ZyXEL

Firmware Release Note

ZyWALL 70

Release 4.00(WM.1)

Date:	**Sep, 29, 2005**
Author:	**Tim Tseng**
Project Leader:	**Stanley Liu**

ZyXEL ZyWALL 70 Standard Version
Release 4.00(WM.1)
Release Note

Date: Sep 29, 2005

Supported Platforms:

ZyXEL ZyWALL 70

Versions:

ZyNOS Version: V4.00 (WM.1) | 09/29/2005
BootBase : V1.08 | 07/04/2005

Notes:

1. **Restore to Factory Defaults Setting Requirement: No.**
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. When firewall turns from "off" to "on", the firewall initialization procedure will disconnect all connections running through the ZyWALL.
5. SUA/NAT address loopback feature was enabled on ZyWALL by default, however, if users do not need it, a C/I command "ip nat loopback off" could turn it off.
6. In WLAN configuration, a switch for enable / disable WLAN is added. The default value is “disable” since WLAN without any security setting is vulnerable. Please configure MAC filter, WEP, 802.1X and WPA when you enable WLAN feature.
7. When UPnP is on, and then reboot the ZyWALL, Windows XP will not detect UPnP and refresh “My Network Places→Local Network”. Plug in network wire again can solve this problem.
8. If the encapsulation type of WAN1 and WAN2 are both PPTP, The PPTP IP settings (My IP Addr, My IP Mask and Server IP Addr) on WAN1 and WAN2 must be different subnet.
9. The first two entries for static route are reserved for creating WAN1 and WAN2 default routes and are READ-ONLY.
10. In bridge mode, If LAN side DHCP clients want to get DHCP address from WAN side DHCP server, you may need to add and turn on the firewall rule for BOOT_CLIENT service type in WAN→LAN direction.
11. In previous 3.64 firmware, the VID value of DPD is not correct. VID change will

cause current version doesn't work with the wrong value. Please be sure to connect with devices which has updated VID, or the DPD may not work correctly.

12. In SMT menu 24.1, "WCRD" only represents the WLAN card status when you insert WLAN card into the ZyWALL. If you insert TRUBO card, you will see "WCRD" is always down.
13. If you do not want a mail to be scanned by Anti-Spam feature, you can add this mail into white list in eWC->Anti-Spam->Lists
14. If you had activated content filtering service but the registration service state is "Inactive" after upgrading to 4.00, please click "Service License Refresh" in "eWC->REGISTRATION->Registration" or wait until device synchronize with myzyxel.com

Known Issues:

[Interface]

1. Currently, ZyWALL Multiple WAN does not support WAN 1/WAN 2 on the same sub-net. If you configure WAN 1 and WAN 2 to "Ethernet" encapsulation, you should not connect then to the same IP subnet.
2. You must notice those metric values of WAN 1, WAN 2, Traffic-Redirect and Dial-backup. You should better give those values, Dial-backup > Traffic-Redirect > WAN 2 > WAN 1. For example, WAN 1(1), WAN 2(2), Traffic-Redirect(14), Dial-backup(15).

[UPnP]

1. Sometimes on screen the "Local Area Connection" icon for UPnP disappears. The icon shows again when restarting PC.
2. 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..
3. If you were using MSN Messenger Voice Communication through ZyWALL UPnP and found voice is blocked by firewall, we suggest you download MSN Messenger 7.0 and try again. This is because we found MSN Messenger 6.2 sometimes fails to detect UPnP status when it's starting voice invitation.

[Bandwidth Management]

1. Bandwidth Management doesn't work on wireless LAN.
2. Bandwidth management H.323 service does not support Netmeeting H.323 application.
3. Using BWM in PPPoE/PPTP mode, there are two filters for FTP and H323 ALG
   (1) If we execute FTP first then H323 can not pass through ZyWALL.
   (2) If we execute H323 before FTP, all functions work properly.
4. In some cases, BWM (Fairness-Based mode) cannot manage bandwidth accurately. Ex. In WAN interface, there are two subclasses for FTP service, their speed are 100Kbps and 500Kbps, the traffic match the filter which speed is 500Kbps may only use half of it's bandwidth.

[Content Filter]

1. Can't block ActiveX in some case.(Windows will cache it in C:\WINNT\Downloaded Program Files\)

[Bridge Mode]

1. 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.
2. Under Bridge Mode, all DMZ ports will behave as a hub.
3. Don't use CI command "bridge rstp bridge enable" to enable RSTP", it will change the initial Path Cost value to an incorrect value..

[WLAN]

1. G-100 WLAN card, does not support the fragment size below 800.
2. Device sometimes crash when use wireless for a long time.

[Firewall]

1. Some limitations on Firewall CLI configuration, (1) User can not delete specific address or custom port entry from a rule. (2) CLI doesn't support Modify and Move for rules implemented in eWC. (3) eWC can not display firewall rule field correctly if rule is added by CI command and its type is port/address range.

[ALG]

1. Symptom:P2002 can not connect with each other in Peer-to-Peer mode.
   Condition
   Topology:
   P2002--(LAN)ZyWALL_A(WAN, IP=172.21.2.151)--(WAN, IP=172.21.1.134)ZyWALL_B(LAN)--P2002
   (1) In ZyWALL_A and ZyWALL_B, add a "WAN to LAN" firewall rule to pass traffic with port "5060".
   (2) In ZyWALL_A and ZyWALL_B, add a port forwarding rule "5060" to P2002.
   (3) In ZyWALL_A and ZyWALL_B, enable SIP ALG.
   (4) Setup both P2002 to Peer-to-Peer mode.
   (5) Making the SIP connection by P2002 will be failed.
   (6) Turn off firewall in ZyWALL_A and ZyWALL_B, sometimes the connnection can be built up if we dial from P2002 which is behind ZyWALL_A.

[Anti-Spam]

Current Anti-Spam feature works fine when (1) network quality is stable and good , (2) delivered mail size is small, and (3) not many mails in the same mail session. But if users environment does not satisfy all of above conditions, the following problems may happen:

1. Anti-Spam external database query timeout rate will increase when the traffic through device is heavy or when the internet traffic is busy.
2. Symptom: Mail can not be delivered successfully.
   Condition:
   Topology: Mail Client ----- ZyWALL_A---- ZyWALL_B--- Mail Server
   (1) Turn on Anti-Spam at ZyWALL A and B.
   (2) Mail Client send mail to Mail Server.
   (3) Sometimes mail can not be sent successfully.
   (4) The situation also happens when mail client receive mail.
3. Symptom: Mail can not be delivered successfully.
   Condition:
   Topology: Mail Client ----- ZyWALL_A--- Mail Server

(1) Turn on Anti-Spam at ZyWALL A
(2) Mail Client send mail to Mail Server.
(3) Sometimes ZyWALL_A may deliver incorrect mail content to Mail Server.
(4) The situation also happens when mail client receive mail.

4. When Anti-Spam is enabled, sometimes users may see an abnormal repeated count number for the LOG "Exceed maximum mail sessions" in eWC->LOGS.
5. When Anti-Spam is enabled, sometimes some mails may be logged as "query timeout" in LOGS but not tagged with the user-specified timeout string.

[MISC]

1. Symptom: ZyWALL crashes with WAN2 interface.
   Condition:
   (1) Connect internet with WAN2.
   (2) Generate heavy traffic from LAN to WAN.
   (3) When the WAN2's metric is down, pull and plug WAN2 and router crashes.
2. Symptom: Sometimes the device will hang and reboot after “Email Log Now” in bridge mode.
   Condition:
   Topology: PC ----- (LAN)ZyWALL_BridgeMode(WAN) ----- Internet(Mail Server/Mail Recipient)
   (1) Set the device as Bridge mode.
   (2) Configure eWC->LOGS: “E-mail Log Settings“.
   (3) Click eWC->“Email Log Now” to send log mail,
   (4) System will hang and then reboot by software watchdog.
3. When device is performing (a) device registration, (b) service registration or refresh, or (c) signature update, users will see the following message in centralized log: "Due to error code(11), cert not trusted: SSL/TLS peer certif..." This is an expected condition and will not impact the correct behavior of registration or signature update. Please do not worry about this message. This issue will be solved in future patch release.

Features:

Modifications in V 4.00(WM.1) | 09/29/2005

Modify for formal release

Modifications in V 4.00(WM.1)b2 | 09/21/2005

1. [BUG FIX]
   Symptom: Content filter was registered in router mode and changed to bridge mode without configure DNS server. One PC open a web site can make DUT crash.
   Condition:
   (1) In router mode, register content filter and enable it. Edit eWC/Content Filter/Categories/Select Categories, and enable some items(Pornography, Business, Gambling,…,etc)
   (2) Change DUT to bridge mode without configure DNS server.
   (3) PC1 on LAN open a website, and IE would show “block(DNS resolving failed)”
   (4) DUT crashed.

Modifications in V 4.00(WM.1)b1 | 09/12/2005

1. [ENHANCEMENT]
   Add CI command "ip urlfiler bypass [LAN/DMZ/WAN] [ON/OFF]" to let traffic matches LAN->LAN, DMZ->DMZ or WAN->WAN directions can be bypassed content filtering.
   NOTE: (1) This is a runtime CI command, user can add it into autoexec.net.
   (2) This command only support in router mode.
2. [ENHANCEMENT]
   Periodically sending the keep-alive zero window TCP ACK when the AS engine handles the mail. The default value is 5 seconds.
3. [BUG FIX] 050830189
   Symptom: Enable AS ”Discard SMTP mail” and send a mail with attached file will cause the device hangs up (ZW 5,35,70)
   Condition:
   (1) Enable AS ”Discard SMTP mail”
   (2) Send a over 20k sized mail
   (3) The device hangs up
4. [BUG FIX] 050831205
   Symptom: Device will crash if users turn on myZyxelCom debug message then process device registration and trial service activation.
   Condition:
   (1) Turn on myzyxel.com debug message by "sys myZyxelCom debug type 3"
   (2) Go to eWC>REGISTRATION, register device and activate trial service for Content Filter.
   (3) Device will crash.
5. [BUG FIX] 050701018
   Symptom: DHCP client gets IP failed!
   Condition:
   (1) Topology
   original: PC --- (192.168.1.1) Router
   switch to: PC --- (192.168.70.250) DUT
   (2) PC connects to the router LAN port with DHCP, and get an IP.
   (3) DUT set a static DHCP rule for the PC.
   (4) PC switch to DUT, and gets an IP failed. The user must release IP manually, then PC will get IP successfully.
6. [BUG FIX]
   Symptom: ZyWALL sends [HASH][DELETE] to delete VPN tunnel after output timed-out even they keeps traffic via the tunnel.
   Condition: PC1 -----ZyWALL----------PC2(Zywall VPN client)
   (L) (W) |----------PC3(Zywall VPN client)
   (1). Configure a dynamic VPN-rule in the ZyWALL.
   (2). Establish first VPN tunnel by PC2 using ZyWALL VPN client.
   (3). Establish Second VPN tunnel by PC3 using ZyWALL VPN client.
   (4). Both PC2 and PC3s’ PCs keep ping to PC1.
   (5). ZyWALL sends [HASH][DEL] to 2nd VPN peer only every 2 minutes which is output Idle time-out timer.

7. [BUG FIX] 050907311
   Symptom: Bridge mode VPN can't work if configure by Wizard.
   Condition:
   (1) Configure bridge mode VPN with wizard.
   (2) Dial VPN rule and it always fail.
8. [BUG FIX] 050907308
   Symptom: Device will hang forever when editing firewall custom service
   Condition:
   (1) Enable firewll and add custom service, service name=test1, IP protocol=TCP/UDP , port range=2222-2223.
   (2) Edit eWC/firewall/rule summary, packet direction=WAN to WAN/ZyWALL, insert service "test1", Action for matched packet=permit.
   (3) Edit eWC/firewall/service and add another custom service, service name=test2, IP protocol=TCP , port range=100-200.
   (4) Edit eWC/firewall/rule summary, packet direction=LAN to WAN, insert service "test2", Action for matched packet=Drop.
   (5) Edit eWC/firewall/service and modify custom service "test2", change IP protocol to UDP then click apply.
   (6) Device will hang.

Modifications in V 4.00(WM.0) | 09/02/2005
Modify for formal release.

Modifications in V 4.00(WM.0) b5 | 09/02/2005
i. [BUG FIX]
Device crashed because "mbuf double free" when doing FTP Stress test.

Modifications in V 4.00(WM.0) b4 | 08/27/2005
ii. [BUG FIX]
Symptom: Device will crash.
Condition:
(1) Enable Anti Spam.
(2) Enable "Discard SMTP mail. Forward POP3 mail with tag in mail subject".
(3) Send a spam mail.
(4) Device will crash.
iii. [BUG FIX]
Symptom: CPU loading will be very heavy.
Condition:
(1) Set two IKE rules which secure gateways are both domain name.
(2) Go to CI command "sys cpu display", CPU loading is 100%.
iv. [BUG FIX]
Symptom: Sometimes system DNS cannot resolve domain name to IP address.
Condition:
(1) In CLI, enter "ip dns query name myupdate.zywall.zyxel.com"
(2) Try (1) more times and sometimes cannot be resolved.
v. [BUG FIX]

Symptom: The IPSec rule swap without configuring ID Content will fail (XAUTH case).
Condition:
(1) Add one static IPSec rule with XAuth (Rule one).
(2) Add one dynamic IPSec rule with XAuth. Keep the "Peer ID Content" and "Local ID Content" unchanged "0.0.0.0" (Rule two).
(3) Dial the VPN tunnel from peer gateway, the device won't swap to rule two, and the connection can not be built up.

vi. [BUG FIX]
Symptom: VPN can not be established if reponder has multiple rules and the correct rule's phase 2 ID type is subnet.
Condition:
Topology: ZyWALL_A(WAN)----(Internet)----(WAN) ZyWALL_B
(1) IPSec policy in ZyWALL_A:
Policy 1:
Local: 192.168.3.10/255.255.255.0
Remote: 192.168.2.7/255.255.255.0
Policy 2:
Local: 192.168.1.10/255.255.255.0
Remote: 192.168.2.6/255.255.255.0
(2) IPSec policy in ZyWALL_B:
Policy 1:
Local: 192.168.2.0/255.255.255.0
Remote: 192.168.1.0/255.255.255.0
(3) The other phase 1 and phase 2 parameters for ZyWALL_A and ZyWALL_B are the same.
(4) Establish policy 1 tunnel from ZyWALL_B.
(5) ZyWALL_A should establish VPN tunnel by using policy 2, but it fails.

vii. [ENHANCEMENT]
Add CI command "aux usrmdn [1/0]" to switch USR modem flag. If this flag is on, user can dial USR modem successfully.
Note:
(1) For USR modem, user should disable hardware flow control(initial string is "at&f1"); or the modem speed should be 38400 bps
(2) This is a runtime CI command, and this flag is not saved into flash. User can add this command into autoexec.net.

viii. [BUG FIX]
Symptom: IPSec check rule conflict on IP 0.0.0.0 is incorrect.
Condition:
(1) Restore default romfile.
(2) Configure the two IPSec rules shown as follow:
Rule A: local:0.0.0.0 remote:192.168.3.33
Rule B: local:192.168.70.94 remote:192.168.3.33
These two IPSec rules conflict and we should add check for it.

ix. [BUG FIX] 050823946, 050819858, 050820885

Symptom: The UPnP discovery mechanism cannot work normally.
Condition:
(1) Disable the UPnP function.
(2) Reboot device.
(3) Enable the UPnP function.
(4) The XP network place cannot show the UPnP icon.

x. [BUG FIX]
Symptom: Device crashes when doing VPN stress test.
Condition:

(1) Create several VPN tunnls and do stress test.
(2) Device will crash and output the following message on console.
- Prefetch abort exception
Fault Status = 0xXXXXXXXX
Fault Addr = 0xXXXXXXXX

Modifications in V 4.00(WM.0) b3 | 08/16/2005

1. [BUG FIX]
Symptom: Spelling invalid in IDP eWC.
Condition:
(3) In eWC>IDP>Signature, click the "Switch to query view".
(4) The wording of the type selection item "Trojan Hourse" is not right. The word "Hourse" should be "Horse".
2. [BUG FIX]
Symptom: VPN can’t update gateway domain.
Condition: PC A – ZyWALL A -- Internet – ZyWALL B -- PC B
(1) ZyWALL A adds a DDNS rule with Policy ”Use WAN IP address” and enable HA.
(2) ZyWALL B adds a VPN tunnel and Remote Gateway is ZyWALL A’s DDNS.
(3) Set Global Setting>Gateway Domain Name Update Timer to 2 minutes in ZyWALL B.
(4) Build up VPN, and change ZyWALL A link from WAN1 to WAN2.
(5) Make sure that ZyWALL A DDNS been update.
(6) Wait more than 2 min, ZyWALL B’s VPN gateway was not updated.
3. [BUG FIX]
Symptom: Inactivate Wireless without wireless card will cause device hang.
Condition:
(1) Insert wireless card, and enable wireless function.
(2) After taking out B-100 card, upgrade firmware and disable wireless function.
(3) Reboot the device, the device will hang and cannot finish the system booting.
4. [BUG FIX]
Symptom: The wireless clients with 802.1x + dynamic WEP cannot ping each other.
Condition:
(1) Setup 802.1x+dynamic WEP environment.
(2) We find that these wireless clients cannot ping each other after rebooting the device.

5. [ENHANCEMENT]
   Make AntiVirus LOG be consistent with IDP LOG in signature Release Date format.
6. [ENHANCEMENT]
   Change the strategy of the search by name to be case-insensitive in eWC->IDP->Signature->Query page.
7. [FEATURE CHANGE]
   Change the wording "WLAN ZONE" to be "WLAN" in the SMT menu 7.1.
8. [BUG FIX]
   Symptom: Output idle timer should not be disabled.
   Condition: In eWC->VPN->Global Setting page and SMT 24.8, we should not allow users to set output idle timer = 0.
9. [FEATURE CHANGE]
   In SMT 24.1, Wording change: CARD -> WCRD.
10. [BUG FIX]
    Symptom: Execute SMT 24.1->Press Command->"9-Reset Counters", device will crash.
    Condition:
    (1) Insert turbo card.
    (2) Execute SMT 24.1->Press Command->"9-Reset Counters" many times, device will crash.
11. [ENHANCEMENT]
    (1) In eWC>AV/IDP>Update, avoid a blank web page be displayed.
    (2) In eWC>WIRELESS CARD>Wireless Card, remove "Your device must have a wireless card installed…" if the wireless card is installed.
    (3) In eWC>AV>General/IDP>General, remove "Your device must have a turbo card installed…" if the turbo card is installed.
12. [BUG FIX]
    Symptom: System crashes sometimes while signature update or service license refresh.
    Condition:
    (1) Disconnect WAN interface when you update signature. Hence, the update will fail.
    (2) Re-connect the device WAN interface to Internet.
    (3) After the update fail, the device will crash sometimes.
13. [FEATURE CHANGE]
    Change Anti-Spam concurrent session number.
    WAS: 30
    IS: 15
14. [ENHANCEMENT]
    Include "WLAN to WLAN" for FireWall hint message.
    WAS :In eWC>FireWall>Default Rule page, update message is "Warning:When this box is checked, all LAN to LAN, WAN to WAN, DMZ to DMZ and packets will bypass the Firewall check."
    IS: In eWC>FireWall>Default Rule page, change message to "Warning: When this box is checked, all LAN to LAN, WAN to WAN, DMZ to DMZ and WLAN to WLAN packets will bypass the Firewall check."

15. [ENHANCEMENT]
    Message in signature update needs to be update.
    WAS :In eWC>IDP>signature update>waiting page, update message is "This may take up a few seconds. Please wait..."
    IS :In eWC>IDP>signature update>waiting page, change message to "This may take up to minutes. Please wait..."
16. [ENHANCEMENT]
    WAS: In eWC>REGISTRATION>Service page, when service is expired, the Expiration Day field and Registration Type is empty.
    IS : In eWC>REGISTRATION>Service page, when service is expired, the Expiration Day field shows expired date, and Registration Type shows type of expired service.
17. [BUG FIX]
    Symptom: Create two VPN rules which Remote Gateway IP are domain name,the second security gateway can't update automatically.
    Condition: PC1 ---- ZW70_1 (wan)----Internet ---- (wan) ZW70_2 ---- PC2
    (1) ZW70_1 configuration:
        - Set WAN Encapsulation = PPPoE mode.
        - Set DDNS & active it.
        - Create 2 IKE & 2 ipsec, both security gateway are IP address.
    (2) ZW70_2 configuration:
        - Set WAN Encapsulation = Ethernet/ Static IP.
        - Set DNS server= 168.95.1.1.
        - Create 2 IKE & 2 ipsec, both security gateway are domain.
        - eWC/ VPN/ Global Setting, Set " Gateway Domain Name
    (3) Dial up 2 VPN tunnels.
    (4) Drop ZW70_1's PPPoE line then dial up again.
    (5) After 2 minutes into ZW70_2's menu 24.8, issue " ipsec ikeL" to check the security gateway IP --> The Second security gateway not update new IP .
18. [ENHANCEMENT]
    Add a centralized LOG "Error: download signature file failed." for signature update fail due to not receive complete signature file. This situation most happens when the network connection is not stable so that device can not receive complete signature.

19. [BUG FIX]
    Symptom:
    Mail can not be sent or received when device turn on Anti-Spam.
    Condition:
    (1) Device turn on Anti-Spam
    (2) Generate a lot of mail sessions with a lot of mails from LAN side hosts at the same time.
    (3) Mail can not be sent or received in the following conditions:
        i. If queued 20k mail can not be sent successfully after query succeed, then that mail will send fail.
        ii. ACK packets generated by ZyWALL will cause the TCP connection between client and server abnormal.

iii. Retransmitted packets from mail client or server may be dropped by ZyWALL.

20. [ENHANCEMENT]
    Improve Anti-Spam external database query timeout rate by adjusting internal system parameters.
21. [BUG FIX] 050814513
    Symptom: System timer will be exhausted when using TfGen to send heavy traffic to LAN interface.
    Condition:
    (1) Enable AV/IDP feature.
    (2) In LAN side PC, Use TfGen to generate heavy traffic to LAN interface. (Heavy traffic : 40000 kbps/sec up.)
    (3) In SMT 24.8, type "sys updateServer signatureUpdate", the router will crash.
22. [BUG FIX]
    Symptom: Device crashes in Bridge Mode when enable IDP and Content filter
    Condition:
    (1) Insert Turbo card and restart device to Bridge Mode.
    (2) Download signature to device and restart.
    (3) In ”eWC->IDP->General”, enable IDP and activate all interface.
    (4) In CI command, type
    (4.1) idp tune load
    (4.2) idp tune con l7Httpasm on
    (4.3) idp tune save
    (5) In ”eWC->Content Filter->General”, enable content filter.
    (6) In ”eWC->Content Filter->Customization”, enable customization and add a forbidden web site ”www.zyxel.com”.
    (7) Access http://www.zyxel.com from a LAN PC.
    (8) Device crashes.
23. [FEATURE CHANGE]
    Change log behavior when mail session threshold is reached.
    WAS: Only generate log when action is DISCARD.
    IS: Generate log when action is FORWARD and DISCARD.

Modifications in V 4.00(WM.0) b2 | 07/25/2005

1. [FEATURE CHANGE]
   WAS: After deleting the white/black rule via CLI, user needs to type the save command.
   IS: After deleting the white/black rule via CLI, user needn't to type the save command.
2. [BUG FIX] 050614631
   Symptom: IP overlapping check function in eWC->ADVANCED->NAT->Address Mapping sometimes will malfunction
   Condition:
   (1) In eWC->ADVANCED->NAT->Address Mapping->Edit a rule.
   (2) Select Type ”Many-To-Many Overload”, set ”Local Start IP”

as ”0.0.0.0”, ”Local End IP” as ”1.0.0.5” ”Global Start IP” as ”1.0.0.2”, ”Global End IP” as ”6.0.0.8”.

(3) Click ”Apply”, this rule will be saved, it should not.

3. [ENHANCEMENT] AS GUI wordings change
   In eWC>IDP>Signature>Signature Groups Table, refine "select all", "select partial" and "select none" icons in Active / Log / Alert fields.
4. [BUG FIX] 050624163
   Symptom: Host traffic can't pass through VPN tunnel with dial backup
   Condition: PC1-------ZyWALL A------Internet----- ZyWALL B----------PC2 Dial backup
   (1) ZyWALL A add one IKE and one Ipsec rules ,Enable Dial backup
   (2) ZyWALL B add one IKE and one Ipsec rules
   (3) Dial from ZyWALL A, and make sure VPN tunnel build up
   (4) PC1 ping PC2 and PC2 ping PC1 is successful
   (5) Pull out ZyWALL A WAN line ,Dial backup will dial up ,Dial from ZyWALL A, and make sure VPN tunnel is rebuild
   (6) PC1 ping PC2 is successful, but PC2 ping PC1 is fail
5. [BUG FIX] 050628469
   Symptom: In bridge mode of the multiple-WAN devices, the LAN web site hits of eWC->LOGS->Reports on WAN2 have not any data.
   Condition:
   (1) In Bridge mode, the WAN 1 is disconnected and WAN 2 is connected.
   (2) Enable LOGS->Reports "Collect Statistics" and "Send Raw Traffic Statistics to Syslog Server for Analysis".
   (3) A LAN PC uses IE to connect to "www.google.com".
   (4) Set "Statistics Report"->"Report type" is Web Site hits, and we cannot find any data.
6. [BUG FIX] 050701007
   Symptom: After displaying the log by CI, you will see the logs related to Anti-spam are broken.
   Condition:
   (1) Enable Anti-Spam and send a Email(not spam mail) through the ZyWALL.
   (2) Use CI->sys logs display to display the logs.
   (3) You will see the logs related to Anti-spam are broken like "! er1@192.168.70.20 Subject:EmailBomb".
7. [BUG FIX] 050705232
   Symptom: In VPN rule name, when users key-in " ' ", GUI will corrupt.
   Condition:
   (1) In eWC>VPN>VPN Rules(IKE) Summary Table, click "+" to add a gateway policy.
   (2) Fill in "Name" field with " ' ".
   (3) Key in "Pre-Shared Key" with 12345678 and click "Apply".
   (4) The GUI will refresh to VPN Rule(IKE) Summary Table page, but is abnormal.
8. [BUG FIX] 050628421
   Symptom: ZyWALL will crash after testing dial backup a period time.
   Condition:

(1) Set WAN 1 as PPTP and enable Dial backup and Set Allocated Budget=1 minute, period=1 hour.
(2) Ping 168.95.1.1 with DOS command from LAN site host successfully.
(3) Dial backup will hang up after 1 minute.
(4) ZyWALL will crash after pull out WAN and LAN and Dial Backup line for 10 mins.

9. [BUG FIX] 050707366
Symptom: Device cannot get DHCP IP after WAN IP is released.
Condition:
(1) Device WAN port connects to DHCP server (WAN get DHCP IP).
(2) Use SMT 24.4.2, "WAN DHCP Release" but not use "WAN DHCP Renewal".
(3) LAN side PC ping outside, device cannot renew DHCP automatically.

10. [BUG FIX]
Symptom: Content filter cannot add keyword.
Condition:
(1) Go to GUI->Content Filter->Customization page.
(2) Add Trusted website to its maximum number.
(3) Add Forbidden website to its maximum number.
(4) Keyword cannot be added any more.

11. [BUG FIX] 050707368, 050708419
Symptom: In the eWC->Firewall Rule Summary page, insert a new rule and click "Back" button of IE. Then insert rule again, Firewall will have a null record rule.
Condition:
(1) In eWC>Firewall>Rule Summary page, click "Insert" button, then click IE "Back" button.
(2) Click "Insert" button again, and set one rule then "Apply".
(3) Rule Summary page have an additional null record rule.

12. [BUG FIX] 050708444, 050708443
Symptom: When IDP/AV service expired, the expiration day displayed incorrect format in eWC/AV/Update page.
Condition:
(1) DUT IDP/AV service expired.
(2) The expiration day displayed incorrect format in eWC>IDP and AV>Update.

13. [ENHANCEMENT]
Change AV>Update error message.
WAS : In eWC>AV>Update, update message is "The signature search engine is not ready".
IS : In eWC>AV>Update, change message to "Can not find the signature , please update the signature!"

14. [BUG FIX] 050706310
Symptom: Hardware watchdog wake up and sometimes device hand.
Condition:
(1) In SMT24.8, input ”ip ping 168.95.1.1”
(2) Use Ctrl+C to break it.
(3) Repeat steps 1, 2 fast and you can see the watch dog wake up or device hand up.

15. [ENHANCEMENT]

Add firewall predefined services: POP3S/IMAP/IMAPS

16. [BUG FIX] 050627328
    Symptom: ZyWALL will log ”SMTP successfully” when SMTP authentication fail.
    Condition:
    (1) In ”eWC->LOGS->Log Settings”, set ”E-mail Log Settings”.
    (2) Enable ”SMTP Authentication” and set wrong ”Mail Sender”.
    (3) In ”eWC->View Log”, click ”Email Log Now”.
    (4) There will have a log ”SMTP successfully”.
    (5) Actually, the mail was not sent because SMTP server return a error code (454).
17. [BUG FIX] 050725067
    Symptom: Fail in receiving the specific mail when the AV works
    Condition:
    (1) Enable POP3 AV , Enable POP3 Assembly mode
    (2) Run the POP3 Based-64 AV test
    (3) Some mails couldn't be received
18. [FEATURE CHANGE]
    WAS: When Turbo card is not inserted, and accessing IDP at the moment, it shows ”The turbo card is not ready , please insert the card and reboot! ”.
    IS: When Turbo card is not inserted, and accessing IDP at the moment, it shows ”The turbo card is not ready. Please power down the appliance, insert the card and reboot!”.
19. [FEATURE CHANGE]
    WAS: Wording "WLAN" in the network status field in SMT menu 24.1 indicates the wireless card status. Wording "ZONE" indicates the WLANZONE channel status.
    IS: "WLAN" -> "CARD, "ZONE" -> "WLAN". So that Wording "CARD" in the network status field in SMT menu 24.1 indicates the wireless card status. Wording "WLAN" indicates the WLANZONE channel status.
20. [FEATURE CHANGE]
    When the ZyWALL sends registration information to MyZyXEL.com server, the router should send 3 digit country number.
21. [BUG FIX] 050713682
    Symptom: The ZyWALL should filter the country code when it is "0".
    Condition:
    (1) In SMT 24.8, type "sys myZyxelCom register 123456 123456 1234@1.2.3.4 0" (the country code is 0 which is invalid).
    (2) It should not be accepted by the router.
22. [BUG FIX] 050712614
    Symptom: In eWC>WIRELESS CARD>Wireless card page, the max length of "ESSID" field is too short.
    Condition:
    In eWC>WIRELESS CARD>Wireless card page, the max length of "ESSID" field is 30 characters, but user can key in 32 characters via SMT.
23. [BUG FIX] 050715784, 050715785, 050715786
    Symptom: In eWC->UPnP page, after saving the related items by Firefox will cause device crash sometimes.
    Condition:

(1) Open the Firefox browser and goto the eWC->UPnP page.
(2) Disable the UPnP function, and enable some items.
(3) Click the "Apply" button, the device will crash sometimes.

24. [ENHANCEMENT]
Add help pages.
25. [FEATURE CHANGE]
(1) Modify "Update Server" and "myZyXEL.com" logs.
(2) Pop-up new browser in IDP security policy links.
26. [ENHANCEMENT]
Add hyper link to pop up a new window to display certificate error reasons for certificate log message.
27. [ENHANCEMENT]
Unify eWC>Logs datetime format to ISO 8601 (YYYY-MM-DD hh:mm:ss)
28. [ENHANCEMENT]
Update AP F/W version from 1.0.4.3 to 1.2.8.0 for G100/110 AP F/W.
29. [ENHANCEMENT]
Add the Anti-Virus decompress option in eWC>Anti-Virus->General.
30. [BUG FIX] 050715809
Symptom: The ZyWALL will reboot in bridge mode when setting wireless authentication as 802.1x.
31. [ENHANCEMENT]
In eWC>REGISTRATION>Registration page and eWC>HOME>wizard page, add username field format check for the myzyxel.com registration.
32. [ENHANCEMENT]
(1) Add the available free memory to the eWC->Home->memory
(2) GUI Memory bar will become red when the memory usage percentage is larger than 90%
33. [ENHANCEMENT]
(1) Change signature version format from 001.001 to 1.001 in the eWC->IDP/AV->Update page
(2) After signature updated, GUI shows "Get signature success". It should be "Get signature successfully."
(3) Clear signature files by "idp/av clearAllSig".
(4) When the Turbo card is not inserted, in the console: change "Current IDP Signatures: N/A" to "Turbo card is not installed" when Turbo card is not installed.
(5) The severity sorting function should perform according to the severity ,not the string case in the eWC->IDP->Signature/Query page
(6) There should be one space after the SID in the IDP log. Was: IDP:10578,Windows Ping Is: IDP:10578, Windows Ping
(7) In LOG "Update the signature file successfully", it should be modified as "Signature updat OK - New pattern version: V1.001 Release Date: 2005-06-24".
(8) The "idp/av update display" should be consistent to the eWC->IDP->Update page
34. [BUG FIX] 050714719 ,050714720, 050714735
Symptom: If VPN policy enable NAT Traversal, VPN tunnel can’t be built up.

Condition:
PC1(192.168.33.33)------VPN1(192.168.1.33)--(L)DUT(W)(192.168.12.100)----(192.168.12.101)VPN2--(192.168.2.33)PC2
(1) Edit DUT web eWC/NAT/Port Forwarding, index1/Incoming Port(s)=500-500, index1/Server IP Address=192.168.1.33
(2) Edit VPN1 web eWC/VPN:
- IKE: NAT-T=Enable, Name=IKE1, Remote Gateway Address=192.168.12.101, Pre-Shared Key=12345678, Local ID Content=192.168.1.33, Peer ID Content=192.168.12.101
- IPSec: Active=Yes, Name=IPSec1, Gateway Policy=IKE1, Local Network Starting IP Address=192.168.33.33 Remote Network Starting IP Address=192.168.2.33

(3) Edit VPN2 web eWC/VPN:
- IKE: NAT-T=Enable, Name=IKE1, Remote Gateway Address=192.168.12.100, Pre-Shared Key=12345678, Local ID Content=192.168.12.101, Peer ID Content=192.168.1.33
- IPSec: Active=Yes, Name=IPSec1, Gateway Policy=IKE1, Local Network Starting IP Address=192.168.2.33, Remote Network Starting IP Address=192.168.33.33

(4) To dial up VPN policy, and it will fail.

35. [ENHANCEMENT]
(1) In eWC>AV/IDP>General, add some warning messages if turbo card is not inserted but AV/IDP is activated. The behavior is similar with WLAN.
(2) When Turbo card is not inserted, in eWC>IDP/AV>Update>Current IDP Signatures will display "Turbo card is not installed".
(3) eWC> MAINTENANCE> Backup&Restore changes to eWC> MAINTENANCE> Backup & Restore.

36. [ENHANCEMENT]
Add centralized logs for signature updating events and errors.

37. [ENHANCEMENT]
Add a centralized log when WAN ping check fails.

38. [FEATURE CHANGE]
Change signature numbers displayed in "eWC->IDP->Signature" page.

39. [ENHANCEMENT]
Display IDP action in centralized log.

40. [BUG FIX] 050715787, 050715788, 050715789.
Symptom: In eWC "HOME" page , "System Time" display error.
Condition:
1.Go to eWC>HOME Page.
2."System Time" display error, the field length is too short.

41. [BUG FIX] 050719921
Symptom: Mail can't be received via POP3.
Condition: Topology:
PC ----- ZyWALL ----- Mail Server
(1) Enable Anti-Spam.
(2) PC receives mails from Mail Server.

(3) PC sometimes can't receive mail and mail client will timeout.

42. [ENHANCEMENT] 050708486, 050712606, 050719906, 050707395, 050712605
    Add protection to avoid setting unsupported security in "eWC->Wireless Card" when inserted wireless card is B100. Note: B100 does not support WPA, WPA-PSK, 802.1x + Dynamic WEP.
43. [ENHANCEMENT] Wording
    WAS: The ZyWALL will now reboot. As there will be no indication of when the process is complete, please wait for one minute before attempting to access the router again
    IS: The system will now reboot. As there will be no indication of when the process is complete, please wait for one minute before attempting to access the system again.
44. [FEATURE CHANGE] Update registration message
    WAS:
    (1) When user upgrade IDP/AV/AS services, the LOGS shows "service upgrade successfully" but users can not know which service is upgraded"
    (2) When user activate trial service(s), the LOGS shows "trial service activation successfully" but users can not know which service is activated.
    IS:
    (1) When user upgrade services, the LOGS will show "Content Filter service upgrade successfully" or "IDP/Anti-Virus service upgrade successfully" or "Anti-Spam service upgrade successfully" depends on which service license key is used.
    (2) When user activate trial service(s), the LOGS shows which trial service is activated. Ex. "Content Filter, IDP/Anti-Virus trial service(s) activation successfully"

Modifications in V 4.00(WM.0) b1 | 07/01/2005

1. [ENHANCEMENT]
   Change the input format of trap destination in eWC->Remote Management->SNMP from text to IP format.
2. [ENHANCEMENT]
   Support small font size on ZyWALL GUI.
3. [ENHANCEMENT]
   Replace the Cerberian logo by Blue Coat in Content Filter blocked page.
4. [ENHANCEMENT]
   Support Turbo Card (external IDP/AV signature search accelerator)
5. [ENHANCEMENT]
   Add ARP probe for DHCP server.
   1. Change probe type by CI command "sys probeType [icmp | arp]".
   2. Default type is "ICMP".
   3. ARP probe only works when you use arp probe type and dhcp mode should be "Server".
   4. This value will be saved in ROM.
6. [FEATURE CHANGE]
   Add ALG configuration in navigation panel.
7. [ENHANCEMENT]

Re-layout ZyWALL navigation panel on GUI.

8. [ENHANCEMENT]
   Add "Service Status" and "Expiration Date" in Content Filter GUI. The modified GUIs are:
   eWC>CONTENT FILTER>Categories
9. [ENHANCEMENT]
   Add a sender email field in "E-mail Log Settings".
10. [ENHANCEMENT]
    When the daylight saving is activated, there should be a "DST" string trailed behind the time in eWC.
11. [ENHANCEMENT]
    WAS: DNS domain name is not case insensitive.
    IS: DNS domain name is case insensitive.
12. [ENHANCEMENT]
    Firewall ”Available Services” add some common services which are
    1. Microsoft RDP (remote desktop protocol) - tcp:3389
    2. VNC (virtual network computer) - tcp:5900
    3. NTP - tcp/udp:123
13. [ENHANCEMENT]
    Consolidate log “Under SYN flood attack, sent TCP RST”
14. [ENHANCEMENT]
    1. Users cannot enter characters into eWC>VPN>GATEWAY POLICY >EDIT>SA Life Time (Seconds)
    2. User cannot enter characters in eWC>VPN>NETWORK POLICY >EDIT>Protocol
    3. Users cannot enter characters into eWC>VPN>NETWORK POLICY >EDIT>SA Life Time (Seconds)
15. [ENCHANCEMENT]
    Add IDP,Anti-Virus and Anti-Spam features.
16. [ENHANCEMENT]
    Add the SMTP server to the log entry.
17. [ENHANCEMENT]
    Add sequence number and SPI in log for ESP / AH packets.
18. [ENHANCEMENT]
    DHCP log shows the hostname.
19. [ENHANCEMENT]
    Add VPN over Bridge feature.
20. [ENCHANCEMENT]
    Add MyZyxel.Com and Registration features.
21. [ENHANCEMENT]
    Add Firewall Custom Service enhancements.
    Modifications are listed below:
    (1) Allow user to configure ICMP type and code in Firewall ACL.
    (2) Allow user to configure IP protocol in Firewall ACL.
    (3) Add "Any IP Protocol" in default service.(GUI only)
    (4) Replace "PING" with "Any ICMP" in default service. (GUI only)

(5) Allow user to configure Firewall rule name.
(6) Firewall (defeault/rule) action supports "permit", "drop" and "reject".
(7) Centralized LOGS shows descriptions for matched ICMP packet instead of displaying type/code value only.

22. [ENHANCEMENT]
    Enhance Firewall Custom Service
    1. In eWC>Firewall>add new page "Service", it displays the summary of custom services and predefined services.
    2. In eWC>Firewall>Service>Firewall Service Edit page, add two new options: IP protocol and ICMP.
23. [ENHANCEMENT]
    On eWC>FIREWALL>Threshold, add a GUI option to enable/disable DoS Attack protection.
24. [ENHANCEMENT]
    Each static route entry should have its own "Modify" and "Delete" icons.
25. [ENHANCEMENT]
    Add dial backup support for CI command.
    The following is the original SPR description.
    Enhance SMT “sys rn accessblock 0 ” debug message.
    1. CI “sys rn load 3”
    2. CI “sys rn accessblock 0”
    3. CI “sys rn save”
    4. And SMT will occur message “[-6103] Bad entry number”
26. [ENHANCEMENT]
    Enhance Firewall Edit GUI to make it more user-friendly.
    Before: When users click Add/Modify/Delete button to configure an address or select a service from Available Service to Selected Service, the page will be submitted to the ZyWALL immediately to have a rule check and then refresh. It consumed too much time on editing a firewall rule for a user.
    Now: When users click Add/Modify/Delete or select a service, the page will not be submitted to the ZyWALL immediately. The page will be submitted to the ZyWALL to have a rule check after users click "Apply" button. It reduces the refresh time and it is more convenient for the users.
27. [ENCHANCEMENT]
    1. Enhance WLAN to be an independent interface so that traffic passes through WLAN can be handled by firewall.
    2. WLAN can be bound to LAN or DMZ for user’s chosen.
    3. DHCP sever can be applied on LAN, DMZ and WLAN.

28. [FEATURE CHANGE]
    WAS: For firmware downgrade to V3.64 from V4.00 on ZW70w, this enhancement will modify model ID to original one.
    IS: ZyWALL with new model ID will change its ID to old one when user downgrade firmware which only support old model ID.
29. [ENHANCEMENT]

For firmware downgrade to V3.64 from V4.00 on ZW70w, this enhancement will modify model ID to original one.

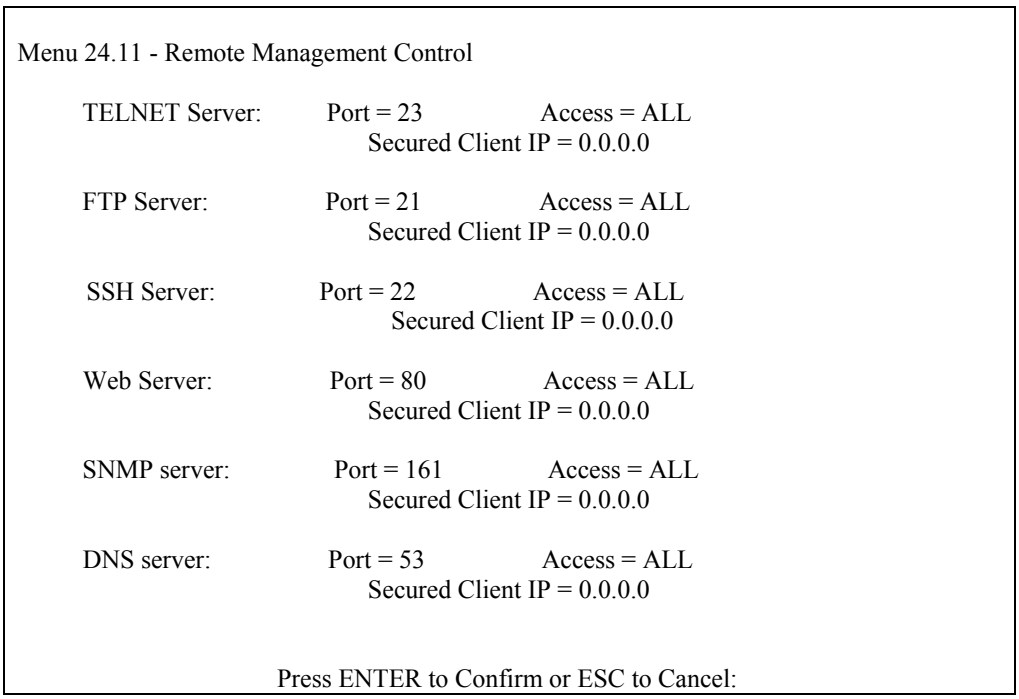
Appendix 1 Remote Management Enhancement (Add SNMP & DNS Control)

New function

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

Modification

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



Appendix 2 Trigger Port

Introduction

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

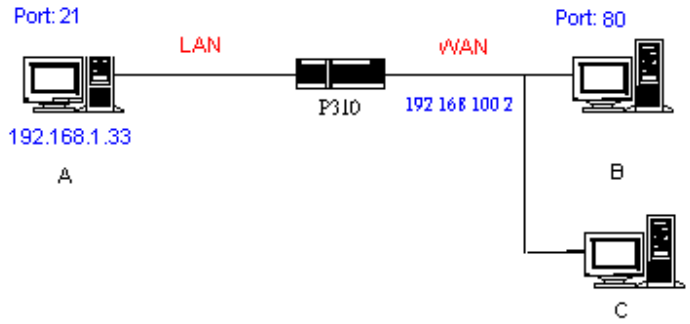
These triggered events can be timed so that they erase the port mapping as soon as they are done with the data transfer, so that the port mapping can be triggered by another Client computer. This gives the ***illusion*** that multiple computers can use the same port mapping at the same time, but the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

How to use it

Following table is a configuration table.

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

How it works



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

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

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

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

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

Notes

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

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

Appendix 3 Hard-coded packet filter for "NetBIOS over TCP/IP" (NBT)

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

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

Example ouput:

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

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

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

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

Appendix 4 Traffic Redirect/Static Route Application Note

Why traffic redirect/static route be blocked by ZyWALL

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

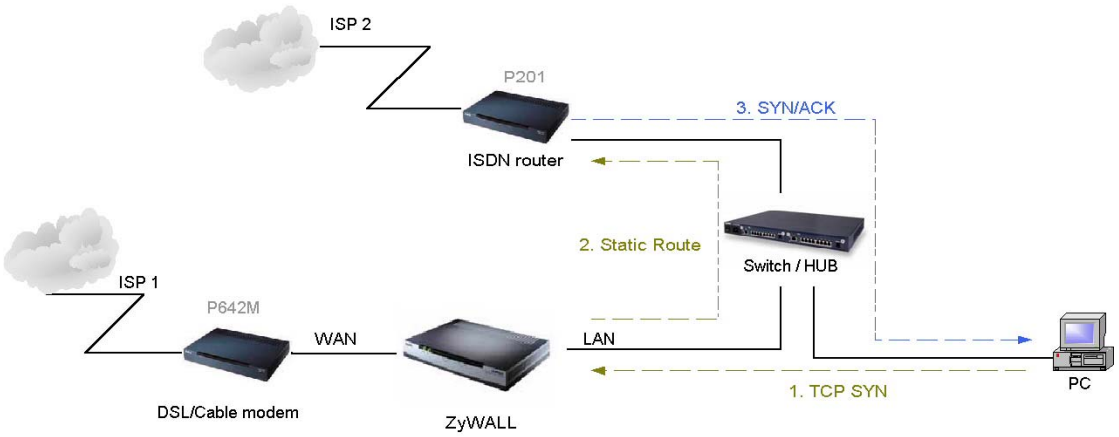


Figure 5-1 Triangle Route

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

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

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

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

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

That causes all of outgoing TCP traffics being reset!

How traffic redirect/static route works under protection - Solutions

(1) Gateway on alias IP network

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

normal function.

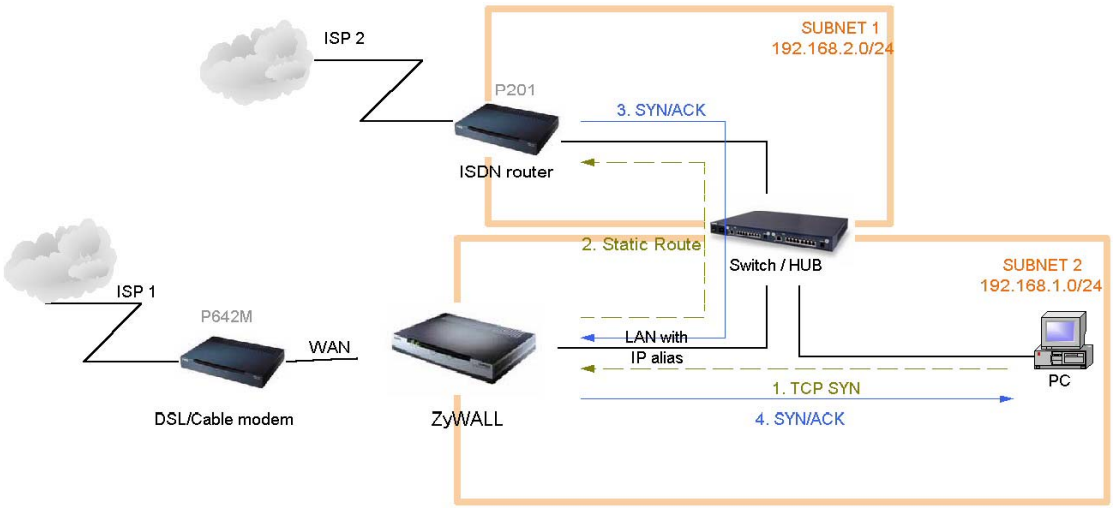


Figure 5-2 Gateway on alias IP network

(2) Gateway on WAN side

A working topology is suggested as below.

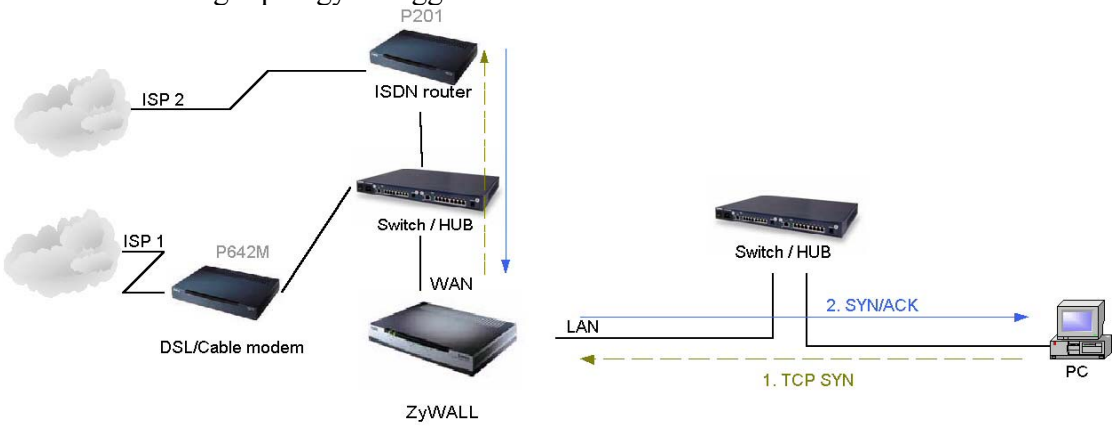


Figure 5-3 Gateway on WAN side

Appendix 5 IPSec FQDN support

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

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

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

contents are consistent and they can connect.

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

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

We can put all combinations in to these two tables:

(Local ID Type is IP):

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

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

(Peer ID Type is IP):

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

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

Summary:

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

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.

Appendix 7 Multiple WAN Access

Because of the expansion of broad band service, the bandwidth is more and more cheap. Some of audio and video applications become usable, such as VoIP and video conference. The company will subscribe several links for different application. They may use it for VoIP, Backup line, Load sharing, and extend bandwidth. Thus they will need a device to manage these kinds of application.

The ZyWALL has two independent WAN ports, so it offers the ability to configure a secondary WAN port for highly reliable network connectivity and robust performance. The user can connect WAN 1 to one ISP(or network), and connect the other to a second

ISP(or network). This secondary WAN port can be used in “active-active” load sharing or fail-over configuration providing a highly efficient method for maximizing total network bandwidth.

The default mode of the WAN 2 interface is “Active-Passive” or “Fail-Over” mode, that is the secondary WAN will automatically “bring-up” when the first WAN fails. The user can enter eWC/WAN/General page to select WAN to “Active/Active” mode. At “Active/Active” mode, ZyWALL can access internet through WAN 1 and WAN 2 simultaneously. The user also can setup policy route rule and static route rule to specify the traffic to certain link. ZyWALL Connectivity Check will check the connectivity of WAN 1, WAN 2 and Traffic Redirect. Please notice that even at the “Active/Active” mode, WAN 2 is still the backup line of WAN 1, and WAN 1 is also the backup line of WAN 2.

The user can use policy routing to specify the WAN port that specific services go through. If one WAN port’s connection goes down, the ZyWALL can automatically send its traffic through the other WAN port, if the user allows this traffic to use the other WAN port.

The ZyWALL NAT feature allows the user to give two separate sets of rules(NAT Mapping rules and Port Forwarding rules) for WAN 1 and WAN 2.

The DDNS also has the high availability feature based on Multiple WAN. That is the ZyWALL can use the other WAN interface for domain names if the original configured WAN interface goes down.

Appendix 8 Wi-Fi Protected Access

Wi-Fi Protected Access(WPA) is a subset of the IEEE 802.11i. WPA improves data encryption by using TKIP, MIC and IEEE 802.1X. Because WPA applies 802.1X to authenticate WLAN users by using an external RADIUS server, so you can not use the Local User Database for WPA authentication.

For those users in home or small office, they have no RADIUS server, WPA provides the benefit of WPA through the simple “WPA-PSK”. Pre-Shared Key(PSK) is manually entered in the client and ZyWALL for authentication. ZyWALL will check the client PSK and allow it join the network if it’s PSK is matched. After the client pass the authentication, ZyWALL will derived and distribute key to the client, and both of then will use TKIP process to encrypt exchanging data.

Appendix 9 IPSec IP Overlap Support

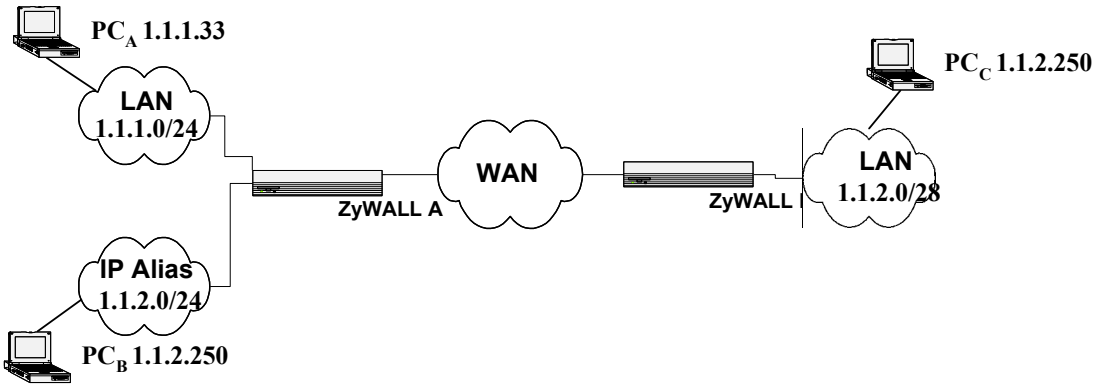


Figure 1

The ZyWALL uses the network policy to decide if the traffic matches a VPN rule. But if the ZyWALL finds that the traffic whose local address overlaps with the remote address range, it will be confused if it needs to trigger the VPN tunnel or just route this packet.

So we provide a CI command "ipsec swSkipOverlapIp" to trigger the VPN rule. For example, you configure a VPN rule on the ZyWALL A as below:

Local IP Address Start= 1.1.1.1 End= 1.1.2.254
Remote IP Address Start= 1.1.2.240 End = 1.1.2.254

You can see that the Local IP Address and the remote IP address overlap in the range from 1.1.2.240 to 1.1.2.254.

(1) Enter "ipsec swSkipOverlapIp off":
To trigger the tunnel for packets from 1.1.1.33 to 1.1.2.250. If there is traffic from LAN to IP Alias (Like the traffic from PC_A to PC_B in Figure 1), the traffic still will be encrypted as VPN traffic and routed to WAN, you will find their traffic disappears on LAN.
(2) Enter "ipsec swSkipOverlapIp on":
Not to trigger the tunnel for packets from 1.1.1.33 to 1.1.2.250. Even the tunnel has been built up, the traffic in this overlapped range still cannot be passed.

[Note]
If you configure a rule on the ZyWALL A whose
Local IP Address Start= 0.0.0.0
Remote IP Address Start= 1.1.2.240 End = 1.1.2.254
No matter swSkipOverlapIp is on or off, any traffic from any interfaces on the ZyWALL A will match the tunnel. Thus swSkipOverlapIp is not applicable in this case.

Appendix 10 VPN Local IP Address Limitation

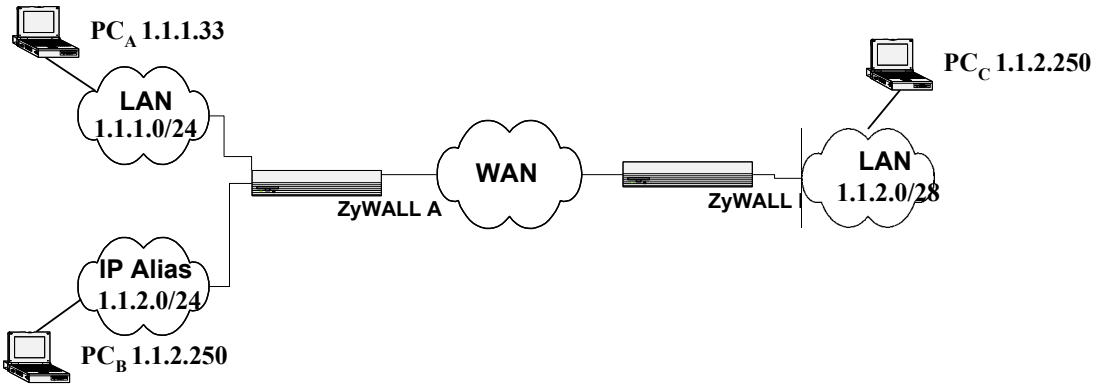


Figure 1

There is a limitation when you configure the VPN network policy to use any Local IP address. When you set the Local address to 0.0.0.0 and the Remote address to include any interface IP of the ZyWALL at the same time, it may cause the traffic related to remote management or DHCP between PCs and the ZyWALL to work incorrectly. This is because the traffic will all be encrypted and sent to WAN.

For example, you configure a VPN rule on the ZyWALL A as below:

Local IP Address Start= 1.1.1.1 End= 1.1.2.254
Remote IP Address Start= 1.1.2.240 End = 1.1.2.254

ZyWALL LAN IP = 1.1.1.10

ZyWALL LAN IP falls into the Local Address of this rule, when you want to manage the ZyWALL A from PC_A, you will find that you cannot get a DHCP Client IP from the ZyWALL anymore. Even if you set your IP on PC_A as static one, you cannot access the ZyWALL.

Appendix 11 VPN rule swap limitation with VPN Client on XAuth

Example 1:

ZyWALL (WAN)---------- VPN Client
(IP:1.1.1.1) (IP:1.1.1.2)

ZyWALL VPN Rule: Two IKE rule	
➢ Dynamic IKE rule: Security Gateway: 0.0.0.0 X-Auth: Server I. Policy one: - Name: “Rule_A” - Local: 192.168.2.0/24 - Remote: 0.0.0.0	➢ Static IKE rule: Security Gateway: 1.1.1.2 X-Auth: None I. Policy one: - Name: “Rule_B” - Local: 192.168.1.0/24 - Remote: 1.1.1.2/32

ZyXEL VPN Client
Security Gateway: 1.1.1.1 Phase one Authentication method: Preshare Key Remote: 192.168.1.0/24

In example 1, user may wonder why ZyWALL swap to dynamic rule even VPN client only set authentication method as “Preshare Key” not “Preshare Key+XAuth”. The root cause is that currently ZyXEL VPN Cient will send XAuth VID no matter what authentication mode that him set. Because of the XAuth VID, ZyWALL will swap to dynamic rule.

This unexpected rule swap result is a limitation of our design. For ZyWALL, when we got initiator’s XAuth VID in IKE Phase One period, we know initiator can support XAuth. To take account of security, we will judge that initiator want to do XAuth, and we will search one matched IKE Phase One rule with XAuth server mode as the top priority. To our rule swap scheme, we search static rule first then dynamic rule. In example 1, we will find the static rule, named “Rule_B”, to build phase one tunnel at first. After finished IKE phase one negotiation, we known initiator want to do XAuth. Since Rule_B has no XAuth server mode, we try to search another rule with correct IKE Phase One parameter and XAuth server mode. The search result will lead us to swap rule to dynamic rule, named “Rule_A”. Thus to build VPN tunnel will fail by Phase Two local ip mismatch.

To avoid this scenario, the short-term solution is that we recommend user to set two IKE rule with different Phase One parameter. The long-term solution is that VPN Client needs to modify the XAuth VID behavior. VPN Client should not send XAuth VID when authentication method is “Preshare key”, but send XAuth VID when authentication method is “Preshare key+XAuth”.

Annex A CI Command List

Last Updated: 2005/08/01

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	PPP Related Command	Bandwidth Management
Firewall Related Command	Certificate Management (PKI) Command	Load Sharing Command
Bridge Related Command	myZyXEL.com Command	Anti-Spam Command
IDP Command	Anti-Virus Command	

System Related Command Home

Command				Description
sys				
	atsh			Display system information
	cbuf			
		display	[a|f|u]	display cbuf a: all f: free u: used
		cnt		cbuf static
			Display	display cbuf static
			Clear	clear cbuf static
	baud		<1..5>	change console speed
	callhist			
		display		display call history
		remove	<index>	remove entry from call history
	clear			clear the counters in GUI status menu
	countrycode		[countrycode]	set country code
	datetime		[year month date]	set/display date
	domainname			display domain name
	edit		<filename>	edit a text file
	enhanced			return OK if commands are supported for PWC purposes
	errctl		[level]	set the error control level 0:crash no save,not in debug mode (default) 1:crash no save,in debug mode 2:crash save,not in debug mode 3:crash save,in debug mode
	event			
		display		display tag flags information
		trace		display system event information
			display	display trace event
			clear <num>	clear trace event
	extraphnum			maintain extra phone numbers for outcalls
		add	<set 1-3> <1st phone num> [2nd phone num]	add extra phone numbers
		display		display extra phone numbers
		node	<num>	set all extend phone number to remote node <num>
		remove	<set 1-3>	remove extra phone numbers
		reset		reset flag and mask
	feature			display feature bit

	fid			
		display		display function id list
	firmware			display ISDN firmware type
	hostname		[hostname]	display system hostname
	iface			
		disp	[#]	display iface list
	interrupt			display interrupt status
	logs			
		category		
			access [0:none/1:log/2:alert/3:both]	record the access control logs
			attack [0:none/1:log/2:alert/3:both]	record and alert the firewall attack logs
			display	display the category setting
			error [0:none/1:log/2:alert/3:both]	record and alert the system error logs
			ipsec [0:none/1:log/2:alert/3:both]	record the access control logs
			ike [0:none/1:log/2:alert/3:both]	record the access control logs
			javablocked [0:none/1:log]	record the java etc. blocked logs
			mten [0:none/1:log]	record the system maintenance logs
			packetfilter [0:none/1:log]	record the packet filter logs
			pki [0:none/1:log/2:alert/3:both]	record the pki logs
			tcpreset [0:none/1:log]	record the tcp reset logs
			upnp [0:none/1:log]	record upnp logs
			urlblocked [0:none/1:log/2:alert/3:both]	record and alert the web blocked logs
			urlforward [0:none/1:log]	record web forward logs
		clear		clear log
		display	[access|attack|error|ipsec|ike|javablocked|mten|packetfilter|pki|tcpreset|urlblocked|urlforward]	display all logs or specify category logs
		dispSvrIP		Display the IP address of email log server and syslog server
		errlog		
			clear	display log error
			disp	clear log error
			online	turn on/off error log online display
		load		load the log setting buffer
		mail		
			alertAddr [mail address]	send alerts to this mail address
			display	display mail setting
			logAddr [mail address]	send logs to this mail address
			schedule display	display mail schedule
			schedule hour [0-23]	hour time to send the logs
			schedule minute [0-59]	minute time to send the logs
			schedule policy [0:full/1:hourly/2:daily/3:weekly/4:none]	mail schedule policy
			schedule week [0:sun/1:mon/2:tue/3:wed/4:thu/5:fri/6:sat]	weekly time to send the logs
			server [domainName/IP]	mail server to send the logs
			subject [mail subject]	mail subject
		save		save the log setting buffer
		syslog		
			active [0:no/1:yes]	active to enable unix syslog
			display	display syslog setting

			facility [Local ID(1-7)]	log the messages to different files
			server [domainName/IP]	syslog server to send the logs
		updateSvrIP	<minute>	If there is one parameter <minute>, it will change the dns timer task timeout value. Otherwise, do dns resolve to find email log server and syslog server IP.
		consolidate		
			switch <0:on|1:off>	active to enable log consolidation
			period	consolidation period (seconds)
			msglist	display the consolidated messages
		switch		
			bmlog <0:no|1:yes>	active to enable broadcast/multicast log
			display	display switch setting
			trilog <0:no|1:yes>	active to enable triangle route log
	mbuf			
		link	link	list system mbuf link
		pool	<id> [type][num]	list system mbuf pool
		status		display system mbuf status
		disp	<address>[1|0]	display mbuf status
		cnt		
			disp	display system mbuf count
			clear	clear system mbuf count
		debug	[on|off]	
	memwrite		<address> <len> [data list ...]	write some data to memory at <address>
	memutil			
		usage		display memory allocate and heap status
		mqueue	<address> <len>	display memory queues
		mcell	mid [f|u]	display memory cells by given ID
		msecs	[a|f|u]	display memory sections
		mtstart	<n-mcell>	start memory test
		mtstop		stop memory test
		mtalloc	<size> [n-mcell]	allocate memory for testing
		mtfree	<start-idx> [end-idx]	free the test memory
	mode	<router/bridge>		switch router and bridge mode
	model			display server model name
	proc			
		display		Display all process information. State: process state. Pri: priority, a_usg: accumulated cpu usage, p_usg: profiling cpi usage.(take count after do clear command). Size: (lowest available stack size)/(total stack size).
		stack	[tag]	display process's stack by a give TAG
		pstatus		display process's status by a give TAG
		clear		Restart cpu usage measurement. (Result will be in p_usg column from display command.
	pwc			sends information to PWC via telnet
	pwderrtm		[minute]	Set or display the password error blocking timeout value.
	queue			
		display	[a|f|u] [start#] [end#]	display queue by given status and range numbers
		ndisp	[qid]	display a queue by a given number
	quit			quit CI command mode
	reboot		[code]	reboot system

				code = 0 cold boot, = 1 immediately boot = 2 bootModule debug mode
	reslog			
		disp		display resources trace
		clear		clear resources trace
	rn			
		load	<entry no.>	load remote node information
		disp	<entry no.>(0:working buffer)	display remote node information
		nat	<none|sua|full_feature>	config remote node nat
		nailup	<no|yes>	config remote node nailup
		mtu	<value>	set remote node mtu
		save	[entry no.]	save remote node information
	smt			not support in this product
	stdio		[second]	change terminal timeout value
	time		[hour [min [sec]]]	display/set system time
	timer			
		disp		display timer cell
	tos			
		display		display all runtime TOS
		listPerHost		display all host session count
		debug	[on|off]	turn on or off TOS debug message
		sessPerHost	<number>	configure session per host value
		timeout		
			display	display all TOS timeout information
			icmp <idle timeout>	set idle timeout value
			igmp <idle timeout>	set idle timeout value
			tcpsyn <idle timeout>	set idle timeout value
			tcp <idle timeout>	set idle timeout value
			tcpfin <idle timeout>	set idle timeout value
			udp <idle timeout>	set idle timeout value
			gre <idle timeout>	set idle timeout value
			esp <idle timeout>	set idle timeout value
			ah <idle timeout>	set idle timeout value
			other <idle timeout>	set idle timeout value
	trcdisp	parse, brief, disp		monitor packets
	trclog			
		switch	[on|off]	set system trace log
		online	[on|off]	set on/off trace log online
		level	[level]	set trace level of trace log #:1-10
		type	<bitmap>	set trace type of trace log
		disp		display trace log
		clear		clear trace
		call		display call event
		encapmask	[mask]	set/display tracelog encapsulation mask
	trcpacket			
		create	<entry> <size>	create packet trace buffer
		destroy		packet trace related commands
		channel	<name> [none|incoming|outgoing|bothway]	<channel name>=enet0,sdsl00, fr0 set packet trace direction for a given channel
		string		enable smt trace log
		switch	[on|off]	turn on/off the packet trace
		disp		display packet trace
		udp		send packet trace to other system

			switch [on|off]	set tracepacket upd switch
			addr <addr>	send trace packet to remote udp address
			port <port>	set tracepacket udp port
		parse	[[start_idx], end_idx]	parse packet content
		brief		display packet content briefly
	syslog			
		server	[destIP]	set syslog server IP address
		facility	<FacilityNo>	set syslog facility
		type	[type]	set/display syslog type flag
		mode	[on|off]	set syslog mode
	version			display RAS code and driver version
	view		<filename>	view a text file
	wdog			
		switch	[on|off]	set on/off wdog
		cnt	[value]	display watchdog counts value: 0-34463
	romreset			restore default romfile
	mrd			
		atwe	<mac> [country code] [debug flag] [featurebit]	configure mac, country code, debug flag, featurebit in the boot module
		atse		generate the engeneering debug flag password seed
		aten	<password>	enter the engeneering debug flag password
		atfl	<0:1>	set engeneering debug flag
		atsh		show mrd setting
	server			
		access	<telnet|ftp|web|icmp|snmp|dns> <value>	set server access type
		load		load server information
		disp		display server information
		port	<telnet|ftp|web|snmp> <port>	set server port
		save		save server information
		secureip	<telnet|ftp|web|icmp|snmp|dns> <ip>	set server secure ip addr
		certificate	<https|ssh> [certificate name]	set server certificate
		auth_client	<https> [on|off]	specifies whether the server authenticates the client
	fwnotify			
		load		load fwnotify entry from spt
		save		save fwnotify entry to spt
		url	<url>	set fwnotify url
		days	<days>	set fwnotify days
		active	<flag>	turn on/off fwnotify flag
		disp		display firmware notify information
		check		check firmware notify event
		debug	<flag>	turn on/off firmware notify debug flag
	spt			
		dump		dump spt raw data
			root	dump spt root data
			rn	dump spt remote node data
			user	dump spt user data
			slot	dump spt slot data
		set	<offset> <len> <value...>	set spt value in memory address
		save		save spt data
		size		display spt record size
		clear		clear spt data

	cmgr			
		trace		
			disp <ch-name>	show the connection trace of this channel
			clear <ch-name>	clear the connection trace of this channel
		data	<ch-name>	show channel connection related data
		cnt	<ch-name>	show channel connection related counter
	socket			display system socket information
	filter			
		clear		clear filter statistic counter
		disp		display filter statistic counters
		sw	[on|off]	set filter status switch
		rule	<iface>	display iface filter flag
		set	<set>	display filter rule
		addNetBios		add netbios filter
		removeNetBios		remove netbios filter
		netbios		
			disp	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>	config netbios filter
		blockbc	[on|off]	set/display broadcast filter mode
	roadrunner			
		debug	<level>	enable/disable roadrunner service 0: diable <default> 1: enable
		display	<iface name>	display roadrunner information iface-name: enif0, wanif0
		restart	<iface name>	restart roadrunner
		logout	<iface name>	logout roadrunner
		set	<iface name>	set roadrunner
	ddns			
		debug	<level>	enable/disable ddns service
		display	<iface name>	display ddns information
		restart	<iface name>	restart ddns
		logout	<iface name>	logout ddns
	cpu			
		display		display CPU utilization
	upnp			
		active	[0:no/1:yes]	Activate or deactivate the saved upnp settings
		config	[0:deny/1:permit]	Allow users to make configuration changes. through UPnP
		display		display upnp information
		firewall	[0:deny/1:pass]	Allow UPnP to pass through Firewall.
		load		save upnp information
		reserve	[0:no/1:yes]	Reserve UPnP NAT rules in flash after system bootup.
		save		save upnp information
	mwan			
		load		Load the multiple wan common data to the memory
		mode	<0:Active/Passive|1:Active/Active>	Change the Multiple WAN operation mode.
		Save		Save the configuration
		Disp		Display the data

	atmu			Show multiboot client version
	ProbeType		[icmp | arp]	DHCP server probing type

Exit Command Home

Command				Description
exit				exit smt menu

Device Related Command Home

Command				Description
dev				
	channel			
		name	<all|use>	list channel name
		drop	<channel_name>	drop channel
		disp	<channel_name> [level]	display channel
		threshold	<channel_name> [number]	set channel threshold
	dial		<node#>	dial to remote node

Ethernet Related Command Home

Command				Description
ether				
	config			display LAN configuration information
	driver			
		cnt		
			disp <name>	display ether driver counters
			clear <name>	clear ether driver counters
		iface	<ch_name> <num>	send driver iface
		ioctl	<ch_name>	Useless in this stage.
		mac	<ch_name> <mac_addr>	Set LAN Mac address
		reg	<ch_name>	display LAN hardware related registers
		rxmod	<ch_name> <mode>	set LAN receive mode. mode: 1: turn off receiving 2: receive only packets of this interface 3: mode 2+ broadcast 5: mode 2 + multicast 6: all packets
		status	<ch_name>	see LAN status
		init	<ch_name>	initialize LAN
	version			see ethernet device type
	pkttest			
		disp		
			packet <level>	set ether test packet display level
			event <ch> [on|off]	turn on/off ether test event display
		sap	[ch_name]	send sap packet
		arp	<ch_name> <ip-addr>	send arp packet to ip-addr
	test		<ch_id> <test_id> [arg3] [arg4]	do LAN test
	ipmul		<num>	only receive ip multicast and broadcast packet
	pncconfig		<ch_name>	do pnc config
	mac		<src_ch> <dest_ch> <ipaddr>	fake mac address
	edit			
		load	<ether no.>	load ether data from spt
		mtu	<value>	set ether data mtu
		speed	<speed>	set ether data speed

		save		save ether data to spt
	dynamicPort			
		dump		display the relation between physical port and channel.
		set	<port> <type>	set physical port belongs to which channel.
		spt		display channel setting stored in SPT.

POE Related Command Home

Command				Description
poe				
	debug		[on|off]	switch poe debug
	retry			
		count	[count]	set/display poe retry count
		interval	[interval]	set/display poe retry interval
	status		[ch_name]	see poe status
	master			
		promiscuous	[on|off]	provide pppoe server list to client
		easy	[on|off]	response for no service name request
	service			
		add	<service-name>	add poe service
		show		show poe service
	dial		<node>	dial a remote node
	drop		<node>	drop a pppoe call
	channel			
		enable	<channel>	enable a channel to carry pppoe traffic
		disable	<channel>	disable a pppoe channel
		show		show pppoe channel
	padt		[limit]	set/display pppoe PADT limit
	inout		<node_name>	set call direction to both
	ippool		[ip] [cnt]	set/display pppoe ippool information
	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 Home

Command				Description
pptp				
	debug		[on|off]	switch pptp debug flag
	dial		<rn-name>	dial a remote node
	drop		<rn-name>	drop a remote node call
	tunnel		<tunnel id>	display pptp tunnel information
	enque		[size]	set pptp max en-queued size

AUX Related Command Home

Command				Description
aux				
	atring		<device name>	Command the AT command to the device.
	clearstat		<device name>	reset channel statistics
	cnt			

		disp	<device name>	display aux counter information
		clear	<device name>	clear aux counter information
	cond			
		disp	<device name>	display aux condition information
		clear	<device name>	clear aux condition information
	config			display aux config, board, line, channel information
	data			
	drop		<device name>	disconnect
	event			
		disp		aux event trace display
		clear		aux event trace clear
	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
	ringbuf			
		cmd		
			clear <device name>	clear ringbuffer
			disp <device name>	display ringbuffer
		data		
			clear	clear command ringbuffer
			disp <start> <len>	display command ringbuffer
	signal		<device name>	show aux signal
	speed		<device name> <type> [value]	display/set aux speed

Configuration Related Command Home

Command					Description
config					The parameters of config are listed below.
edit	firewall	active <yes|no>			Activate or deactivate the saved firewall settings
	custom-service <entry#>	name <string>			Configure selected custom-service with name = <string>
		ip-protocol < icmp | tcp | udp | tcp/udp | user-defined>			Configure IP Protocol Type for selected custom-service
		port-range <start port> <end port>			When ip-protocol = “tcp | udp | tcp/udp “. configure port range for custom-service entry #. For single port configuration, start port equals to end port.
		user-defined-ip <1~65535>			When ip-protocol = “user-defined”. Configure user defined IP protocol.
		icmp-type <0~255>			When ip-protocol = “icmp”, configure ICMP type.
		icmp-code <0~255>			When ip-protocol = “icmp”, configure ICMP code. This field is optional for ICMP.
retrieve	firewall				Retrieve current saved firewall settings
save	firewall				Save the current firewall settings
	custom-service <entry#>				Save the custom service entry specified by <entry#>

	anti-spam				Save current AntiSpam settings
	all				Save all working SPT buffer into flash.
displa y	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
	custom-serv ice				Display all configured custom services.
	custom-serv ice <entry #>				Display custom service <entry #>
	anti-spam				Display AntiSpam settings
edit		e-mail	mail-server <mail server IP>		Edit the mail server IP to send the alert
			return-addr <e-mail address>		Edit the mail address for returning an email alert
			e-mail-to <e-mail address>		Edit the mail address to send the alert
			policy <full | hourly |daily | weekly>		Edit email schedule when log is full or per hour, day, week.
			day <sunday | monday | tuesday | wednesday | thursday | friday | saturday>		Edit the day to send the log when the email policy is set to Weekly
			hour <0~23>		Edit the hour to send the log when the email policy is set to daily or weekly
			minute <0~59>		Edit the minute to send to log when the email policy is set to daily or weekly
			Subject <mail subject>		Edit the email subject
		attack	send-alert <yes|no>		Activate or deactivate the firewall DoS attacks notification emails
			block <yes|no>		Yes: Block the traffic when exceeds the tcp-max-incomplete threshold
					No: Delete the oldest half-open session when exceeds the tcp-max-incomplete threshold
			block-minute <0~255>		Only valid when sets 'Block' to yes. The unit is minute
			minute-high <0~255>		The threshold to start to delete the old half-opened sessions to minute-low
			minute-low <0~255>		The threshold to stop deleting the old half-opened session
			max-incomplete-high <0~255>		The threshold to start to delete the old half-opened sessions to max-incomplete-low
			max-incomplete-low <0~255>		The threshold to stop deleting the half-opened session
			tcp-max-incomplete <0~255>		The threshold to start executing the block field
		set <set#>	name <desired name>		Edit the name for a set
			default-permit <forward|block>		Edit whether a packet is dropped or allowed when it does not match the default set

			icmp-timeout <seconds>		Edit the timeout for an idle ICMP session before it is terminated
			udp-idle-timeout <seconds>		Edit the timeout for an idle UDP session before it is terminated
			connection-timeout <seconds>		Edit the wait time for the SYN TCP sessions before it is terminated
			fin-wait-timeout <seconds>		Edit the wait time for FIN in concluding a TCP session before it is terminated
			tcp-idle-timeout <seconds>		Edit the timeout for an idle TCP session before it is terminated
			pnc <yes|no>		PNC is allowed when 'yes' is set even there is a rule to block PNC
			log <yes|no>		Switch on/off sending the log for matching the default permit
			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-rang	Select and edit a destination address range of a

				e <start ip address> <end ip address>	packet which complies to this rule.
				tcp destport-single <port#>	Select and edit the destination port of a packet which comply to this rule. For non-consecutive port numbers, the user may repeat this command line to enter the multiple port numbers.
				tcp destport-range <start port#> <end port#>	Select and edit a destination port range of a packet which comply to this rule.
				udp destport-single <port#>	Select and edit the destination port of a packet which comply to this rule. For non-consecutive port numbers, users may repeat this command line to enter the multiple port numbers.
				udp destport-range <start port#> <end port#>	Select and edit a destination port range of a packet which comply to this rule.
				desport-custom <desired custom port name>	Type in the desired custom port name
				custom-ip <desired custom service name>	Type in the desired User Defined IP Protocol custom service.
				custom-icmp <desired custom service name>	Type in the desired ICMP custom service
	anti-spam				
		action	<0|1>		Set the action for Spam Mail: add tag(0) or discard mail(1).
		markString	<spam tag>		Set the Spam tag string. This tag will add to the subject of spam mail.
		externDB	<0|1>		Enable(1)/Disable(0) External Database Query.
		query	<0|1>		Set the action for no spam score: add tag(0) ot discard mail(1).
		queryString	<no spam score tag>		Set the tag string for no spam score. This tag will add to the subject of spam mail.
		threshold	<threshold>		Set the spam score threshold. If the spam score is higher than this threshold, this mail will be judge as spam mail.
		switch	<0|1>		Enable(1)/Disable(0) AntiSpam function.
		whiteRule	<0|1>		Enable(1)/Disable(0) AntiSpam White Rule Filter.
		blackRule	<0|1>		Enable(1)/Disable(0) AntiSpam Black Rule Filter.
		phishingString	<Phishing tag>		Set the phishing tag string. This tag will add to

					the subject of spam mail.
		rule	<rule number>	ip <index> active <0|1> address <ip address> netmask <netmask>	Set the While(1)/Black(2) Rule IP Filter. The <index> is start from 0.
				email <index> active <0|1> data <email address>	Set the While(1)/Black(2) Rule Email Filter. The <index> is start from 0.
				mime <index> active <0|1> header <MIME Header> value <MIME Value>	Set the While(1)/Black(2) Rule MIME Filter. The <index> is start from 0.
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
	anti-spam	blackRule			Remove the AntiSpam Black Rule.
		whiteRule			Remove the AntiSpam White Rule.
insert	firewall	e-mail			Insert email alert settings
		attack			Insert attack alert settings
		set <set#>			Insert a specified rule set to the firewall configuration
		set <set#>	rule <rule#>		Insert a specified rule in a set to the firewall configuration
cli					Display the choices of command list.
debug	<1|0>				Turn on|off trace for firewall debug information.

IP Related Command Home

Command				Description
ip				
	address		[addr]	display host ip address
	alias		<iface>	alias iface
	aliasdis		<0|1>	disable alias
	alg			
		disp		Show ALG enable disable status
		enable	<ALG_FTP|ALG_H323|ALG_SIP>	Enable ALG command
		disable	<ALG_FTP|ALG_H323|ALG_SIP>	Disable ALG command
		siptimeout	<timeout in second> or 0 for no timeout	Configure SIP timeout command
	arp			
		status	<iface>	display ip arp status
		add	<hostid> ether <ether addr>	add arp information
		resolve	<hostid>	resolve ip-addr

		replydif	[<0:No|1:yes>]	reply different inteface ip-addr's arp request
		drop	<hostid> [hardware]	drop arp
		flush		flush arp table
		publish		add proxy arp
		period	< value: 30~3000>	Set arp period.
		attpret	<on|off>	Switch receive APR from the different network or not.
		force	<on|off>	Switch the time out function of the APR.
	dhcp		<iface>	
		client		
			release	release DHCP client IP
			renew	renew DHCP client IP
		mode	<server|relay|none|client>	set dhcp mode
		relay	server <serverIP>	set dicp relay server ip-addr
		reset		reset dhcp table
		server		
			probecount <num>	set dhcp probe count
			dnsserver <IP1> [IP2] [IP3]	set dns server ip-addr
			winsserver <winsIP1> [<winsIP2>]	set wins server ip-addr
			gateway <gatewayIP>	set gateway
			hostname <hostname>	set hostname
			initialize	fills in DHCP parameters and initializes (for PWC purposes)
			leasetime <period>	set dhcp leasetime
			netmask <netmask>	set dhcp netmask
			pool <startIP> <numIP>	set dhcp ip pool
			renewaltime <period>	set dhcp renew time
			rebindtime <period>	set dhcp rebind time
			reset	reset dhcp table
			server <serverIP>	set dhcp server ip for relay
			dnsorder [router|isp]	set dhcp dns order
			release <entry num>	release specific entry of the dhcp server pool
		status	[option]	show dhcp status
		static		
			Delete <num>|all	delete static dhcp mac table
			display	display static dhcp mac table
			update <num> <mac> <ip>	update static dhcp mac table
	dns			
		query		
			address <ipaddr> [timeout]	resolve ip-addr to name
			Debug <num>	enable dns debug value
			Name <hostname> [timeout]	resolve name to multiple IP addresses
			Status	display dns query status
			Table	display dns query table
		server	<primary> [secondary] [third]	set dns server
		stats		
			Clear	clear dns statistics
			Disp	display dns statistics
		table		display dns table
		default	<ip>	Set default DNS server
		system		
			display	display dns system information
			edita <record idx> <name> <0:FQDN|1:wildcard> <0:from ISP	edit dns A record

			group|1:user defined> <isp group idx|ip address>	
			editns <record idx> <*|domain name> <0:from ISP|1:user defined(public)|2: user defined(private)> <isp group idx|dns server ip>	edit dns NS record
			inserta <before record idx|-1:new> <name> <0:FQDN|1:wildcard> <0:from ISP group|1:user defined> <isp group idx|ip address>	insert dns A record
			insertns <before record idx|-1:new> <*|domain name> <0:from ISP|1:user defined(public)|2: user defined(private)> <isp group idx|dns server ip>	insert dns NS record
			movea <record idx> <record idx>	move dns A record
			movens <record idx> <record idx>	move dns NS record
			dela <record idx>	delete DNS A record
			delns <record idx>	delete DNS NS record
		system cache		
			disp <0:none|1:name|2:type|3:IP|4:refCnt|5:ttl> [0:increase|1:decrease]	display DNS cache table
			flush	flush DNS cache
			negaperiod <second(60 ~ 3600)>	set negative cache period
			negative <0: disable|1: enable>	enable/disable dns negative cache
			positive <0: disable|1: enable>	enable/disable dns positive cache
	Httpd			
		debug	[on|off]	set http debug flag
	icmp			
		echo	[on|off]	set icmp echo response flag
		data	<option>	select general data type
			cmd [on|off]	check icmp echo reply command data
			rsp [on|off]	check icmp response
			indication [i|r|l|p]	set icmp indication
		status		display icmp statistic counter
		trace	[on|off]	turn on/off trace for debugging
		discovery	<iface> [on|off]	set icmp router discovery flag
	ifconfig		[iface] [ipaddr] [broadcast <addr> |mtu <value>|dynamic]	configure network interface
	ping		<hostid>	ping remote host
	route			
		status	[if]	display routing table
		add	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add route
		addiface	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add an entry to the routing table to iface
		drop	<host addr> [/<bits>]	drop a route
		flush		flush route table
		lookup	<addr>	find a route to the destination
		errcnt		
			disp	display routing statistic counters
			clear	clear routing statistic counters

	status			display ip statistic counters
	stroute			
		display	[rule # | buf]	display rule index or detail message in rule.
		load	<rule #>	load static route rule in buffer
		save		save rule from buffer to spt.
		config		
			name <site name>	set name for static route.
			destination <dest addr>[/<bits>] <gateway> [<metric>]	set static route destination address and gateway.
			mask <IP subnet mask>	set static route subnet mask.
			gateway <IP address>	set static route gateway address.
			metric <metric #>	set static route metric number.
			private <yes|no>	set private mode.
			active <yes|no>	set static route rule enable or disable.
	adjTcp		<iface> [<mss>]	adjust the TCP mss of iface
	adjmss		[mss]	adjust all system TCP mss of iface
	udp			
		status		display udp status
	rip			
		accept	<gateway>	drop an entry from the RIP refuse list
		activate		enable rip
		merge	[on|off]	set RIP merge flag
		refuse	<gateway>	add an entry to the rip refuse list
		request	<addr> [port]	send rip request to some address and port
		reverse	[on|off]	RIP Poisoned Reverse
		status		display rip statistic counters
		trace		enable debug rip trace
		mode		
			<iface> in [mode]	set rip in mode
			<iface> out [mode]	set rip out mode
		dialin_user	[show|in|out|both|none]	show dialin user rip direction
	tcp			
		ceiling	[value]	TCP maximum round trip time
		floor	[value]	TCP minimum rtt
		irtt	[value]	TCP default init rtt
		kick	<tcb>	kick tcb
		limit	[value]	set tcp output window limit
		max-incomplete	[number]	Set the maximum number of TCP incomplete connection.
		mss	[value]	TCP input MSS
		reset	<tcb>	reset tcb
		rtt	<tcb> <value>	set round trip time for tcb
		status	[tcb] [<interval>]	display TCP statistic counters
		syndata	[on|off]	TCP syndata piggyback
		trace	[on|off]	turn on/off trace for debugging
		window	[tcb]	TCP input window size
	samenet		<iface1> [<iface2>]	display the ifaces that in the same net
	uninet		<iface>	set the iface to uninet
	telnet		<host> [port]	execute telnet clinet command
	tftp			
		support		pritn if tfpt is support
		stats		display tftp status
	traceroute		<host> [ttl] [wait] [queries]	send probes to trace route of a remote host
	xparent			

		join	<iface1> [<iface2>]	join iface2 to iface1 group
		break	<iface>	break iface to leave ipxparent group
	anitprobe		<0|1> 1:yes 0:no	set ip anti-probe flag
	forceproxy		<display|set> [on|off] [servicePort] [proxyIp] [proxyport]	enable TCP forceproxy
	ave			anti-virus enforce
	urlfilter			
		enable		enable/disable url filter function
		reginfo		
			display	display urlfilter registration information
			name	set urlfilter registration name
			eMail <size>	set urlfilter registration email addr
			country <size>	set urlfilter registration country
			clearAll	clear urlfilter register information
		category		
			display	display urlfilter category
			webFeature [block/nonblock] [activex/java/cookei/webproxy]	block or unblock webfeature
			logAndBlock [log/logAndBlock]	set log only or log and block
			blockCategory [block/nonblock] [all/type(1-14)]	block or unblock type
			timeOfDay [always/hh:mm] [hh:mm]	set block time
			clearAll	clear all category information
		listUpdate		
			display	display listupdate status
			actionFlags [yes/no]	set listupdate or not
			scheduleFlag [pending]	set schedule flag
			dayFlag [pending]	set day flag
			time [pending]	set time
			clearAll	clear all listupdate information
		exemptZone		
			display	display exemptzone information
			actionFlags [type(1-3)][enable/disable]	set action flags
			add [ip1] [ip2]	add exempt range
			delete [ip1] [ip2]	delete exempt range
			reset	clear exemptzone information
		customize		
			display	display customize action flags
			actionFlags [filterList/disableAllExceptTrusted/ unblockRWFToTrusted/keywordBlock/fullPath/caseInsensitive/fileName][enable/disable]	set action flags
			logFlags [type(1-3)][enable/disable]	set log flags
			add [string] [trust/untrust/keyword]	add url string
			delete [string] [trust/untrust/keyword]	delete url string
			reset	clear all information
		logDisplay		display cyber log
		ftplist		update cyber list data
		listServerIP	<ipaddr>	set list server ip
		listServerName	<name>	set list server name
		general		

			enable	enable/disable url filter function
			display	display content filer's general setting
			webFeature	[block/nonblock] [activex/java/cookei/webproxy]
			timeOfDay[always/hh:mm] [hh:mm]	set block time
			exemptZone display	display exemptzone information
			exemptZone actionFlags [type(1-3)][enable/disable]	set action flags
			exemptZone add [ip1] [ip2]	add exempt range
			exemptZone delete [ip1] [ip2]	delete exempt range
			exemptZone reset	clear exemptzone information
			reset	reset content filter's general setting
		webControl		
			enable	enable cbr_filter
			display	display cbr_filter's setting
			logAndBlock [log/block/both]	set log or block on matched web site
			category	set blocked categories
			serverList display	display current cbr_filter servers
			serverList refresh	refresh cbr_filter servers
			queryURL [url][Server/localCache]	query url need to block or forward according the database on server or local cache
			cache display	display the local cache entries
			cache delete [entrynum/All]	delete the local cache entries
			cache timeout [hour]	Set timeout value of cache entries
			blockonerror [log/block][on/off]	choose log or block when server is unavailable
			unratedwebsite[block|log][on|off]	hoose log or block for unrated web site
			waitingTime [sec]	set waiting time for server
			reginfo display	display the license key with cerberian
			reginfo refresh	Check whether device had been registered and write the original license key to flash
			zssw	change the zssw's URL
	tredir			
		failcount	<count>	set tredir failcount
		partner	<ipaddr>	set tredir partner
		target	<ipaddr>	set tredir target
		timeout	<timeout>	set tredir timeout
		checktime	<period>	set tredir checktime
		active	<on|off>	set tredir active
		save		save tredir information
		disp		display tredir information
		debug	<value>	set tredir debug value
	rpt			
		active	[0:lan|1:dmz][1:yes|0:no]	active report
		start	[0:lan|1:dmz]	start report
		stop	[0:lan|1:dmz]	stop report
		url	[0:lan|1:dmz] [num]	top url hit list
		ip	[0:lan|1:dmz] [num]	top ip addr list
		srv	[0:lan|1:dmz] [num]	top service port list
	dropIcmp		[0 | 1]	to drop ICMP fragment packets
	nat			
		period	[period]	set nat timer period
		port	[port]	set nat starting external port number
		checkport		verify all server tables are valid
		timeout		

			gre [timeout]	set nat gre timeout value
			iamt [timeout]	set nat iamt timeout value
			generic [timeout]	set nat generic timeout value
			reset [timeout]	set nat reset timeout value
			tcp [timeout]	set nat tcp timeout value
			tcpother [timeout]	set nat tcp other timeout value
			udp [port] <value>	set nat udp timeout value of specific port
			display	display all the timeout values
		update		create nat system information from spSysParam
		iamt	<iface>	display nat iamt information
		lookup	<rule set>	display nat lookup rule
		loopback	[on|off]	turn on/off nat loopback flag
		reset	<iface>	reset nat table of an iface
		server		
			disp	display nat server table
			load <set id>	load nat server information from ROM
			save	save nat server information to ROM
			clear <set id>	clear nat server information
			edit active <yes|no>	set nat server edit active flag
			edit svrport <start port> [end port]	set nat server server port
			edit intport <start port> [end port]	set nat server forward port
			edit remotehost <start ip> [end ip]	set nat server remote host ip
			edit leasetime [time]	set nat server lease time
			edit rulename [name]	set nat server rule name
			edit forwardip [ip]	set nat server server ip
			edit protocol [protocol id]	set nat server protocol
			edit clear	clear one rule in the set
		service		
			irc [on|off]	turn on/off irc flag
			xboxlive [on|off]	turn on/off xboxlive flag
			sip debug	enable/disable sip debug flag
			sip display	display the sip call buffer
			aol [on|off]	Turn on/off aol flag
		resetport		reset all nat server table entries
		incikeport	[on|off]	turn on/off increase ike port flag
		session	[session per host]	set nat session per host value
		deleteslot	<iface> <slot>	delete specific slot of iface
		debug		
			natTraversal [on|off]	set NAT traversal debug flag
			hash [on|off]	set NAT hash table debug flag
			session [on|off]	set NAT session debug flag
		hashtable	<enifX, X=0, 1, 2, …>	show the NAT hash table of enifX
		natTable	[enifX, X=0, 1, 2, …]	show the NAT global information
		simulation	<enifX, X=0, 1, 2, …>	for engineer debug only
		acl		
			display	display all NAT acl set and rule information
			load <set number>	load a specific acl of set number
			save <set number>	save a specific acl of set number
		routing	[0:LAN|1:DMZ] [0:no|1:yes]	set NAT routing attributes
		historicalCHigh		Display the historical highest count of concurrent NAT sessions
		historicalHigh		Display the historical highest count of NAT sessions based on per host.
	igmp			

		debug	[level]	set igmp debug level
		forwardall	[on|off]	turn on/off igmp forward to all interfaces flag
		querier	[on|off]	turn on/off igmp stop query flag
		iface		
			<iface> grouptm <timeout>	set igmp group timeout
			<iface> interval <interval>	set igmp query interval
			<iface> join <group>	join a group on iface
			<iface> leave <group>	leave a group on iface
			<iface> query	send query on iface
			<iface> rsptime [time]	set igmp response time
			<iface> start	turn on of igmp on iface
			<iface> stop	turn off of igmp on iface
			<iface> ttl <threshold>	set ttl threshold
			<iface> v1compat [on|off]	turn on/off v1compat on iface
		robustness	<num>	set igmp robustness variable
		status		dump igmp status
	pr			
		clear		clear ip pr table counter information
		disp		display policy route set and rule information
		move		move specific policy route rule to another rule
		dispCnt		dump ip pr table counter information
		switch		turn on/off ip pr table counter flag

IPSec Related Command Home

Command				Description
ipsec				
	debug	type	<0:Disable | 1:Original on|off | 2:IKE on|off | 3: IPSec [SPI]|on|off | 4:XAUTH on|off | 5:CERT on|off | 6: All>	Turn on|off trace for IPsec debug information
		level	<0:None | 1:User | 2:Low | 3:High>	Set the debug level. Higher number means more detailed.
		display		Show debugging information, include type and level.
	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.
		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.
		wlan	<on|off>	After a packet is IPSec processed and will be sent to WLAN side, this switch is to control if this packet can be applied IPSec again.
	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.

		List		Display brief runtime phase 1 and phase 2 SA information
	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_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
	dial	<policy index>		Initiate IPSec rule <policy index> from ZyWALL box
	ikeDisplay	<rule #>		Display IKE rule #, if no rule number assigned, this command will show current working buffer. NOTE: If working buffer is null, it will show error messages. Please ADD or EDIT an IKE rule before display.
	ikeAdd			Create a working buffer for IKE rule.
	ikeEdit	<rule #>		Edit an existing IKE rule #
	ikeSave			Save working buffer of IKE rule to romfile.
	ikeList			List all IKE rules
	ikeDelete	<rule #>		Delete IKE rule #
	ikeConfig	name	<string>	Set rule name (max length is 31)
		negotiationMode	<0:Main | 1:Aggressive>	Set negotiation mode
		natTraversal	<Yes| No>	Enable NAT traversal or not.
		multiPro	<Yes|No>	Enable multiple proposals in IKE 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
		authMethod	<0:PreSharedKey | 1:RSASignature | 2:preShare Key+XAUTH | 3:RSASignature+XAUTH>	Set authentication method in phase 1 in IKE
		preShareKey	<ASCII | 0xHEX>	Set pre shared key in phase 1 in IKE
		certificate	<certificate name>	Set certificate file if using RSA signature as authentication method.

		encryAlgo	<0:DES | 1:3DES | 2:AES>	Set encryption algorithm in phase 1 in IKE
		authAlgo	<0:MD5 | 1:SHA1>	Set authentication algorithm in phase 1 in IKE
		saLifeTime	<seconds>	Set sa life time in phase 1 in IKE
		keyGroup	<0:DH1 | 1:DH2>	Set key group in phase 1 in IKE
		xauth	type <0:Client Mode | 1:Server Mode>	Set client or server mode.
			username <name>	Set xauth user name
			password <password>	Set xauth password
			radius <username> <password>	Ser radius username and password
	ipsecDisplay	<rule #>		Display IPSec rule #, if no rule number assigned, this command will show current working buffer. NOTE: If working buffer is null, it will show error messages. Please ADD or EDIT an IPSec rule before display.
	ipsecAdd			Create a working buffer for IPSec rule.
	ipsecEdit	<rule #>		Edit IPSec rule #
	ipsecSave			Save working buffer of IPSec rule to romfile.
	ipsecList			List all IPSec rules
	ipsecDelete	<rule #>		Delete IPSec rule #
	ipsecConfig	name	<string>	Set rule name. (max length is 31)
		active	<Yes | No>	Set active or not
		saIndex	<index>	Bind to which IKE rule.
		multiPro	<Yes | No>	Enable multiple proposals in IPSec or not
		nailUp	<Yes | No>	Enable nailed-up or not
		activeProtocol	<0:AH | 1:ESP>	Set active protocol in IPSec
		encryAlgo	<0:Null | 1:DES | 2:3DES | 3:AES>	Set encryption algorithm in IPSec
		encryKeyLen	<0:128 | 1:192 | 2:256>	Set encryption key length in IPSec
		authAlgo	<0:MD5 | 1:SHA1>	Set authentication algorithm in IPSec
		saLifeTime	<seconds>	Set sa life time in IPSec
		encap	<0:Tunnel | 1:Transport>	set encapsulation in IPSec
		pfs	<0:None | 1:DH1 | 2:DH2>	set pfs in phase 2 in IPSec
		antiReplay	<Yes | No>	Set anitreplay or not
		controlPing	<Yes|No>	Enable control ping or not
		logControlPing	<Yes|No>	Enable logging control ping events or not
		controlPingAddr	<IP>	Set control ping address
		protocol	<1:ICMP | 6:TCP | 17:UDP>	Set protocol
		lcAddrType	<0:single | 1:range | 2:subnet>	Set local address type
		lcAddrStart	<IP>	Set local start address
		lcAddrEndMask	<IP>	Set local end address or mask
		lcPortStart	<port>	Set local start port
		lcPortEnd	<port>	Set local end port
		rmAddrType	<0:single | 1:range | 2:subnet>	Set remote address type
		rmAddrStart	<IP>	Set remote start address
		rmAddrEndMask	<IP>	Set remote end address or mask
		rmPortStart	<port>	Set remote start port
		rmPortEnd	<port>	Set remote end port
	policyList			List all IPSec policies
	manualDisplay	<rule #>		Display manual rule #
	manualAdd			Add manual rule
	manualEdit	<rule #>		Edit manual rule #

	manualSave			Save IPSec rules
	manualList			List all IPSec rule
	manualDelete	<rule #>		Delete IPSec rule #
	manualConfig	name	<string>	Set rule name
		active	<Yes | No>	Set active or not
		myIpAddr	<IP address>	Set my IP address
		secureGwAddr	<IP address>	Set secure gateway
		protocol	<1:ICMP | 6:TCP | 17:UDP>	Set protocol
		lcAddrType	<0:single | 1:range | 2:subnet>	Set local address type
		lcAddrStart	<IP>	Set local start address
		lcAddrEndMask	<IP>	Set local end address or mask
		lcPortStart	<port>	Set local start port
		lcPortEnd	<port>	Set local end port
		rmAddrType	<0:single | 1:range | 2:subnet>	Set remote address type
		rmAddrStart	<IP>	Set remote start address
		rmAddrEndMask	<IP>	Set remote end address or mask
		rmPortStart	<port>	Set remote start port
		rmPortEnd	<port>	Set remote end port
		activeProtocol	<0:AH | 1:ESP>	Set active protocol in 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
		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
	manualPolicyList			List all manual policy
	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.
	Drop		<policy index>	Drop an active tunnel.
				-

PPP Related Command Home

Command				Description
ppp				
	bod			
		remote	<iface>	show remote bod information
		reset		reset bod
		setremote	<iface>	set remote bod

		status	<wan_iface>	show wan port bod status
		clear	<wan_iface>	clear wan port bod data
		on		set bod flag on
		off		set bod flag off
		node	<node> <dir>	config the statistic method for remote node bod traffic data
		debug	[on|off]	show bod debug flag
		cnt		
			disp	show bod state
			clear	clear bod state
	ccp		[on|off]	set/display dial-in ccp switch
	lcp			
		acfc	[on|off]	set address/control field compression flag
		pfc	[on|off]	set protocol field compression flag
		mpin	[on|off]	set incoming call MP flag
		callback	[on|off]	set callback flag
		bacp	[on|off]	set bandwidth allocation control flag
		echo		
			retry <retry_count>	set/display retry count to send echo-request
			time <interval>	set/display time interval to send echo-request
	ipcp			
		close		close connection on ppp interface
		list	<iface>	show ipcp state
		open		open fsm link
		timeout	[value]	set timeout interval when waiting for response from remote peer
		try		
			configure [value]	set/display fsm try config
			failure [value]	set/display fsm try failure
			terminate [value]	set/display fsm try terminate
		compress	[on|off]	set compress flag
		slots	[slot_num]	set number of slots
		idcompress	[on|off]	set/display slot id compress
		address	[on|off]	set/display ip one address option
	mp			
		default		show link default flag
			rotate	set link default to rotate
			split	set link default to split
		split	[0|1]	set/display link split
		rotate	[0|1]	set/display link rotate
		sequence		set/display mp start sequence
	configure			
		ipcp		
			compress [on|off]	enable/disable compress
			slots [slot_num]	select number of slots
			idcompress [on|off]	enable/disable slot id compress
			address [on|off]	set/display ip one address option
		atcp		apple talk feature not supported anymore
		ccp		
			ascend [on|off]	set/display ascend stac flag
			history <count>	set/display stac history count
			check [argv]	set/display stac check mode
			reset <mode>	set/display stac reset mode

			pfc [on|off]	set/display pfc flag
			debug [on|off]	set/display ccp debug flag
	iface			
			<iface> ipcp	show the ipcp status of the given iface
			<iface> ipxcp	show the ipxcp status of the given iface
			<iface> atcp	
			<iface> ccp [reset|skip|flush]	show the ccp status of the given iface
			<iface> mp	show the mp status of the given iface
	show		<channel>	show the ppp channel status
	fsm			
		trace		
			break [num] [count] [flag]	set the fsm log break value
			clear	clear the fsm log data
			disp	display the fsm log data
			filter [mask] [protocol]	set the fsm log filter value
		tdata		
			filter [protocol1] [protocol2] …	set the fsm filter data
			disp	display the fsm data
			clear	clear the fsm data
		struc		dump fsm data structure
	delay		[inteval]	set the delay timer for sending first PPP packet after call answered

Firewall Related Command Home

Command					Description
sys	Firewall				
		acl			
			disp		Display specific ACL set # rule #, or all ACLs.
		active	<yes|no>		Active firewall or deactivate firewall
		cnt			
			disp		Display firewall log type and count.
			clear		Clear firewall log count.
		dynamicrule			SUPPORT_DYNAMIC_PORT
		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			
			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 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 <name> <CA addr> <CA cert> <auth key> <subject> [key size]	Create a certificate request and enroll for a certificate immediately 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		Rename the specified trusted CA certificate. <old name>

		name> <new 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 <name> [on|off]		Specify whether or not the specified CA issues CRL. <name> 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.

Bandwidth management Related Command Home

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	The class can borrow bandwidth from its parent

					on|off>	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 <mask Smask> Sport protocol		Add a filter for class # in DMZ. 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 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.
	moveFilter	< channName>	<from>	<to>		User can move BWM filter order via this command. <channName>: lan, wan/wan1, dmz, wan2, wlan <from>: filter index <to>: filter index
	config	save				Save the configuration.
		load				Load the configuration.
		clear				Clear the configuration.

Load Sharing Command Home

Command				Description
ls				
	band	<up|down>	<WAN1 bandwidth+WAN2 bandwidth>	It is used to configure the bandwidth parameters. The CI format is ls band <method(up, down)|WAN1 loading bandwidth |WAN2 bandwidth. Ex: “ls band up 100 200” will configure the Load Sharing function dispatch the loading between WAN1 and WAN2 with 100K and 200K upstream loading.
	wrr		<Weight of WAN1> + <Weight of WAN2>	It is used to configure the weight parameters. The CI format is ls wrr <Weight of WAN1> + <Weight of WAN2>. The valid numver of weight is 0~10 Ex: “ls wrr 10 5” will configure the weight of the WAN1 to be 10, weight of the WAN2 to be 5.
	spillover		< upper bandwidth of primary WAN >	It is used to configure the spillover upper bandwidth of primary WAN.

				Ex: “ls spillover 100”, the router will send the traffic to secondary WAN when the primary WAN bandwidth exceeds 100Kbps.
	mode		<1:Least Load First|2:WRR|3:Spillover|255:None>	Change the dispatch mode. 1 is for dispatch packets by Dynamic Load Balancing, 2 is for dispatch packets by WRR, 3 is dispatch packets by Spillover. And 255 is for disable the Load Sharing function.
	timeframe		<10~600>	Change the Time Frame number. The valid number of it is 10~600
	disp			Display the Load Sharing configuration data
	debug			Debug CI commands
		online	<on|off>	To toggle the debug message on or off. This command is useful for debugging.

Bridge Related Command Home

Command				Description
bridge				
	mode		<1/0> (enable/disable)	turn on/off (1/0) LAN promiscious mode
	blt			related to bridge local table
		disp	<channel>	display blt data
		reset	<channel>	reset blt data
		traffic		display local LAN traffic table
		monitor	[on|off]	turn on/off traffice monotor. Default is off.
		time	<sec>	set blt re-init interval
	brt			related to bridge route table
		disp	[id]	display brt data
		reset	[id]	reset brt data
	cnt			related to bridge routing statistic table
		disp		display bridge route counter
		clear		clear bridge route counter
	Iface			Related to “bridge mode” access interface
		active	<yes/no>	Active bridge mode iface or not
		address	[ip]	Remote access IP address
		dns1	[ip]	First DNS server
		dns2	[ip]	Second DNS server
		dns3	[ip]	Third DNS server
		mask	[network mask]	Network mask
		gateway	[gateway ip]	Network gateway
		display		Display whole interface information
	Stat			related to bridge packet statistic table
		disp		display bridge route packet counter
		clear		clear bridge route packet counter
	Disp			display bridge source table
	fcs		<BriFcsCtl>	set bridge fcs control flag
	rstp			
		bridge		
			enable	enable this device RSTP function
			disable	disable this device RSTP function

			priority [pirority]	set RSTP pirority
			maxAge [max age]	set RSTP max age
			helloTime [hello time]	set hello time
			forwardDelay [forwarding delay]	set forwarding delay
			version <STP:0|RSTP:2>	switch STP or RSTP
		port		
			enable <Port_NO>	enable RSTP on this port
			disable <Port_NO>	disable RSTP on this port
			pathCost <Port_NO> [path cost]	set path cost on this port
			pirority <Port_NO> [pirority]	set pirority on this port
			edgePort <Port_NO> <True:1|False:0>	set edge or non-edge on this port
			p2pLink <Port_NO> <Auto:2|True:1|False:0>	set per to per link on this port
			mcheck <Port_NO>	set migrate check on this port
		disp		display RSTP information
		trace		turn on debug/trace message
		state		display RSTP information

myZyXEL.com Command Home

Command				Description
sys				
	myZyxelCom			
		checkUserName	<username>	Check the username exists or not
		register	<username> <password> <email> <countryCode>	Inout the registration information, include username, password, email, and country code.
		trialService	<service>, 1 : CF, 2 : 3in1, 3 : CF + 3in1	Input the service that to be tried.
		serviceUpgrade	<licence key>	Inout license key that you want to let service from trial to standard
		serviceRefresh	NULL	Refresh the myZyXEL.com service status
		display	NULL	Display all myZyXEL.com setting
		serviceDisplay	NULL	Display all service status, include expired day.

IDP Command Home

Command					Description
idp					IDP CI commands
	display				Display the enable setting and the protected interface setting
	load				Load the enable setting and the protected interface setting
	config				Config the enable setting and the protected interface setting
		enable	<on|off>		Config the enable setting.
		wan1	<on|off>		Config the protected interface setting.
		wan2	<on|off>		Config the protected interface setting.
		lan	<on|off>		Config the protected interface setting.
		dmz	<on|off>		Config the protected interface setting.
		wlan	<on|off>		Config the protected interface setting.
		wan	<on|off>		Config the protected interface setting.
	save				Save the enable setting and the protected interface setting
	tune				The tune command for

					IDP/Anti-Virus/Anti-Spam
		load			Load the tune configuration
		save			Save the tune configuration
		display			Display the tune configuration
		config			Config the tune configuration
			l4Udpcksum	<on|off>	Enable/Disable UDP checksum check
			l4Icmpcjsum	<on|off>	Enable/Disable ICMP checksum check
			l4Tcpcksum	<on|off>	Enable/Disable TCP checksum check
			l4Tcpwindowck	<on|off>	Enable/Disable TCP window check
			l4Tcpmssck	<on|off>	Enable/Disable TCP mss check
			l7Smtpasm	<on|off>	Enable/Disable TCP assembly for SMTP
			l7Pop3asm	<on|off>	Enable/Disable TCP assembly for POP3
			l7Httpasm	<on|off>	Enable/Disable TCP assembly for HTTP
			l7Ftpasm	<on|off>	Enable/Disable TCP assembly for FTP
			l7Ftpdataasm	<on|off>	Enable/Disable TCP assembly for FTPDATA
			l7Otherasm	<on|off>	Enable/Disable TCP assembly for other protocols
	update				The command about signature and signature update stuffs
		display			Show the signature information and the update setting
		load			Load the signature update setting
		save			Save the signature update setting
		start			Start the signature update
		config			Config the signature update setting
			autoupdate	<on|off>	Enable/Disable the autoupdate
			method	<1-3>	Config the update method
			dailyTime	<00-23>	Config the daily hour update schedule
			weeklyDay	<1-7>	Config the weekly day update schedule
			weeklyTime	<00-23>	Config the weekly hour update schedule
	signature				The command about signature post-process setting
		display			Display the current signature setting
		load	<Signature_ID>		Load the signature setting that its ID is SignatureIID
		save			Save the signature setting
		config			Config the current signature setting
			active	<on|off>	Enable/Disable the active option
			log	<on|off>	Enable/Disable the log option
			alert	<on|off>	Enable/Disable the alert option
			action	<1-6>	Set the post action
		reset			Reset the signature setting to the default setting
		listFullRef			List the IDP reference table of the full version signature
		listDeltaRef			List the IDP reference table of the delta version signature
		listUserConf			List the all signature setting
		reinit			Re-initialize the search engine/backend process engine
		clearAll			Clear signature file from the flash
		configAll			Config all signature settings
			active	<on|off>	Enable/Disable the active option to all

					signature settings
			log	<on|off>	Enable/Disable the log option to all signature settings
			alert	<on|off>	Enable/Disable the alert option to all signature settings
			action	<1-6>	Set the post action to all signature settings

Anti-Virus Command Home

Command					Description
av					Anti-Virus CI commands
	display				Show the anti-virus setting
	load				Load the anti-virus setting
	config				Config the anti-virus setting
		enable			Enable/Disable the anti-virus function
		httpScanAllMime	<on|off>		Enable/Disable scanning all mime type files. If we don't enable this option , ZyWall will just scan files with the application type
		pop3ScanAllMime	<on|off>		Enable/Disable scanning all mime type files. If we don't enable this option , ZyWall will just scan files with the application type
		smtpScanAllMime	Mon|off>		Enable/Disable scanning all mime type files. If we don't enable this option , ZyWall will just scan files with the application type
		decompress	<on|off>		Enable/Disable the decompress on the fly. You should also enable tcp assembly to support the decompress on the fly.
		ftp			Config the anti-virus setting for FTP
			display		Show the anti-virus setting for FTP
			active	<on|off>	Enable/Disable the anti-virus function for FTP
			log	<on|off>	Enable/Disable the log option
			alert	<on|off>	Enable/Disable the alert option
			breakfile	<on|off>	Enable/Disable the breakfile option
			sendmsg	<on|off>	Enable/Disable the sendmsg option
			wan1	<on|off>	Config the protected interface setting.
			wan2	<on|off>	Config the protected interface setting
			lan	<on|off>	Config the protected interface setting
			dmz	<on|off>	Config the protected interface setting
			wlan	<on|off>	Config the protected interface setting
		http			Config the anti-virus setting for HTTP
			display		Show the anti-virus setting for HTTP
			active	<on|off>	Enable/Disable the anti-virus function for HTTP
			log	<on|off>	Enable/Disable the log option
			alert	<on|off>	Enable/Disable the alert option
			breakfile	<on|off>	Enable/Disable the breakfile option
			sendmsg	<on|off>	Enable/Disable the sendmsg option
			wan1	<on|off>	Config the protected interface setting.
			wan2	<on|off>	Config the protected interface setting
			lan	<on|off>	Config the protected interface setting
			dmz	<on|off>	Config the protected interface setting
			wlan	<on|off>	Config the protected interface setting
		smtp			Config the anti-virus setting for SMTP
			display		Show the anti-virus setting for SMTP
			active	<on|off>	Enable/Disable the anti-virus function for SMTP

			log	<on|off>	Enable/Disable the log option
			alert	<on|off>	Enable/Disable the alert option
			breakfile	<on|off>	Enable/Disable the breakfile option
			sendmsg	<on|off>	Enable/Disable the sendmsg option
			wan1	<on|off>	Config the protected interface setting.
			wan2	<on|off>	Config the protected interface setting
			lan	<on|off>	Config the protected interface setting
			dmz	<on|off>	Config the protected interface setting
			wlan	<on|off>	Config the protected interface setting
		pop3			Config the anti-virus setting for POP3
			display		Show the anti-virus setting for POP3
			active	<on|off>	Enable/Disable the anti-virus function for POP3
			log	<on|off>	Enable/Disable the log option
			alert	<on|off>	Enable/Disable the alert option
			breakfile	<on|off>	Enable/Disable the breakfile option
			sendmsg	<on|off>	Enable/Disable the sendmsg option
			wan1	<on|off>	Config the protected interface setting.
			wan2	<on|off>	Config the protected interface setting
			lan	<on|off>	Config the protected interface setting
			dmz	<on|off>	Config the protected interface setting
			wlan	<on|off>	Config the protected interface setting
	save				Save the anti-virus setting
	update				The command about signature and signature update stuffs
		display			Show the signature information and the update setting
		load			Load the signature update setting
		save			Save the signature update setting
		start			Start the signature update
		config			Config the signature update setting
			autoupdate	<on|off>	Enable/Disable the autoupdate
			method	<1-3>	Config the update method
			dailyTime	<00-23>	Config the daily hour update schedule
			weeklyDay	<1-7>	Config the weekly day update schedule
			weeklyTime	<00-23>	Config the weekly hour update schedule
	tune				The tune command for IDP/Anti-Virus/Anti-Spam
		load			Load the tune configuration
		save			Save the tune configuration
		display			Display the tune configuration
		config			Config the tune configuration
			l4Udpcksum	<on|off>	Enable/Disable UDP checksum check
			l4Icmpcjsum	<on|off>	Enable/Disable ICMP checksum check
			l4Tcpcksum	<on|off>	Enable/Disable TCP checksum check
			l4Tcpwindowck	<on|off>	Enable/Disable TCP window check
			l4Tcpmssck	<on|off>	Enable/Disable TCP mss check
			l7Smtpasm	<on|off>	Enable/Disable TCP assembly for SMTP
			l7Pop3asm	<on|off>	Enable/Disable TCP assembly for POP3
			l7Httpasm	<on|off>	Enable/Disable TCP assembly for HTTP
			l7Ftpasm	<on|off>	Enable/Disable TCP assembly for FTP
			l7Ftpdataas	<on|off>	Enable/Disable TCP assembly for FTPDATA

			m		
			l7Otherasm	<on|off>	Enable/Disable TCP assembly for other protocols

Anti-Spam Command [Home]

Command					Description
as					Anti-Spam CI commands
	asAction	[0|1]			Forward/Block exceeding mails sessions.
	debug				Debug for AntiSpam
		customListServ			Set custom server list server
			ip	[IP address]	Set custom server list server IP address
			enable	[0:disable|1:enable]	Enable/Disable custom server list server
		customRateServ			Set custom rating server server.
			ip	[IP address]	Set custom rating server IP address
			enable	[0:disable|1:enable]	Enable/Disable custom rating server
		envelope	[on|off]		Enable/Disable envelope debug message.
		http	[on|off]		Enable/Disable http debug message.
		mail	[on|off]		Enable/Disable mail debug message.
		pop3	[on|off]		Enable/Disable pop3 debug message.
		smtp	[on|off]		Enable/Disable smtp debug message.
	delete				Delete AntiSpam static filter.
		blackRule	<num start> [num end]		Delete black rule filter. User can delete one or a set of filter.
		whiteRule	<num start> [num end]		Delete white rule filter. User can delete one or a set of filter.
	display				
		antispam			Display AntiSpam configuration.
		serverlist			Display rating server list.
	enable	<0:disable | 1:enable>			Enable/Disable AntiSpam.
	failTolerance	[time]			Set rating server fail tolerance time. If the rating server timeout interval over this tolerance, this server will be removed from server list.
	freeSession				Free all mail ssessions.
	getServerList	<Y:Yes|N:No>			Send server list request manually.