_cert
                   Authenticate Client Certificates = No
                   Port = 443        Access = ALL
                   Secure Client IP = 0.0.0.0
HTTP Server:       Port = 80         Access = ALL
                   Secure Client IP = 0.0.0.0
SNMP Service:      Port = 161        Access = ALL
                   Secure Client IP = 0.0.0.0
DNS Service:       Port = 53         Access = ALL
                   Secure 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.

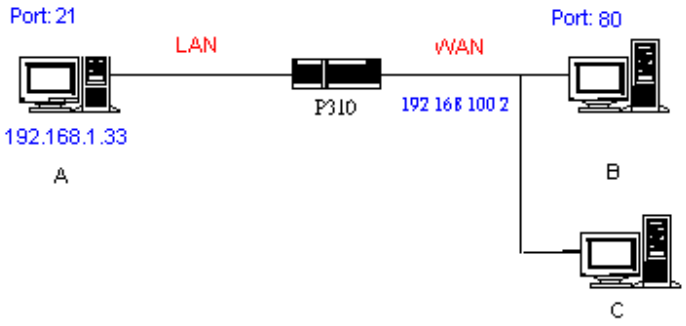
These triggered events can be timed so that they erase the port mapping as soon as they are done with the data transfer, so that the port mapping can be triggered by another Client computer. This gives the ***illusion*** that multiple computers can use the same port mapping at the same time, but the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

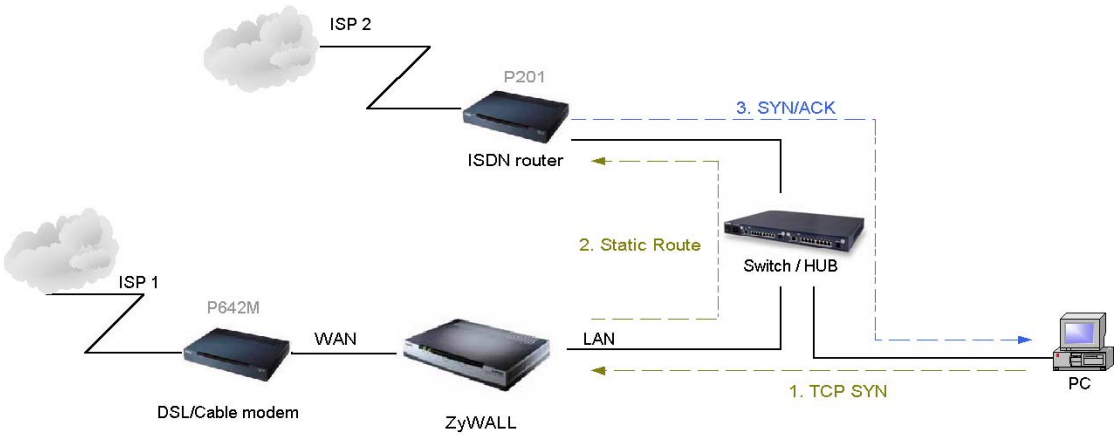


Figure 4-1 Triangle Route

Figure 4-1 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.

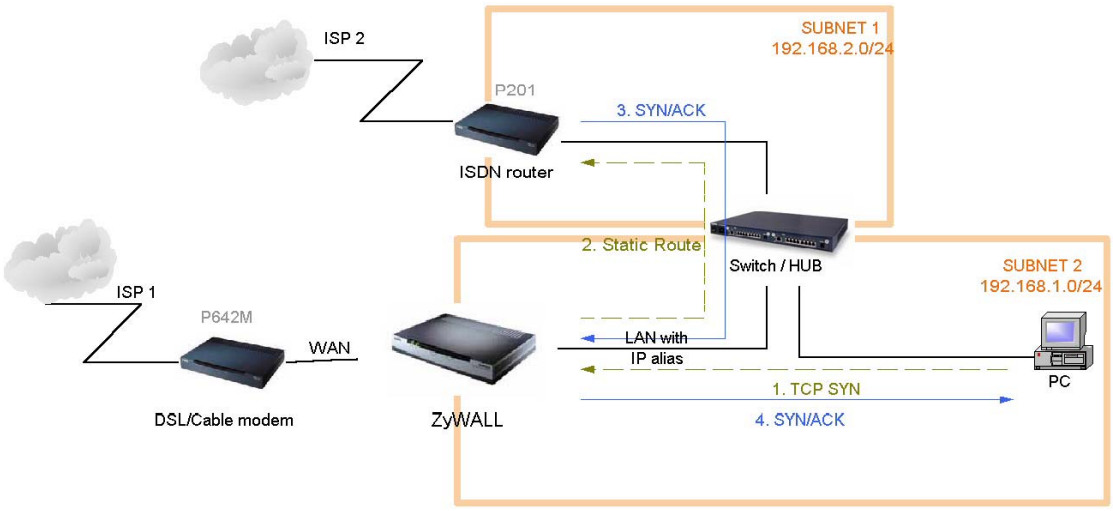


Figure 4-2 Gateway on alias IP network

(2) Gateway on WAN side

A working topology is suggested as below.

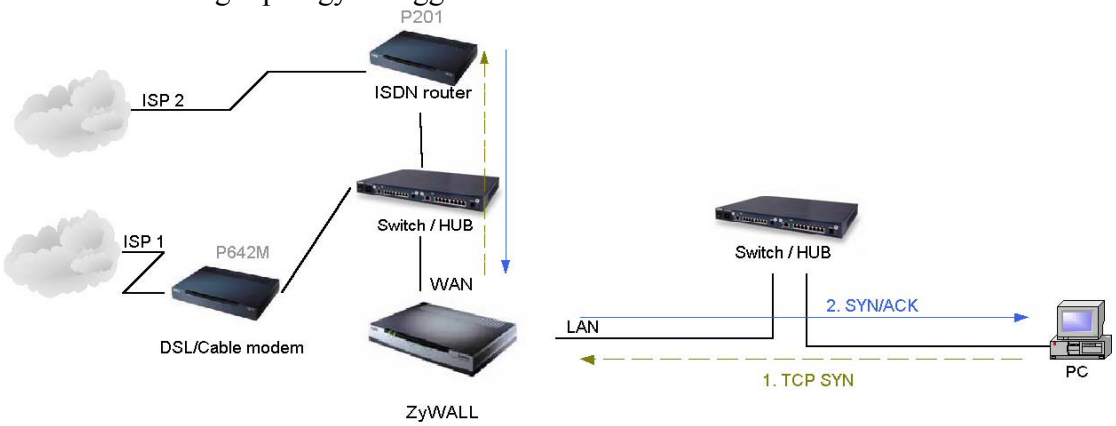


Figure 5-3 Gateway on WAN side

Appendix 5 IPSec FQDN support

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

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

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

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

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

We can put all combinations in to these two tables:

(Local ID Type is IP):

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

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

(Peer ID Type is IP):

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

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

Summary:

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

Appendix 6 Embedded HTTPS proxy server

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

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

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

Annex A CI Command List

Last Updated: 2004/04/27

Command Class List Table		
System Related Command	Exit Command	Device Related Command
Ethernet Related Command	POE Related Command	PPTP Related Command
AUX Related Command	Configuration Related Command	IP Related Command
IPSec Related Command	Bridge Related Command	Bandwidth Management
Firewall Related Command	Certificate Management (PKI) Command	

Flag :
R: This command can be used in Router Mode
B: This command can be used in Bridge Mode

System Related Command Home

Command				Flag	Description
sys					
	adjtime			R + B	retrieve date and time from Internet
	cbuf				
		cnt			cbuf static
			display	R + B	display cbuf static
	callhist				
		display		R	display call history
		remove	<index>	R	remove entry from call history
	countrycode		[countrycode]	R + B	set country code
	date		[year month date]	R + B	set/display date
	debug			R + B	
		romfile		R + B	
			cert [0:reserve/1:erase]	R + B	erase all the certificates
			display	R + B	display romfile debug settings
			isp [0:reserve/1:erase]	R	erase the account and password of ISP
			prekey [0:reserve/1:reset]	R	reset the system IPSec pre-shared key
			profile [0:reserve/1:erase]	R + B	erase the accounts and passwords of 802.1X and XAUTH
			pwd [0:reserve/1:reset]	R + B	reset system password
			radius	R + B	erase Authentication and Accounting keys
			update [0:reserve/1:erase]	R + B	update romfile depend on current configuration
			wep [0:reserve/1:erase]	R + B	erase all WEP encryption keys
	domainname			R + B	display domain name
	edit		<filename>	R + B	edit a text file
	extraphnum			R	maintain extra phone numbers for outcalls
		add	<set 1-3> <1st phone num> [2nd phone num]	R	add extra phone numbers
		display		R	display extra phone numbers
		node	<num>	R	set all extend phone number to remote node <num>
		remove	<set 1-3>	R	remove extra phone numbers
		reset		R	reset flag and mask
	feature			R + B	display feature bit
	hostname		[hostname]	R + B	display system hostname
	logs			R + B	
		category		R + B	

			access [0:none/1:log/2:alert/3:both]	R + B	record the access control logs
			attack [0:none/1:log/2:alert/3:both]	R + B	record and alert the firewall attack logs
			display	R + B	display the category setting
			error [0:none/1:log/2:alert/3:both]	R + B	record and alert the system error logs
			ipsec [0:none/1:log/2:alert/3:both]	R	record the access control logs
			ike [0:none/1:log/2:alert/3:both]	R	record the access control logs
			javablocked [0:none/1:log]	R + B	record the java etc. blocked logs
			mten [0:none/1:log]	R + B	record the system maintenance logs
			packetfilter [0:none/1:log]	R + B	record the packet filter logs
			pki [0:none/1:log/2:alert/3:both]	R	record the pki logs
			tcpreset [0:none/1:log]	R + B	record the tcp reset logs
			upnp [0:none/1:log]	R	record upnp logs
			urlblocked [0:none/1:log/2:alert/3:both]	R + B	record and alert the web blocked logs
			urlforward [0:none/1:log]	R + B	record web forward logs
		clear		R + B	clear log
		display	[access|attack|error|ipsec|ike|javablocked|mten|packetfilter|pki|tcpreset|urlblocked|urlforward]	R + B	display all logs or specify category logs
		errlog		R + B	
			clear	R + B	display log error
			disp	R + B	clear log error
			online	R + B	turn on/off error log online display
		load		R + B	load the log setting buffer
		mail		R + B	
			alertAddr [mail address]	R + B	send alerts to this mail address
			display	R + B	display mail setting
			logAddr [mail address]	R + B	send logs to this mail address
			schedule display	R + B	display mail schedule
			schedule hour [0-23]	R + B	hour time to send the logs
			schedule minute [0-59]	R + B	minute time to send the logs
			schedule policy [0:full/1:hourly/2:daily/3:weekly/4:none]	R + B	mail schedule policy
			schedule week [0:sun/1:mon/2:tue/3:wed/4:thu/5:fri/6:sat]	R + B	weekly time to send the logs
			server [domainName/IP]	R + B	mail server to send the logs
			subject [mail subject]	R + B	mail subject
		save		R + B	save the log setting buffer
		syslog		R + B	
			active [0:no/1:yes]	R + B	active to enable unix syslog
			display	R + B	display syslog setting
			facility [Local ID(1-7)]	R + B	log the messages to different files
			server [domainName/IP]	R + B	syslog server to send the logs
		updateSvrIP	<minute>	R + B	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.
	mbuf			R + B	
		link	link	R + B	list system mbuf link

		pool	<id> [type][num]	R + B	list system mbuf pool
		status		R + B	display system mbuf status
		disp	<address>[1|0]	R + B	display mbuf status
		cnt		R + B	
			disp	R + B	display system mbuf count
			clear	R + B	clear system mbuf count
		debug	[on|off]	R + B	
	mode	<router/bridge>		R + B	switch router and bridge mode
	pwderrtm		[minute]	R + B	Set or display the password error blocking timeout value.
	rn			R	
		load	<entry no.>	R	load remote node information
		disp	<entry no.>(0:working buffer)	R	display remote node information
		nat	<none|sua|full_feature>	R	config remote node nat
		nailup	<no|yes>	R	config remote node nailup
		mtu	<value>	R	set remote node mtu
		save	[entry no.]	R	save remote node information
	smt			R + B	not support in this product
	stdio		[second]	R + B	change terminal timeout value
	time		[hour [min [sec]]]	R + B	display/set system time
	tos			R + B	
		display		R + B	display all runtime TOS
		listPerHost		R + B	display all host session count
		debug	[on|off]	R + B	turn on or off TOS debug message
		sessPerHost	<number>	R + B	configure session per host value
		timeout		R + B	
			display	R + B	display all TOS timeout information
			icmp <idle timeout>	R + B	set idle timeout value
			igmp <idle timeout>	R + B	set idle timeout value
			tcpsyn <idle timeout>	R + B	set idle timeout value
			tcp <idle timeout>	R + B	set idle timeout value
			tcpfin <idle timeout>	R + B	set idle timeout value
			udp <idle timeout>	R + B	set idle timeout value
			gre <idle timeout>	R + B	set idle timeout value
			esp <idle timeout>	R + B	set idle timeout value
			ah <idle timeout>	R + B	set idle timeout value
			other <idle timeout>	R + B	set idle timeout value
	trcdisp	parse, brief, disp		R + B	monitor packets
	trclog			R + B	
	trcpacket			R + B	
	syslog			R + B	
		server	[destIP]	R + B	set syslog server IP address
		facility	<FacilityNo>	R + B	set syslog facility
		type	[type]	R + B	set/display syslog type flag
		mode	[on|off]	R + B	set syslog mode
	version			R + B	display RAS code and driver version
	view		<filename>	R + B	view a text file
	wdog			R + B	
		switch	[on|off]	R + B	set on/off wdog
		cnt	[value]	R + B	display watchdog counts value: 0-34463
	romreset			R + B	restore default romfile
	server				

		access	<telnet|ftp|web|icmp|snmp|dns> <value>	R + B	set server access type
		load		R + B	load server information
		disp		R + B	display server information
		port	<telnet|ftp|web|snmp> <port>	R + B	set server port
		save		R + B	save server information
		secureip	<telnet|ftp|web|icmp|snmp|dns> <ip>	R + B	set server secure ip addr
		certificate	<https|ssh> [certificate name]	R + B	set server certificate
		auth_client	<https> [on|off]	R + B	specifies whether the server authenticates the client
	fwnotify			R + B	
		load		R + B	load fwnotify entry from spt
		save		R + B	save fwnotify entry to spt
		url	<url>	R + B	set fwnotify url
		days	<days>	R + B	set fwnotify days
		active	<flag>	R + B	turn on/off fwnotify flag
		disp		R + B	display firmware notify information
		check		R + B	check firmware notify event
		debug	<flag>	R + B	turn on/off firmware notify debug flag
	cmgr			R + B	
		trace		R + B	
			disp <ch-name>	R + B	show the connection trace of this channel
			clear <ch-name>	R + B	clear the connection trace of this channel
		cnt	<ch-name>	R + B	show channel connection related counter
	socket			R + B	display system socket information
	filter			R + B	
		netbios		R + B	
			disp	R + B	display netbios filter status
			config <0:Between LAN and WAN, 1: Between LAN and DMZ, 2: Between WAN and DMZ, 3:IPSec passthrough, 4:Trigger Dial> <on|off>	R + B	config netbios filter
	roadrunner			R	
		debug	<level>	R	enable/disable roadrunner service 0: diable <default> 1: enable
		display	<iface name>	R	display roadrunner information iface-name: enif0, wanif0
		restart	<iface name>	R	restart roadrunner
	ddns			R + B	
		debug	<level>	R + B	enable/disable ddns service
		display	<iface name>	R + B	display ddns information
		restart	<iface name>	R + B	restart ddns
		logout	<iface name>	R + B	logout ddns
	cpu			R + B	
		display		R + B	display CPU utilization
	upnp			R	
		active	[0:no/1:yes]	R	Activate or deactivate the saved upnp settings
		config	[0:deny/1:permit]	R	Allow users to make configuration changes. through UPnP
		display		R	display upnp information
		firewall	[0:deny/1:pass]	R	Allow UPnP to pass through Firewall.

		load		R	save upnp information
		reserve	[0:no/1:yes]	R	Reserve UPnP NAT rules in flash after system bootup.
		save		R	save upnp information

Exit Command Home

Command				Flag	Description
exit				R + B	exit smt menu

Device Related Command Home

Command				Flag	Description
dev					
	channel				
		drop	<channel_name>	R + B	drop channel
	dial		<node#>	R + B	dial to remote node

Ethernet Related Command Home

Command				Flag	Description
ether				R + B	
	config			R + B	display LAN configuration information
	driver			R + B	
		cnt		R + B	
			disp <name>	R + B	display ether driver counters
		ioctl	<ch_name>	R + B	Useless in this stage.
		mac	<ch_name> <mac_addr>	R	Set LAN Mac address
		status	<ch_name>	R + B	see LAN status
	version			R + B	see ethernet device type
	pkttest				
		disp			
			packet <level>	R + B	set ether test packet display level
			event <ch> [on|off]	R + B	turn on/off ether test event display
		sap	[ch_name]	R + B	send sap packet
		arp	<ch_name> <ip-addr>	R + B	send arp packet to ip-addr
	debug				
		disp	<ch_name>	R + B	display ethernet debug infomation
		level	<ch_name> <level>	R + B	set the ethernet debug level level 0: disable debug log level 1:enable debug log (default)
	edit			R + B	
		load	<ether no.>	R + B	load ether data from spt
		mtu	<value>	R + B	set ether data mtu
		speed	<speed>	R + B	set ether data speed
		save		R + B	save ether data to spt
	dynamicPort				
		dump		U+R+B	display the relation between physical port and channel.
		set	<port> <type>	U+R+B	set physical port belongs to which channel.
		spt		U+R+B	display channel setting stored in SPT.

POE Related Command(All commands can only be used in Router Mode) 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
	proxy	disp		Display PPPoE proxy client session table
		active	[on | off]	Turn on / off PPPoE proxy function
		debug	[on | off]	Turn on / off PPPoE proxy debug function
		time	<interval>	Set the time out interval, it's a count. Actual time is count * 5 seconds.
		init		Initialize PPPoE proxy client session table
		flush		Clear PPPoE proxy client session table

PPTP Related Command (All commands can only be used in Router Mode) Home

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

AUX Related Command (All commands can only be used in Router Mode) Home

Command				Description
aux				
	atring		<device name>	Command the AT command to the device.
	cnt			
		disp	<device name>	display aux counter information
		clear	<device name>	clear aux counter information
	drop		<device name>	disconnect
	init		<device name>	initialize aux channel
	mstatus		<device name>	display modem last call status
	mtype		<device name>	display modem type
	netstat		<device name>	prints upper layer packet information
	rate		<device name>	show tx rx rate
	redirect		<device name>	invalid
	signal		<device name>	show aux signal

Configuration Related Command
(All commands can be used in both Router Mode and Bridge Mode) 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-tim		Edit the wait time for the SYN TCP sessions

			eout <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
			logone <yes|no>		Switch on/off for one packet that create just one log message.
			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.

IP Related Command Home

Command				Flag	Description
ip					
	address		[addr]		display host ip address
	alias		<iface>	R	alias iface
	aliasdis		<0|1>	R	disable alias
	arp				
		status	<iface>		display ip arp status
	dhcp		<iface>	R	
		client		R	
			release	R	release DHCP client IP
			renew	R	renew DHCP client IP
			release <entry num>	R	release specific entry of the dhcp server pool
		status	[option]	R	show dhcp status
	dns			R	
		query		R	
			address <ipaddr> [timeout]	R	resolve ip-addr to name
			Debug <num>	R	enable dns debug value
			Name <hostname> [timeout]	R	resolve name to multiple IP addresses
			Status	R	display dns query status
			Table	R	display dns query table
		server	<primary> [secondary] [third]	R	set dns server
		stats		R	
			Clear	R	clear dns statistics
			Disp	R	display dns statistics
		table		R	display dns table
		default	<ip>	R	Set default DNS server
	Httpd			R + B	
		debug	[on|off]	R + B	set http debug flag
	icmp				
		status		R + B	display icmp statistic counter
		discovery	<iface> [on|off]	R + B	set icmp router discovery flag
	ifconfig		[iface] [ipaddr] [broadcast <addr> |mtu <value>|dynamic]	R + B	configure network interface
	ping		<hostid>	R + B	ping remote host
	route			R	
		status	[if]	R	display routing table
		add	<dest_addr|default>[/<bits>] <gateway> [<metric>]	R	add route
		addiface	<dest_addr|default>[/<bits>] <gateway> [<metric>]	R	add an entry to the routing table to iface
		addprivate	<dest_addr|default>[/<bits>] <gateway>	R	add private route

			[<metric>]		
		drop	<host addr> [/<bits>]	R	drop a route
	status			R + B	display ip statistic counters
	stroute			R	
		display	[rule # | buf]	R	display rule index or detail message in rule.
		load	<rule #>	R	load static route rule in buffer
		save		R	save rule from buffer to spt.
		config		R	
			name <site name>	R	set name for static route.
			destination <dest addr>[/<bits>] <gateway> [<metric>]	R	set static route destination address and gateway.
			mask <IP subnet mask>	R	set static route subnet mask.
			gateway <IP address>	R	set static route gateway address.
			metric <metric #>	R	set static route metric number.
			private <yes|no>	R	set private mode.
			active <yes|no>	R	set static route rule enable or disable.
	udp			R + B	
		status		R + B	display udp status
	tcp			R + B	
		status	[tcb] [<interval>]	R + B	display TCP statistic counters
	telnet		<host> [port]	R + B	execute telnet clinet command
	traceroute		<host> [ttl] [wait] [queries]	R + B	send probes to trace route of a remote host
	xparent			R	
		join	<iface1> [<iface2>]	R	join iface2 to iface1 group
		break	<iface>	R	break iface to leave ipxparent group
	urlfilter			R + B	
		customize		R + B	
			display	R + B	display customize action flags
			actionFlags [filterList/disableAllExceptTrusted/unblockRWFToTrusted/keywordBlock/fullPath/caseInsensitive/fileName][enable/disable]	R + B	set action flags
			logFlags [type(1-3)][enable/disable]	R + B	set log flags
			add [string] [trust/untrust/keyword]	R + B	add url string
			delete [string] [trust/untrust/keyword]	R + B	delete url string
			reset	R + B	clear all information
		general		R + B	
			enable	R + B	enable/disable url filter function
			display	R + B	display content filer's general setting
			webFeature	R + B	[block/nonblock] [activex/java/cookei/webproxy]
			timeOfDay[always/hh:mm] [hh:mm]	R + B	set block time
			exemptZone display	R + B	display exemptzone information
			exemptZone actionFlags [type(1-3)][enable/disable]	R + B	set action flags
			exemptZone add [ip1] [ip2]	R + B	add exempt range
			exemptZone delete [ip1] [ip2]	R + B	delete exempt range
			exemptZone reset	R + B	clear exemptzone information
			reset	R + B	reset content filter's general setting
		webControl		R + B	
			enable	R + B	enable cbr_filter
			display	R + B	display cbr_filter's setting
			logAndBlock [log/block/both]	R + B	set log or block on matched web site

			category	R + B	set blocked categories
			serverList display	R + B	display current cbr_filter servers
			serverList refresh	R + B	refresh cbr_filter servers
			queryURL [url][Server/localCache]	R + B	query url need to block or forward according the database on server or local cache
			cache display	R + B	display the local cache entries
			cache delete [entrynum/All]	R + B	delete the local cache entries
			cache timeout [hour]	R + B	Set timeout value of cache entries
			blockonerror [log/block][on/off]	R + B	choose log or block when server is unavailable
			waitingTime [sec]	R + B	set waiting time for server
			reginfo display	R + B	display the license key with cerberian
			reginfo	R + B	No used
			zssw	R + B	change the zssw's URL
	tredir			R	
		failcount	<count>	R	set tredir failcount
		partner	<ipaddr>	R	set tredir partner
		target	<ipaddr>	R	set tredir target
		timeout	<timeout>	R	set tredir timeout
		checktime	<period>	R	set tredir checktime
		active	<on|off>	R	set tredir active
		save		R	save tredir information
		disp		R	display tredir information
		debug	<value>	R	set tredir debug value
	rpt			R + B	
		start		R + B	start report
		stop		R + B	stop report
		url	[num]	R + B	top url hit list
		ip	[num]	R + B	top ip addr list
		srv	[num]	R + B	top service port list
	dropIcmp		[0 | 1]	R + B	to drop ICMP fragment packets
	nat			R	
		period	[period]	R	set nat timer period
		port	[port]	R	set nat starting external port number
		checkport		R	verify all server tables are valid
		timeout		R	
			gre [timeout]	R	set nat gre timeout value
			iamt [timeout]	R	set nat iamt timeout value
			generic [timeout]	R	set nat generic timeout value
			reset [timeout]	R	set nat reset timeout value
			tcp [timeout]	R	set nat tcp timeout value
			tcpother [timeout]	R	set nat tcp other timeout value
			udp [port] <value>	R	set nat udp timeout value of specific port
		update		R	create nat system information from spSysParam
		iamt	<iface>	R	display nat iamt information
		iface	<iface>	R	show nat status of an interface
		lookup	<rule set>	R	display nat lookup rule
		new-lookup	<rule set>	R	display new nat lookup rule
		loopback	[on|off]	R	turn on/off nat loopback flag
		reset	<iface>	R	reset nat table of an iface
		server		R	

			disp	R	display nat server table
			load <set id>	R	load nat server information from ROM
			save	R	save nat server information to ROM
			clear <set id>	R	clear nat server information
			edit active <yes|no>	R	set nat server edit active flag
			edit svrport <start port> [end port]	R	set nat server server port
			edit intport <start port> [end port]	R	set nat server forward port
			edit remotehost <start ip> [end ip]	R	set nat server remote host ip
			edit leasetime [time]	R	set nat server lease time
			edit rulename [name]	R	set nat server rule name
			edit forwardip [ip]	R	set nat server server ip
			edit protocol [protocol id]	R	set nat server protocol
			edit clear	R	clear one rule in the set
		service		R	
			irc [on|off]	R	turn on/off irc flag
			xboxlive [on|off]	R	turn on/off xboxlive flag
		resetport		R	reset all nat server table entries
		incikeport	<iface>[on|off]	R	turn on/off increase ike port flag
		session	[session per host]	R	set nat session per host value
		deleteslot	<iface> <slot>	R	delete specific slot of iface
		debug		R	
			natTraversal [on|off]	R	set NAT traversal debug flag
			hash [on|off]	R	set NAT hash table debug flag
			session [on|off]	R	set NAT session debug flag
		hashtable	<enifX, X=0, 1, 2, …>	R	show the NAT hash table of enifX
	igmp			R	
		debug	[level]	R	set igmp debug level
		forwardall	[on|off]	R	turn on/off igmp forward to all interfaces flag
		querier	[on|off]	R	turn on/off igmp stop query flag
		iface		R	
			<iface> grouptm <timeout>	R	set igmp group timeout
			<iface> interval <interval>	R	set igmp query interval
			<iface> join <group>	R	join a group on iface
			<iface> leave <group>	R	leave a group on iface
			<iface> query	R	send query on iface
			<iface> rsptime [time]	R	set igmp response time
			<iface> start	R	turn on of igmp on iface
			<iface> stop	R	turn off of igmp on iface
			<iface> ttl <threshold>	R	set ttl threshold
			<iface> v1compat [on|off]	R	turn on/off v1compat on iface
		robustness	<num>	R	set igmp robustness variable
		status		R	dump igmp status

IPSec Related Command (All commands can only be used in Router Mode) Home

Command				Description
ipsec				
	debug	<1|0>		turn on|off trace for IPsec debug information
	ipsec_log_disp			show IPSec log, same as menu 27.3
	route	dmz	<on|off>	After a packet is IPSec processed and will be sent to DMZ side, this switch is to control if this packet can be applied IPSec again.
				Remark: Only supported in ZyWALL100

		lan	<on|off>	After a packet is IPSec processed and will be sent to LAN side, this switch is to control if this packet can be applied IPSec again.
				Remark: Command available since 3.50(WA.3)
		wan	<on|off>	After a packet is IPSec processed and will be sent to WAN side, this switch is to control if this packet can be applied IPSec again.
				Remark: Command available since 3.50(WA.3)
	show_runtime	sa		display runtime phase 1 and phase 2 SA information
		spd		When a dynamic rule accepts a request and a tunnel is established, a runtime SPD is created according to peer local IP address. This command is to show these runtime SPD.
	switch	<on|off>		As long as there exists one active IPSec rule, all packets will run into IPSec process to check SPD. This switch is to control if a packet should do this. If it is turned on, even there exists active IPSec rules, packets will not run IPSec process.
	timer	chk_my_ip	<1~3600>	- Adjust timer to check if WAN IP in menu is changed
				- Interval is in seconds
				- Default is 10 seconds
				- 0 is not a valid value
		chk_conn.	<0~255>	- Adjust auto-timer to check if any IPsec connection has “only outbound traffic but no inbound 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
		chk_input	<0~255>	- Adjust input timer to check if any IPSec connection has no inbound traffic for a certain period. If yes, system will disconnect it.
				- Interval is in minutes
				- Default is 2 minuets
				- 0 means never timeout
				Remark: Command available since 3.50(WA.3)
	updatePeerIp			Force system to update IPSec rules which use domain name as the secure gateway IP right away.
				Remark: Command available since 3.50(WA.3)
	dial	<rule #>		Initiate IPSec rule <#> from ZyWALL box
				Remark: Command available since 3.50(WA.3)
	display	<rule #>		Display IPSec rule #
	remote	key	<string>	I add a secured remote access tunnel with pre-shared key. It is a dynamic rule with local: the route’s WAN IP. The algorithms with it are fixed to phase1: DES+MD5, DH1 and SA lifetime 28800 seconds; phase2: DES+MD5, PFS

				off, no anti-replay and SA lifetime 28800 seconds. The length of pre-shared key is between 8 to 31 ASCII characters.
		switch	<on|off>	Activate or de-activate the secured remote access tunnel.
	keep_alive	<rule #>	<on|off>	Set ipsec keep_alive flag
	load	<rule #>		Load ipsec rule
	save			Save ipsec rules
	config	netbios	active <on|off>	Set netbios active flag
			group <group index1, group index2…>	Set netbios group
		name	<string>	Set rule name
		active	<Yes | No>	Set active or not
		keeyAlive	<Yes| No>	Set keep alive or not
		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
		dnsServer	<IP>	Set DNS server for IPSec VPN
		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
			encap <0:Tunnel | 1:Transport>	set encapsulation in phase 2 in IKE
			pfs <0:None | 1:DH1 | 2:DH2>	set pfs in phase 2 in IKE
		manual	activeProtocol <0:AH | 1:ESP>	Set active protocol in manual

		manual ah	encap <0:Tunnel | 1:Transport>	Set encapsulation in ah in manual
			spi <decimal>	Set spi in ah in manual
			authAlgo <0:MD5 | 1:SHA1>	Set authentication algorithm in ah in manual
			authKey <string>	Set authentication key in ah in manual
		manual esp	encap <0:Tunnel | 1:Transport>	Set encapsulation in esp in manual
			spi <decimal>	Set spi in esp in manual
			encryAlgo <0:Null | 1:DES | 2:3DES>	Set encryption algorithm in esp in manual
			encryKey <string>	Set encryption key in esp in manual
			authAlgo <0:MD5 | 1:SHA1>	Set authentication algorithm in esp in manual
			authKey < string>	Set authentication key in esp in manual
	swSkipOverlapIp		<on|off>	- When a VPN rule with remote range overlaps with local range, the switch decides if a local to local packet should apply this rule. - 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 (All command can be used in both Router Mode and Bridge Mode) 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.
		dynamicrule			
			display		Display firewall dynamic rules
		tcprst			
			rst		Set TCP reset sending on/off.
			rst113		Set TCP reset sending for port 113 on/off.
			display		Display TCP reset sending setting.
		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
		schedule			

			load [set # rule #]		Load firewall ACL schedule by rule.
			display		Display ACL schedule in buffer.
			save		Save buffer date and update runtime firewall ACL rule.
			week		
				monday [on/off]	Set schedule on or off by day – Monday.
				tuesday [on/off]	Set schedule on or off by day – Tuesday.
				wednesday [on/off]	Set schedule on or off by day – Wednesday.
				thursday [on/off]	Set schedule on or off by day – Thursday.
				friday [on/off]	Set schedule on or off by day – Friday.
				saturday [on/off]	Set schedule on or off by day – Saturday.
				sunday [on/off]	Set schedule on or off by day – Sunday.
				allweek [on/off]	Quick set schedule on or off by week.
			timeOfDay [always/hh:mm]		Set firewall ACL schedule block time of day.

Certificate Management (PKI) Command
(All commands can be used in both Router Mode and Bridge Mode) Home

Command				Description
certificates				
	my_cert			
		create		
			selfsigned <name> <subject> [key size]	Create a self-signed local host certificate. <name> specifies a descriptive name for the generated certificate. <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn;{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.
			request <name> <subject> [key size]	Create a certificate request and save it to the router for later manual enrollment. <name> specifies a descriptive name for the generated certification request. <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn;{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.
			scep_enroll <name> <CA addr> <CA cert> <auth key> <subject> [key size]	Create a certificate request and enroll for a certificate immediately online using SCEP protocol. <name> specifies a descriptive name for the enrolled certificate. <CA addr> specifies the CA server address. <CA cert> specifies the name of the CA certificate. <auth key> specifies the key used for user authentication. If the key contains spaces, please put it in quotes. To leave it blank, type "". <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn;{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.
			cmp_enroll	Create a certificate request and enroll for a certificate immediately

			<name> <CA addr> <CA cert> <auth key> <subject> [key size]	online using CMP protocol. <name> specifies a descriptive name for the enrolled certificate. <CA addr> specifies the CA server address. <CA cert> specifies the name of the CA certificate. <auth key> specifies the id and key used for user authentication. The format is "id:key". To leave the id and key blank, type ":". <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn;{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.
		import [name]		Import the PEM-encoded certificate from stdin. [name] specifies the descriptive name (optional) as which the imported certificate is to be saved. For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on ZyWALL. After the importation, the certification request will automatically be deleted. If a descriptive name is not specified for the imported certificate, the certificate will adopt the descriptive name of the certification request.
		export <name>		Export the PEM-encoded certificate to stdout for user to copy and paste. <name> specifies the name of the certificate to be exported.
		view <name>		View the information of the specified local host certificate. <name> specifies the name of the certificate to be viewed.
		verify <name> [timeout]		Verify the certification path of the specified local host certificate. <name> specifies the name of the certificate to be verified. [timeout] specifies the timeout value in seconds (optional). The default timeout value is 20 seconds.
		delete <name>		Delete the specified local host certificate. <name> specifies the name of the certificate to be deleted.
		list		List all my certificate names and basic information.
		rename <old name> <new name>		Rename the specified my certificate. <old name> specifies the name of the certificate to be renamed. <new name> specifies the new name as which the certificate is to be saved.
		def_selfsigned [name]		Set the specified self-signed certificate as the default self-signed certificate. [name] specifies the name of the certificate to be set as the default self-signed certificate. If [name] is not specified, the name of the current self-signed certificate is displayed.
	ca_trusted			
		import <name>		Import the PEM-encoded certificate from stdin. <name> specifies the name as which the imported CA certificate is to be saved.
		export <name>		Export the PEM-encoded certificate to stdout for user to copy and paste. <name> specifies the name of the certificate to be exported.
		view <name>		View the information of the specified trusted CA certificate. <name> specifies the name of the certificate to be viewed.
		verify <name> [timeout]		Verify the certification path of the specified trusted CA certificate. <name> specifies the name of the certificate to be verified. [timeout] specifies the timeout value in seconds (optional). The default timeout value is 20 seconds.
		delete <name>		Delete the specified trusted CA certificate. <name> specifies the name of the certificate to be deleted.
		list		List all trusted CA certificate names and basic information.
		rename <old name> <new name>		Rename the specified trusted CA certificate. <old name> specifies the name of the certificate to be renamed. <new name> specifies the new name as which the certificate is to be saved.
		crl_issuer		Specify whether or not the specified CA issues CRL. <name>

		<name> [on|off]		specifies the name of the CA certificate. [on|off] specifies whether or not the CA issues CRL. If [on|off] is not specified, the current crl_issuer status of the CA.
	remote_trusted			
		import <name>		Import the PEM-encoded certificate from stdin. <name> specifies the name as which the imported remote host certificate is to be saved.
		export <name>		Export the PEM-encoded certificate to stdout for user to copy and paste. <name> specifies the name of the certificate to be exported.
		view <name>		View the information of the specified trusted remote host certificate. <name> specifies the name of the certificate to be viewed.
		verify <name> [timeout]		Verify the certification path of the specified trusted remote host certificate. <name> specifies the name of the certificate to be verified. [timeout] specifies the timeout value in seconds (optional). The default timeout value is 20 seconds.
		delete <name>		Delete the specified trusted remote host certificate. <name> specifies the name of the certificate to be deleted.
		list		List all trusted remote host certificate names and basic information.
		rename <old name> <new name>		Rename the specified trusted remote host certificate. <old name> specifies the name of the certificate to be renamed. <new name> specifies the new name as which the certificate is to be saved.
	dir_service			
		add <name> <addr[:port]> [login:pswd]		Add a new directory service. <name> specifies a descriptive name as which the added directory server is to be saved. <addr[:port]> specifies the server address (required) and port (optional). The format is "server-address[:port]". The default port is 389. [login:pswd] specifies the login name and password, if required. The format is "[login:password]".
		delete <name>		Delete the specified directory service. <name> specifies the name of the directory server to be deleted.
		view <name>		View the specified directory service. <name> specifies the name of the directory server to be viewed.
		edit <name> <addr[:port]> [login:pswd]		Edit the specified directory service. <name> specifies the name of the directory server to be edited. <addr[:port]> specifies the server address (required) and port (optional). The format is "server-address[:port]". The default port is 389. [login:pswd] specifies the login name and password, if required. The format is "[login:password]".
		list		List all directory service names and basic information.
		rename <old name> <new name>		Rename the specified directory service. <old name> specifies the name of the directory server to be renamed. <new name> specifies the new name as which the directory server is to be saved.
	cert_manager			
		reinit		Reinitialize the certificate manager.

Command						Description
bm						
	interface	lan	enable	<bandwidth xxx>		Enable bandwidth management in LAN with bandwidth xxx bps. If the user doesn't set the bandwidth, the default value is 100Mbps.
				<wrr|prr>		Select fairness-based(WRR) or priority-based(PRR) mechanism. the default value is fairness-based.
				<efficient>		Enable work-conserving feature.
			disable			Disable bandwidth management in LAN
		wan	enable	<bandwidth xxx>		Enable bandwidth management in WAN with bandwidth xxx bps. If the user doesn't set the bandwidth, the default value is 100Mbps.
				<wrr|prr>		Select fairness-based(WRR) or priority-based(PRR) mechanism. the default value is fairness-based.
				<efficient>		Enable work-conserving feature.
			disable			Disable bandwidth management in WAN
		dmz	enable	<bandwidth xxx>		Enable bandwidth management in DMZ with bandwidth xxx bps. If the user doesn't set the bandwidth, the default value is 100Mbps.
				<wrr|prr>		Select fairness-based(WRR) or priority-based(PRR) mechanism. the default value is fairness-based.
				<efficient>		Enable work-conserving feature.
			disable			Disable bandwidth management in DMZ
		wlan	enable	<bandwidth xxx>		Enable bandwidth management in WLAN with bandwidth xxx bps. If the user doesn't set the bandwidth, the default value is 100Mbps.
				<wrr|prr>		Select fairness-based(WRR) or priority-based(PRR) mechanism. the default value is fairness-based.
				<efficient>		Enable work-conserving feature.
			disable			Disable bandwidth management in WLAN
	class	lan	add #	bandwidth xxx	<name xxx>	Add a class with bandwidth xxx bps in LAN. The name is for users' information.
					<priority x>	Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The default value is 3.
					<borrow on|off>	The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The default value is off.
			mod #	<bandwidth xxx>		Modify the parameters of the class in LAN. The bandwidth is unchanged if the user doesn't set a new value.
				<name xxx>		Set the class' name.
				<priority x>		Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The priority is unchanged if the user doesn't set a new value.
				<borrow on|off>		The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The borrow is unchanged if the user doesn't set a new value.
			del #			Delete the class # and its filter and all its children class and their filters in LAN.
		wan	add #	bandwidth xxx	<name xxx>	Add a class with bandwidth xxx bps in WAN. The name is for users' information.
					<priority x>	Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The default value is 3.
					<borrow on|off>	The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The default value is off.
			mod #	<bandwidth xxx>		Modify the parameters of the class in WAN. The bandwidth is unchanged if the user doesn't set a new value.

				<name xxx>		Set the class' name.
				<priority x>		Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The priority is unchanged if the user doesn't set a new value.
				<borrow on|off>		The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The borrow is unchanged if the user doesn't set a new value.
			del #			Delete the class # and its filter and all its children class and their filters in WAN.
		dmz	add #	bandwidth xxx	<name xxx>	Add a class with bandwidth xxx bps in DMZ. The name is for users' information.
					<priority x>	Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The default value is 3.
					<borrow on|off>	The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The default value is off.
			mod #	<bandwidth xxx>		Modify the parameters of the class in DMZ. The bandwidth is unchanged if the user doesn't set a new value.
				<name xxx>		Set the class' name.
				<priority x>		Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The priority is unchanged if the user doesn't set a new value.
				<borrow on|off>		The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The borrow is unchanged if the user doesn't set a new value.
			del #			Delete the class # and its filter and all its children class and their filters in DMZ.
		wlan	add #	bandwidth xxx	<name xxx>	Add a class with bandwidth xxx bps in WLAN. The name is for users' information.
					<priority x>	Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The default value is 3.
					<borrow on|off>	The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The default value is off.
			mod #	<bandwidth xxx>		Modify the parameters of the class in WLAN. The bandwidth is unchanged if the user doesn't set a new value.
				<name xxx>		Set the class' name.
				<priority x>		Set the class' priority. The range is between 0 (the lowest) to 7 (the highest). The priority is unchanged if the user doesn't set a new value.
				<borrow on|off>		The class can borrow bandwidth from its parent class when the borrow is set on, and vice versa. The borrow is unchanged if the user doesn't set a new value.
			del #			Delete the class # and its filter and all its children class and their filters in WLAN.
	filter	lan	add #	Daddr <mask Dmask> Dport Saddr <mask Smask> Sport protocol		Add a filter for class # in LAN. The filter contains destination address (netmask), destination port, source address (netmask), source port and protocol. You may set the value as 0 if you do not care the item.
			del #			Delete a filter which belongs to class # in LAN.
		wan	add #	Daddr <mask Dmask> Dport Saddr <mask Smask> Sport protocol		Add a filter for class # in WAN. The filter contains destination address (netmask), destination port, source address (netmask), source port and protocol. You may set the value as 0 if you do not care the item.
			del #			Delete a filter which belongs to class # in WAN.
		dmz	add #	Daddr <mask Dmask> Dport Saddr		Add a filter for class # in DMZ. The filter contains destination address (netmask), destination port, source

				<mask Smask> Sport protocol		address (netmask), source port and protocol. You may set the value as 0 if you do not care the item.
			del #			Delete a filter which belongs to class # in DMZ.
		wlan	add #	Daddr <mask Dmask> Dport Saddr <mask Smask> Sport protocol		Add a filter for class # in WLAN. The filter contains destination address (netmask), destination port, source address (netmask), source port and protocol. You may set the value as 0 if you do not care the item.
			del #			Delete a filter which belongs to class # in WLAN.
	show	interface	lan			Show the interface settings of LAN
			wan			Show the interface settings of WAN
			dmz			Show the interface settings of DMZ
			wlan			Show the interface settings of WLAN
		class	lan			Show the classes settings of LAN
			wan			Show the classes settings of WAN
			dmz			Show the classes settings of DMZ
			wlan			Show the classes settings of WLAN
		filter	lan			Show the filters settings of LAN
			wan			Show the filters settings of WAN
			dmz			Show the filters settings of DMZ
			wlan			Show the filters settings of WLAN
		statistics	lan			Show the statistics of the classes in LAN
			wan			Show the statistics of the classes in WAN
			dmz			Show the statistics of the classes in DMZ
			wlan			Show the statistics of the classes in WLAN
	monitor	lan	<#>			Monitor the bandwidth of class # in LAN. If the class is not specific, all the classes in LAN will be monitored. The first time you key the command will set it on; the second time you will set it off, and so on.
		wan	<#>			Monitor the bandwidth of class # in WAN. If the class is not specific, all the classes in WAN will be monitored. The first time you key the command will set it on; the second time you will set it off, and so on.
		dmz	<#>			Monitor the bandwidth of class # in DMZ. If the class is not specific, all the classes in DMZ will be monitored. The first time you key the command will set it on; the second time you will set it off, and so on.
		wlan	<#>			Monitor the bandwidth of class # in WLAN. If the class is not specific, all the classes in WLAN will be monitored. The first time you key the command will set it on; the second time you will set it off, and so on.
	config	save				Save the configuration.
		load				Load the configuration.
		clear				Clear the configuration.

Bridge Related Command Home

Command				Flag	Description
bridge				R + B	
	cnt			R + B	related to bridge routing statistic table
		disp		R + B	display bridge route counter
		clear		R + B	clear bridge route counter

	iface			R + B	Related to “bridge mode” access interface
		active	<yes/no>	R + B	Active bridge mode iface or not
		address	[ip]	B	Remote access IP address
		dns1	[ip]	B	First DNS server
		dns2	[ip]	B	Second DNS server
		dns3	[ip]	B	Third DNS server
		mask	[network mask]	B	Network mask
		gateway	[gateway ip]	B	Network gateway
		display		B	Display whole interface information
	stat			R + B	related to bridge packet statistic table
		disp		R + B	display bridge route packet counter
		clear		R + B	clear bridge route packet counter