ZyXEL

Firmware Release Note

ZyWALL 2WG

Release 4.02(AQI.0)

Date:	**Jan., 19, 2007**
Author:	**Nash Fan**
Project Leader:	**Ray. Chu**

ZyXEL ZyWALL 2WG Standard Version release 4.02(AQI.0) Release Note

Date: Jan., 19, 2007

Supported Platforms:

ZyXEL ZyWALL 2WG

Versions:

ZyNOS Version: V4.02(AQI.0) | 01/19/2007 09:43:14
Bootbase Version: V1.08 | 11/01/2006 12:17:09
Vantage Agent Version: 2.1.4

Note:

1. Restore to Factory Defaults Setting Requirement: Yes.
2. The setting of ignore triangle route is on in default ROM FILE. Triangle route network topology has potential security crisis. If you are not clear about it, please refer to Appendix for the triangle route issue.
3. IKE process in phase 2 will check ID information between system and the peer. If you found that the IPSec connection is failed, please check your settings.
4. 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 and 802.1X when you enable WLAN feature.
7. When UPnP is on, and then reboot the device, Windows XP will not detect UPnP and refresh “My Network Places→Local Network”. Plug in network wire again can solve this problem.
8. The default port roles for LAN/DMZ setting is: port 1 to port 4 are all LAN ports.
9. In bridge mode, If LAN side DHCP clients want to get DHCP address from WAN side DHCP server, you may need to turn on the firewall rule for BOOT_CLIENT service type in WAN→LAN direction.
10. Under Bridge Mode, all LAN ports will behave as a hub, and all DMZ ports will also

behave as another hub.

11. If you want traffic redirect feature to work, you should turn on WAN ping check by "sys rn pingcheck 1".
12. The first entry for static route is reserved for creating WAN default route and is READ-ONLY.
13. 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 the myzyxel.com.
14. WAN1 and WAN2 must be different subnet.
15. Web help in eWC is not ready.
16. 802.11h is not supported.
17. 5.25~5.7 GHz is not supported.
18. If you change country code, please reboot device to get the correct wireless RF channels.
19. SMT 7.1 is not supported.

Known Issues:

System Limitation

[Bandwidth Management]

1. Bandwidth Management doesn’t work on wireless LAN.

[Content Filter]

1. Can’t block ActiveX in some case. (Sometime the ActiveX block fails. This is because the ActiveX is cached in C:\WINNT\Downloaded Program Files\ If you want to test the ActiveX block functionality. Please clear the cache in windows.)

[MISC]

1. At SMT24.1, the collisions for WAN, LAN and DMZ port are not really counted.
2. Symptom: LAN host can ping Internet while LAN host change cable from LAN port to DMZ port.
   Condition:
   (1) Host connects to LAN port and gets DHCP address from router.
   (2) Unplug LAN host cable and plug it into DMZ port.
   (3) The host can still ping Internet using LAN DHCP address
   (4) The scenario will continue about 30secs.
3. When device is wirting flash, all the interrupt/service will be stopped. (Firmware upload will take tens of seconds)
4. IDP and Anti-Virus features must accompany with firewall, otherwise some action may fail.

Issues

[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.

[Bandwidth Management]

1. Bandwidth management H.323 service does not support Netmeeting H.323 application.
2. Using BWM in PPPoE/PPTP mode, there are two filters for FTP and H323 ALG
   (1) If we execute FTP first then H323 cannot pass through ZyWALL.
   (2) If we execute H323 before FTP, all functions work properly.
3. 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. CF Denied Access Message and Redirect URL have not limit sepcial character, it will caused DUT crash.
2. CF Denied Access Message can run script.

[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. Don't use CI command "bridge rstp bridge enable" to enable RSTP, it will change the initial Path Cost value to an incorrect value.

[Wireless]

1. Wireless traffic is block.
   Topology:
   PC--------wireless ZyWALL wan-------Internet
   (1) PC using wireless connect to ZW2WG.
   (2) Set a global IP as ZW2WG WAN's IP.
   (3) Using TfGen and set the configuration as follows:
       i. Utilization: 1000000
       ii. Destination: 1.1.1.1
   (4) After a period of time, the PC can scan the wireless SSID but can't associate with ZW2WG.

[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
   (2) In ZyWALL_A and ZyWALL_B, add a "WAN to LAN" firewall rule to pass traffic with port "5060".
   (3) In ZyWALL_A and ZyWALL_B, add a port forwarding rule "5060" to P2002.
   (4) In ZyWALL_A and ZyWALL_B, enable SIP ALG.
   (5) Setup both P2002 to Peer-to-Peer mode.
   (6) Making the SIP connection by P2002 will be failed.
   (7) 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.

[VPN]

1. Symptom: PC can't ping remote gateway through VPN tunnel under this special topology.
   Condition:
   PC------LAN ZyWALL_A WAN-----------------LAN ZyWALL_B
   WAN-------Internet
   (192.168.1.33） （192.168.100.33） (192.168.100.1) （172.202.77.145)

   (1) VPN configuration in ZyWALL_A:
   WAN IP Address=192.168.100.33，WAN IP Subnet Mask=255.255.255.0， Gateway IP Address=192.168.100.1.
   Gateway policy，Name=IKE1，Remote Gateway Address=192.168.100.1， Pre-Shared Key=12345678.
   Network policy for IKE1，Active=enable，Name=IPSec1，Local Network/Starting IP Address=192.168.1.33， Remote Network/Starting IP Address=0.0.0.0
   (2) VPN configuration in ZyWALL_B
   WAN IP Address=172.202.77.145，WAN IP Subnet Mask=255.255.0.0，Gateway IP Address=172.202.77.1.
   Gateway policy，Name=IKE1，Remote Gateway Address=192.168.100.33，
   Pre-Shared Key=12345678.
   Network policy for IKE1，Active=enable，Name=IPSec1，Local Network/Starting IP Address=0.0.0.0， Remote Network/Starting IP Address=192.168.1.33.
   (3) When we established the VPN tunnel between ZyWALL_A and ZyWALL_B, we can access ZyWALL_B (192.168.100.1) with the remote management,
   such as Telnet, FTP…, this traffic will go through VPN tunnel. However, we can not ping ZyWALL_B (192.168.100.1) successfully because this ICMP traffic did not go through VPN tunnel to ZyWALL_B.
2. SNMP tools get ZYWALL VPN MIB data, the index of received data are wrong if rules are larger than 1.
3. VPN rule swap does not support NAT Traversal.
4. When VPN tunnel is up with 3G as “My Gateway”, VPN tunnel will not be dropped when 3G WAN is disconnected.
5. Topology:
   PC1(1.33) --DUT---(VPN)-----ZW2WG---PC5(2.33)
   PC2(11.33)--
   PC3(21.33)--
   PC4(31.33)--
   Configure as attached romfile.
   Steps:
   (1) DUT configures 2 IKE dynamic rules, and each attaches 2 IPSEC rules.
   (2) PC5 can ping PC3 and PC4 and the associated tunnels are built up.
   (3) When PC5 ping PC1, it will fail, and log shows ”[ID] : Remote IP [192.168.2.0] / [255.255.255.0] conflicts”.

[MISC]

1. The DMZ TxPkts counter increment at about 1 pkt/min even without any Ethernet

cables ever connected.

2. Under PPTP encapsulation mode, we can not access some website like http://www.kimo.com.tw/
3. In eWC->Statistics, Tx data for Dial Backup is not correct.
4. Symptom: Dial Backup can’t work when Traffic Redirect is enabled.
   Condition:
   (1)Enable Traffic Redirect and Dial Backup
   (2)When disconnect WAN line, the traffic will go through Backup Gateway
   (3)At now, disconnect the Backup Gateway, the Dial Backup modem should be triggered. But it doesn’t.
5. Symptom : After system password hash, downgrade F/W, user can't use GUI
   Condition:
   (1) In patch 6 support password encrypted, CLI "sys pwdEncryption on". "sys md5 1234" will display a string "xxxxxxx"
   (2) Downgrade F/W to patch2 (not support password encrypted), SMT can use password "xxxxxxx" login but GUI can't
6. The status of WAN2(3G) is ”LCP Up” and WAN2 can’t be dialed anymore.
7. Triangle route issue（LAN side is responder）

Features:

Modifications in V4.02(AQI.0) | 01/19/2007

First release.

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

New function

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

Modification

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

Note

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

```
                 Menu 24.11 - Remote Management Control

    TELNET Server:    Port = 23       Access = ALL
                 Secure Client IP = 0.0.0.0
    FTP Server:      Port = 21       Access = ALL
                 Secure Client IP = 0.0.0.0
    SSH Server:      Certificate = auto_generated_self_signed_cert
                 Port = 22       Access = ALL
                 Secure Client IP = 0.0.0.0
    HTTPS Server:     Certificate = auto_generated_self_signed_cert
                 Authenticate Client Certificates = No
                 Port = 443      Access = ALL
                 Secure Client IP = 0.0.0.0
    HTTP Server:      Port = 80       Access = ALL
                 Secure Client IP = 0.0.0.0
    SNMP Service:     Port = 161      Access = ALL
                 Secure Client IP = 0.0.0.0
    DNS Service:      Port = 53       Access = ALL
                 Secure Client IP = 0.0.0.0
                Press ENTER to Confirm or ESC to Cancel:
```

Appendix 2 Trigger Port

Introduction

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

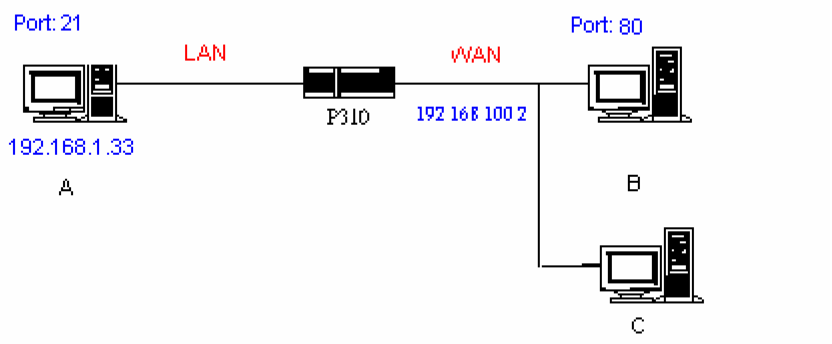
These triggered events can be timed so that they erase the port mapping as soon as they are done with the data transfer, so that the port mapping can be triggered by another Client computer. This gives the ***illusion*** that multiple computers can use the same port mapping at the same time, but the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

How to use it

Following table is a configuration table.

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

How it works



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

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

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

internal table for this port. (This behavior is the same as we did for port forwarding.)

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

Notes

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

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

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

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

There are two CI commands:

(1) "sys filter netbios disp": It will display the current filter mode.

Example ouput:

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

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

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

Example commands:

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

Appendix 4 Traffic Redirect/Static Route Application Note

Why traffic redirect/static route be blocked by ZyWALL

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

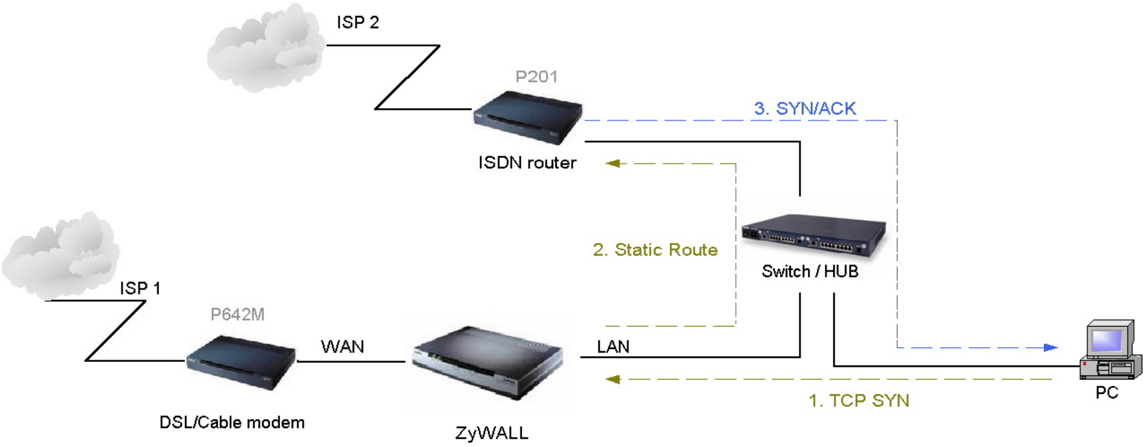


Figure 4-1 Triangle Route

Figure 4-1 indicates the triangle route topology. It works fine with turn off firewall. Let's take a look into the perspective toward this situation.

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

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

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

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

That causes all of outgoing TCP traffics being reset!

How traffic redirect/static route works under protection - Solutions

(1) Gateway on alias IP network

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

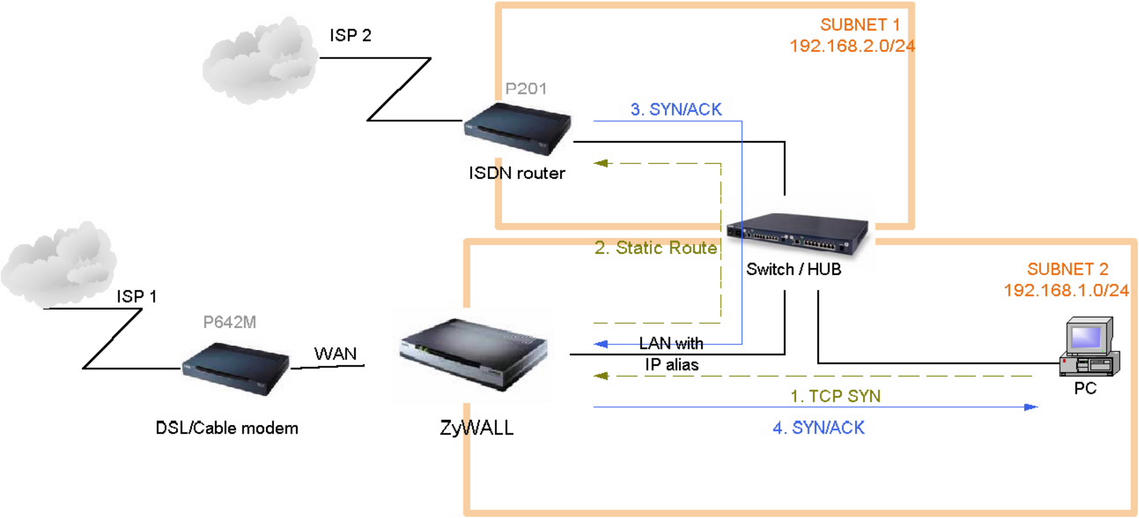


Figure 4-2 Gateway on alias IP network

(2) Gateway on WAN side

A working topology is suggested as below.

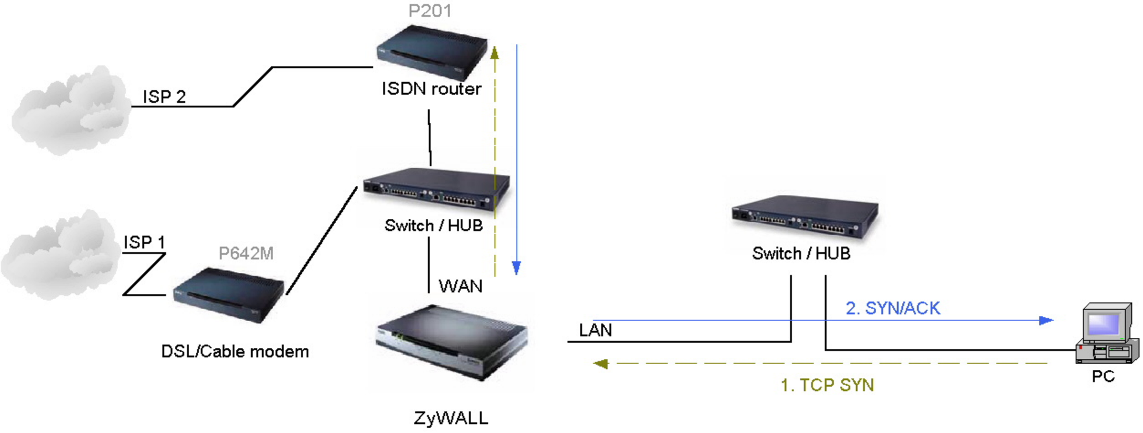


Figure 5-3 Gateway on WAN side

Appendix 5 IPSec FQDN support

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

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

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

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

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

We can put all combinations in to these two tables:

(Local ID Type is IP):

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

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

(Peer ID Type is IP):

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

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

Summary:

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

Appendix 6 Embedded HTTPS proxy server

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

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

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

Appendix 7 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 8 IPSec IP Overlap Support

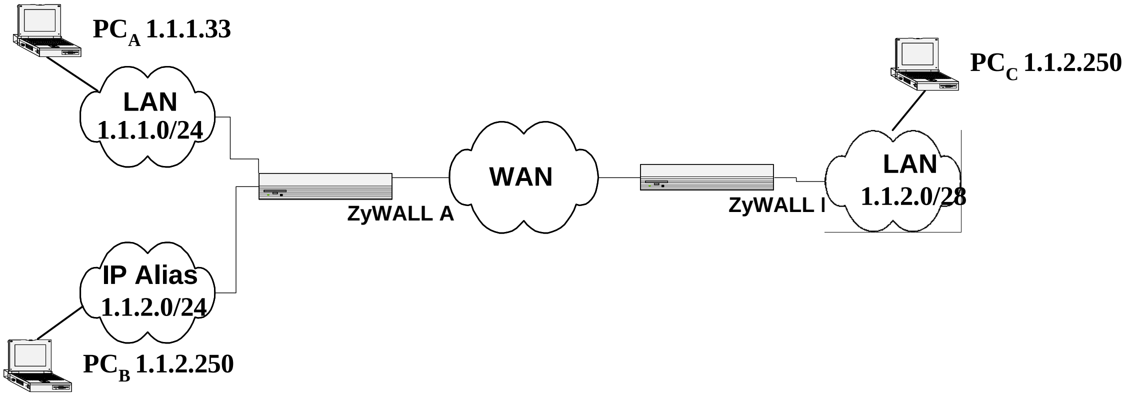


Figure 1

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 9 VPN Local IP Address Limitation

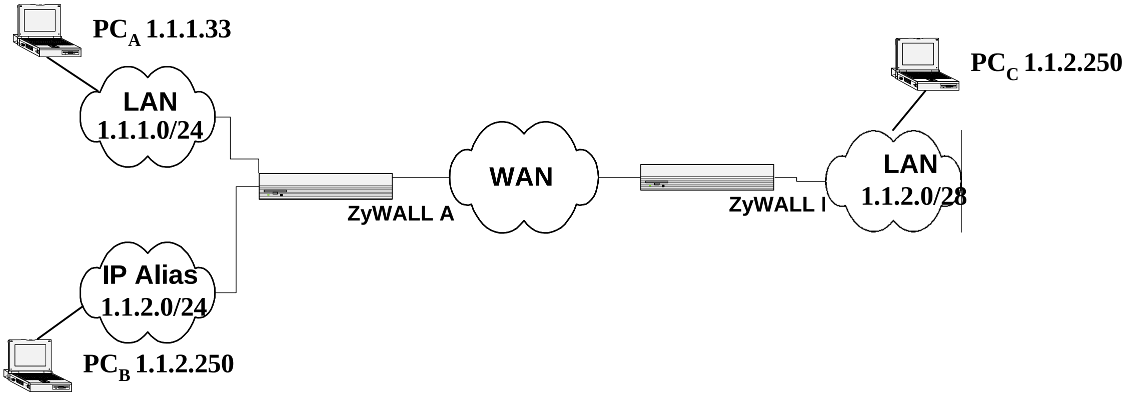


Figure 1

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 10 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

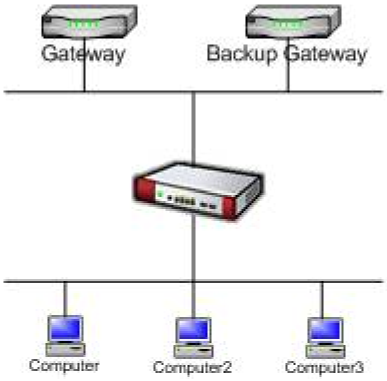
ZyXEL VPN Client
Security Gateway: 1.1.1.1 Phase one Authentication method: Preshare Key Remote: 192.168.1.0/24

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”.

Appendix 11 The mechanism of Gratuitous ARP in the ZyWALL



In the past, if the ZyWALL gets a gratuitous ARP it will not update the sender's MAC mapping into its ARP table. In current design, if you turn on 'ip arp ackGratuitous active yes', the ZyWALL will response such packet depends on two case: 'ip arp ackGratuitous forceUpdate on' or 'ip arp ackGratuitous forceUpdate off'. if you turn on forceUpdate, then the ZyWALL gets gratuitous ARP, it will force to update MAC mapping into the ARP table, otherwise if turn off forceUpdate, then the ZyWALL gets gratuitous

ARP, it will update MAC mapping into the ARP table only when there is no such MAC mapping in the ARP table.

Give an example for its purpose, there is a backup gateway on the network as the picture. One day, the gateway shuts down and the backup gateway is up, the backup gateway is set a static IP as original gateway's IP, it will broadcast a gratuitous ARP to ask who is using this IP. If ackGratuitous is on, the ZyWALL receive the gratuitous ARP from the backup gateway, it will also send an ARP request to ask who is using this IP. Once the ZyWALL gets a reply from backup gateway, it will update its ARP table so that the ZyWALL can keep a correct gateway ARP entry to forward packets. If ackGratuitous is off, the ZyWALL will not keep a correct gateway ARP entry to forward packets.

There is one thing need to be noticed: update the ARP entry might still have dangers more or less if there is a spoofing attack. So we suggest if you have no opportunity to meet the problem, you can turn off ackGratuitous. forceUpdate on will be more dangerous than forceUpdate off because it update ARP table even when ARP entry is existing.

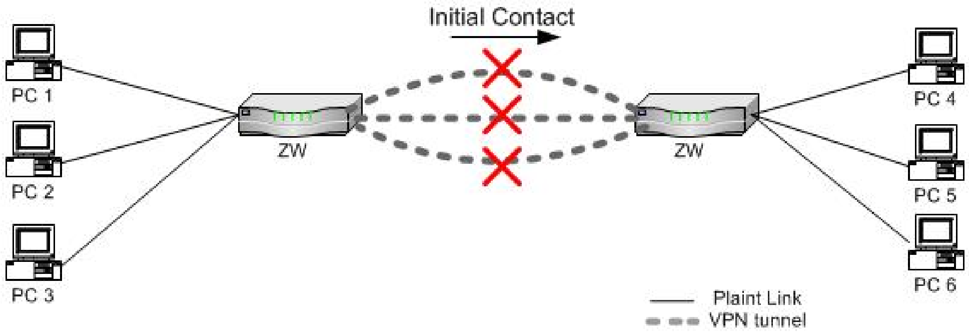
Appendix 12 The mechanism when the ZyWALL receives a IKE packets with IC

[RFC 2407]The INITIAL-CONTACT(IC) status message may be used when one side wishes to inform the other that this is the first SA being established with the remote system. The receiver of this Notification Message might then elect to delete any existing SA's it has for the sending system under the assumption that the sending system has rebooted and no longer has access to the original SA's and their associated keying material.

The ZyWALL has two ways to delete SA when it receives IC, it is switched by a global option 'ipsec initContactMode gateway/tunnel':

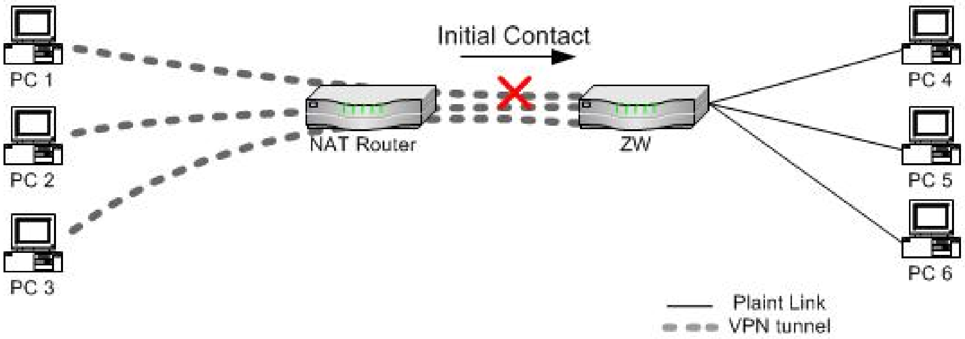
(1)ipsec initContactMode gateway

When the ZyWALL receives a IKE packets with IC, it deletes all tunnels with the same secure gateway IP. It is default option because the ZyWALL is site to site VPN device. Take the picture 1 as example, there are three VPN tunnels are created between ZWA and ZWB, but ZWA reboots for some reasons, and after rebooting, the ZWA will send a IKE with IC to the ZWB, then the ZWB will delete all existing tunnels whose security gateway IP is the same as this IKE's one and build a new VPN tunnel for the sender.



(2)ipsec initContactMode tunnel

When the ZyWALL receives a IKE packets with IC, it deletes only one existing tunnel, whose security gateway IP is not only the same as this IKE's one and also its phase 2 ID(network policy) should match. It is suitable when your tunnel is created from a VPN peer to ZyWALL and there are more than two this kind of VPN peers build tunnels behind the same NAT router. Take the picture 2 as example, PC 1, PC2 and PC3 has it's own VPN software to create tunnels with ZW. Suppose that the PC1, PC2 and PC3 separately create different tunnels with ZW for the traffic to PC4, PC5 and PC6, once the PC1 reboots for some reasons, and after rebooting, the PC1 sends a IKE with IC to the ZWB, then the ZWB will only delete the tunnel which is used by PC1 and PC4 and build a new VPN tunnel for it. So other tunnels will not be disconnected.



Annex A CI Command List

Last Updated: 2006/10/31

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

U : CAT_PUBLIC (0x02) ➔ User usable and visible.
E : CAT_INTERNAL (0x01) ➔ User unusable and invisible.
O : CAT_OEM (0x04) ➔ OEM product only.
H : CAT_HIDE (0) ➔ User usable and invisible.
Following attributes are for the device which has bridge and router capability.
(Compiler flag is “BRIDGE_MODE”)
R : CAT_MODE_ROUTER (1 << 10) ➔ User usable in router mode
B : CAT_MODE_BRIDGE (1 << 11) ➔ User usable in bridge mode

System Related Command

Home

Command				Description
sys				
	adjtime			retrive date and time from Internet
	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			
		add	<phone dir [rate] [upTime]>	add entry to call history
		display		display call history
		remove	<index>	remove entry from call history
	clear			clear the counters in GUI status menu
	clock			
		display		display system clock
	countrycode		[countrycode]	set country code
	date		[year month date]	set/display date

	debug			
		romfile		
			cert [0:reserve/1:erase]	erase all the certificates
			display	display romfile debug settings
			isp [0:reserve/1:erase]	erase the account and password of ISP
			prekey [0:reserve/1:reset]	reset the system IPSec pre-shared key
			profile [0:reserve/1:erase]	erase the accounts and passwords of 802.1X and XAUTH
			pwd [0:reserve/1:reset]	reset system password
			radius	erase Authentication and Accounting keys
			update [0:reserve/1:erase]	update romfile depend on current configuration
			wep [0:reserve/1:erase]	erase all WEP encryption keys
	dir			display file directory
	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
	isr		[all|used|free]	display interrupt service routine
	interrupt			display interrupt status
	lanfilter			
		load		Load the global configuration

		config		Config the global settings
			active [on|off]	Enable/Disable the function
		save		Save the global configuration
		display		Display the global configuration
		entry		Commands about per filter entry configuration
			load [entry_number]	Load the entry_numberTH MAC entry
			config mac [MAC]	Configure the MAC value of the loaded entry
			display	Display the entry configuration
			save	Save the entry configuration
			displayList	Show the all entry settings
	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
.....		updatePeriod	<second>	set the log table update period
		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
			dynacllog <0:no|1:yes>	active to enable dynamic ACL log
		lastAlert	<index>	display the last #index alert in the centralized log.
	map			display whole memory map content
	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]	
	memory		<address> <length>	display memory content
	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
	mode	<router/bridge/ zero>		switch router,bridge and zero configuration mode
	model			display server model name
	ProbeType		[icmp | arp]	DHCP server probing type
	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
		pingcheck	[on|off]	Enable/disable single WAN pingcheck
		save	[entry no.]	save remote node information
	smt			not support in this product

	stdio		[second]	change terminal timeout value
	support			not support in this product
	time		[hour [min [sec]]]	display/set system time
	timer			
		disp		display timer cell
		trace	[on|off]	set/display timer information online
		start	[tmValue]	start a timer
		stop	<ID>	stop a timer
	tos			
		display		display all runtime TOS
		listPerHost		display all host session count
		debug	[on|off]	turn on or off TOS debug message
		dump	<session>	dump session information
		sessPerHost	<number>	configure session per host value
		tcprst	<session>	send TCP RST to both source and dest IP
		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
		tempTOSDisplay		display temporal TOS records.
		tempTOSTimeout	[timeout value]	set/display temporal timeout value
		historicalCHigh		Display the historical highest count of concurrent TOSs
		historicalHigh		Display the historical highest count of TOSs based on per host.
		qatest		For QA IDP test only Run this command just toggle the flag.
	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,sds100, 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
		dead		let watch dog take place using while loop
		info		Display hardware and software watchdog information.
	authserver	localuser	load	Load local user database information
			edit <index> <0:inactive|1:active> <username> <password>	Edit local user database
			disp <all|index>	Display local user database
			save	Save local user database
	romreset			restore default romfile
	mrd			
		atwe	<mac> [country code] [debug flag] [featurebit]	configure mac, country code, debug flag, featurebit in the boot module
		atwz	<12 digitals 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
	management FQDN			
		load		Load the configuration
		config		Config the settings
			enable [On|off]	Enable or disable the function
			fqdn [FQDN]	The FQDN setting
		save		Save the configuration
		display		Show the configuration
	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
	client			
		name	[username]	Display/Set client name
		password	[password]	Display/Set client password
	perfmon			Performance monitoring CI command
		clear		Clear all counters. Restart the

					measurement.
		Show stat			Show delta time statistics. Avg = total / cnt.
		Show cnt			Show time stamps for all counters.
	atmu				Show multiboot client version
	pwdHash		[on | off] <newPassword> <oldPassword>		The password saved in ROM file can be hashed by MD5.
	md5		<string>		This command will hash the string by MD5. Tha maximum length of the string is 64.
	threatReport				
		idp			
			active		Active/inactive threat report functionality for IDP
			dump		Dump all entry in memory
			flush		Flush all data and update time stamp
			summary		Show summary
			statistic	id	Show top N statistic records for id field
			statistic	src	Show top N statistic records for source IP field
			statistic	dst	Show top N statistic records for destination IP field
		av			
			active		Active/inactive URM report functionality for AV
			dump		Dump all entry in memory
			flush		Flush all data and update time stamp
			summary		Show summary
			statistic	id	Show top N statistic records for id field
			statistic	src	Show top N statistic records for source IP field
			statistic	dst	Show top N statistic records for destination IP field
		as			
			active		Active/inactive threat report functionality for AS
			dump		Dump all entry in memory
			flush		Flush all data and update time stamp
			summary		Show summary
			statistic	sender	Show top N statistic records for sender mail address field
			statistic	src	Show top N statistic records for source IP field
			statistic	score	Show score distribution for AS
	usermode				
		active	[yes | no]		Active/inactive ZWP1 user mode
		userPass	[new password] [retype password]		Change user mode password

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

		mem	<addr> <data> [type]	write memory data in address
	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
	debug			
		disp	<ch_name>	display ethernet debug infomation
		reset	<ch_name>	reset ethernet debug state
		create	<ch_name> <num>	create ethernet debug state
		destory	<ch_name>	destory ethernet debug state
		level	<ch_name> <level>	set the ethernet debug level level 0: disable debug log level 1:enable debug log (default)
	edit			
		load	<ether no.>	load ether data from spt
		mtu	<value>	set ether data mtu
		speed	<speed>	set ether data speed
		save		save ether data to spt
	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
	window		[size]	set pptp data rx-window-size
	rxTimeout		[timeout]	set pptp data rx-timeout
	queue		[size]	set pptp data tx-queue-size
	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			
		disp		display TX session information
		send	<device name> <pkt size> <interval(ms)> <count>	start TX session
		stat	<device name>	display data statistic from TX session
		stop	<session>	stop a TX session

	dial		<device name> <phone number>	begin dialing
	disp		<device name>	displays ndis's copy of a channel's spt profile
	dqtest		<device name> <command>	send AT command
	drop		<device name>	disconnect
	dump		<start#> <display#>	dump aux debug information
	st		<start#> <display#>	dump aux state
	event			
		disp		aux event trace display
		clear		aux event trace clear
	init		<device name>	initialize aux channel
	is		<device name>	send event to in-service
	mbuf		<index>	dump mbuf information
	mem		<addr> <data> [type]	write data at addr in memory
	mode		<device name> [mode]	set mode
	mstatus		<device name>	display modem last call status
	mtype		<device name>	display modem type
	netstat		<device name>	prints upper layer packet information
	oos		<device name>	send event to out-of-service
	prtl		<device name> <level>	set display level
	rate		<device name>	show tx rx rate
	read		<device name>	read spt from ROM and copy to ndis's copy
	redirect		<device name>	invalid
	ringbuf			
		cmd		
			clear <device name>	clear ringbuffer
			disp <device name>	display ringbuffer
		data		
			clear	clear command ringbuffer
			disp <start> <len>	display command ringbuffer
	save		<device name>	save aux information
	set		<device name> <field> <value>	set aux information
	signal		<device name>	show aux signal
	speed		<device name> <type> [value]	display/set aux speed
	test		<device name> <type>	test aux channel
	version			invalid
	usrmdm	flag		DUT support USR modem
	cdmamdm	flag		DUT support CDMA modem

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 the current AntiSpam settings
	all				Save all working SPT buffer into flash.
display	firewall				Displays all the firewall settings
		set <set#>			Display current entries of a set configuration; including timeout values, name, default-permit, and number of rules in the set.
		set <set#>	rule <rule#>		Display current entries of a rule in a set.
		attack			Display all the attack alert settings in PNC
		e-mail			Display all the e-mail settings in PNC
		?			Display all the available sub commands
	custom-service				Display all configured custom services.
	custom-service <entry #>				Display custom service <entry #>
	anti-spam				Displays all the AntiSpam settings
edit	firewall				
		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		Edit email schedule when log is full or per hour, day, week.

			|daily | weekly>		
			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		Edit the timeout for an idle UDP session before it is terminated

			<seconds>		
			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#>	action <permit | drop | reject>	Edit whether a packet is permitted, dropped or rejected when it matches this rule
				name <string>	Edit/Update rule name with <string>
				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	Select and edit a source address range of a packet which complies to this rule.

				address>	
				destaddr-single <ip address>	Select and edit a destination address of a packet which complies to this rule
				destaddr-subnet <ip address> <subnet mask>	Select and edit a destination address and subnet mask if a packet which complies to this rule.
				destaddr-range <start ip address> <end ip address>	Select and edit a destination address range of a packet which complies to this rule.
				tcp destport-single <port#>	Select and edit the destination port of a packet which comply to this rule. For non-consecutive port numbers, the user may repeat this command line to enter the multiple port numbers.
				tcp destport-range <start port#> <end port#>	Select and edit a destination port range of a packet which comply to this rule.
				udp destport-single <port#>	Select and edit the destination port of a packet which comply to this rule. For non-consecutive port numbers, users may repeat this command line to enter the multiple port numbers.
				udp destport-range <start port#> <end port#>	Select and edit a destination port range of a packet which comply to this rule.
				desport-custom <desired custom port name>	Type in the desired TCP/UDP 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	
		ftpPortNum	[port number]	Support a different port number on FTP ALG.	
	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.	
		gratuitous	<on|off>	Switch the duplicate IP address detection based on Gratuitous ARP	
		ackgratuitous			
			active	[yes | no]	Active/inactive to accept gratuitous arp request.

			forceUpdate	[on | off]	Force update when we received a gratuitous request and detect our arp catch has the arp entry.
	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 group|1:user defined> <isp group idx|ip address>	edit dns A record
			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
			ttl <second(60 ~ 3600)>	set positive cache maximum ttl
	httpClient			
		display		display the system HTTP client state
		debug	<on|off>	turn on/off HTTP client debug message
		recover		recover the overtime used HTTP client session
	httpd			
		debug	[on|off]	set http debug flag
	icmp			
		echo	[on|off]	set icmp echo response flag
		data	<option>	select general data type
		check		
			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</mask bits>] <broadcast [addr]> <mtu [value]> <mss [value]> <dynamic> <showoff>	configure network interface
	ping		<hostid>	ping remote host
	pong		<hostid> [<size> <time-interval>]	pong 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
	smtp			
		server	[addr]	set smtp server
		destmail	[addr]	set destination mail addr
		srcmail	[addr]	set source mail addr
		sendmail		send mail
		addrlist		list smtp server, dest, return addr
		addrreset		reset smtp server, dest, return addr
	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
	sidepath			
		clear		clear side path
		disp		display side path
		set	<iface> <gateway>	set side path
	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]	enable TCP forceproxy

			[proxyport]	
	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|1 hh:mm hh:mm|2 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|1 hh:mm hh:mm|2 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 licenseid <license key>	Write inputted license key to flash if it is valid
			reginfo refresh	Check whether device had been registered and write the original license key to flash
			zssw	change the zssw's URL
			test slot [num]	send many requests, specified by num, to external Content Filtering server at the same time
			test report	watch the statistics of the time stamp of

				each Content Filtering state
			test clearSlot	disconnect all current connections between router and external Content Filtering server
			test mode <0|1|2>	User need to turn the test mode to 1 or 2 before test mode 0: normal mode. mode 1: The result of a request will not be saved into cache. mode 2: The result of a request will be saved into cache.
			kogserver <domain>	Configure domain name of CF log server.
		Bypass	[LAN|DMZ|WAN] [ON|OFF]	Let traffic matches LAN->LAN, DMZ->DMZ or WAN->WAN directions can be bypassed content filtering.
	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
			ldap [on|pff]	Turn on/off LDAP parser.
		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
			conenat [on|off]	set NAT cone nat 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	<1|0>		turn on|off trace for IPsec debug information
	ipsec_log_disp			show IPSec log, same as menu 27.3
	route	dmz	<on|off>	After a packet is IPSec processed and will be sent to DMZ side, this switch is to control if this packet can be applied IPSec again.
				Remark: Only supported in ZyWALL100
		lan	<on|off>	After a packet is IPSec processed and will be sent to LAN side, this switch is to control if this packet can be applied IPSec again.

				Remark: Command available since 3.50(WA.3)
		wan	<on|off>	After a packet is IPSec processed and will be sent to WAN side, this switch is to control if this packet can be applied IPSec again.
				Remark: Command available since 3.50(WA.3)
	show_runtime	sa		display runtime phase 1 and phase 2 SA information
		spd		When a dynamic rule accepts a request and a tunnel is established, a runtime SPD is created according to peer local IP address. This command is to show these runtime SPD.
	switch	<on|off>		As long as there exists one active IPSec rule, all packets will run into IPSec process to check SPD. This switch is to control if a packet should do this. If it is turned on, even there exists active IPSec rules, packets will not run IPSec process.
	timer	chk_my_ip	<1~3600>	- Adjust timer to check if WAN IP in menu is changed
				- Interval is in seconds
				- Default is 10 seconds
				- 0 is not a valid value
		chk_conn.	<0~255>	- Adjust auto-timer to check if any IPsec connection has “only outbound traffic but no inbound traffic” for certain period. If yes, system will disconnect it.
				- Interval is in minutes
				- Default is 2 minuets
				- 0 means never timeout
		update_peer	<0~255>	- Adjust auto-timer to update IPSec rules which use domain name as the secure gateway IP.
				- Interval is in minutes
				- Default is 30 minutes
				- 0 means never update
		chk_input	<0~255>	- Adjust input timer to check if any IPSec connection has no inbound traffic for a certain period. If yes, system will disconnect it.
				- Interval is in minutes
				- Default is 2 minuets
				- 0 means never timeout
				Remark: Command available since

				3.50(WA.3)
	updatePeerIp			Force system to update IPSec rules which use domain name as the secure gateway IP right away.
				Remark: Command available since 3.50(WA.3)
	dial	<rule #>		Initiate IPSec rule <#> from ZyWALL box
				Remark: Command available since 3.50(WA.3)
	display	<rule #>		Display IPSec rule #
	remote	key	<string>	I add a secured remote access tunnel with pre-shared key. It is a dynamic rule with local: the route's WAN IP. The algorithms with it are fixed to phase1: DES+MD5, DH1 and SA lifetime 28800 seconds; phase2: DES+MD5, PFS off, no anti-replay and SA lifetime 28800 seconds. The length of pre-shared key is between 8 to 31 ASCII characters.
		switch	<on|off>	Activate or de-activate the secured remote access tunnel.
	keep_alive	<rule #>	<on|off>	Set ipsec keep_alive flag
	load	<rule #>		Load ipsec rule
	save			Save ipsec rules
	config	netbios	active <on|off>	Set netbios active flag
			group <group index1, group index2…>	Set netbios group
		name	<string>	Set rule name
		active	<Yes | No>	Set active or not
		keeyAlive	<Yes| No>	Set keep alive or not
		natTraversal	<Yes| No>	Enable NAT traversal or not.
		lcIdType	<0:IP | 1:DNS | 2:Email>	Set local ID type
		lcIdContent	<string>	Set local ID content
		myIpAddr	<IP address>	Set my IP address
		peerIdType	<0:IP | 1:DNS | 2:Email>	Set peer ID type
		peerIdContent	<string>	Set peer ID content
		secureGwAddr	<IP address | Domain name>	Set secure gateway address or domain name
		protocol	<1:ICMP | 6:TCP | 17:UDP>	Set protocol
		lcAddrType	<0:single | 1:range | 2:subnet>	Set local address type
		lcAddrStart	<IP>	Set local start address
		lcAddrEndMask	<IP>	Set local end address or mask
		lcPortStart	<port>	Set local start port
		lcPortEnd	<port>	Set local end port
		dnsServer	<IP>	Set DNS server for IPSec VPN
		rmAddrType	<0:single | 1:range | 2:subnet>	Set remote address type
		rmAddrStart	<IP>	Set remote start address

		rmAddrEndMask	<IP>	Set remote end address or mask
		rmPortStart	<port>	Set remote start port
		rmPortEnd	<port>	Set remote end port
		antiReplay	<Yes | No>	Set anitreplay or not
		keyManage	<0:IKE | 1:Manual>	Set key manage
		ike	negotiationMode <0:Main | 1:Aggressive>	Set negotiation mode in phase 1 in IKE
			authMethod <0:PreSharedKey | 1:RSASignature	Set authentication method in phase 1 in IKE
			preShareKey <string>	Set pre shared key in phase 1 in IKE
			certFile <FILE>	Set certificate file if using RSA signature as authentication method.
			p1EncryAlgo <0:DES | 1:3DES>	Set encryption algorithm in phase 1 in IKE
			p1AuthAlgo <0:MD5 | 1:SHA1>	Set authentication algorithm in phase 1 in IKE
			p1SaLifeTime <seconds>	Set sa life time in phase 1 in IKE
			p1KeyGroup <0:DH1 | 1:DH2>	Set key group in phase 1 in IKE
			activeProtocol <0:AH | 1:ESP>	Set active protocol in phase 2 in IKE
			p2EncryAlgo <0:Null | 1:DES | 2:3DES>	Set encryption algorithm in phase 2 in IKE
			p2AuthAlgo <0:MD5 | 1:SHA1>	Set authentication algorithm in phase 2 in IKE
			p2SaLifeTime <seconds>	Set sa life time in phase 2 in IKE
			encap <0:Tunnel | 1:Transport>	set encapsulation in phase 2 in IKE
			pfs <0:None | 1:DH1 | 2:DH2>	set pfs in phase 2 in IKE
		manual	activeProtocol <0:AH | 1:ESP>	Set active protocol in manual
		manual ah	encap <0:Tunnel | 1:Transport>	Set encapsulation in ah in manual
			spi <decimal>	Set spi in ah in manual
			authAlgo <0:MD5 | 1:SHA1>	Set authentication algorithm in ah in manual
			authKey <string>	Set authentication key in ah in manual
		manual esp	encap <0:Tunnel | 1:Transport>	Set encapsulation in esp in manual
			spi <decimal>	Set spi in esp in manual
			encryAlgo <0:Null | 1:DES | 2:3DES>	Set encryption algorithm in esp in manual
			encryKey <string>	Set encryption key in esp in manual
			authAlgo <0:MD5 | 1:SHA1>	Set authentication algorithm in esp in manual
			authKey < string>	Set authentication key in esp in manual
		exUseMode	[enable|disable]	Set exclusive use mode for client tunnel flag
		exUseMac	[MAC address]	Set exclusive use mode for client tunnel MAC address

	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.
	dropFrag		<on|off>	Set the flag whether fragment packet will be dropped or not if its size is smaller than output MTU.

New 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.
				Remark: Only supported in ZyWALL100
		lan	<on|off>	After a packet is IPSec processed and will be sent to LAN side, this switch is to control if this packet can be applied IPSec again.
				Remark: Command available since 3.50(WA.3)
		wan	<on|off>	After a packet is IPSec processed and will be sent to WAN side, this switch is to control if this packet can be applied IPSec again.
	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
	updatePeerIp			Force system to update IPSec rules which use domain name as the secure gateway IP right away.
	dial	<rule index> <policy index>		Initiate IPSec rule <#> policy <#> from ZyWALL box
	enable	<on|off>		Turn on/off IPSec feature
	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:preShareKey+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
		ha	enable <on|off>	Enable / disable IPSec HA
			redunSecGwAddr <IP address | Domain name>	Configure redundant remote secure gateway address or domain name
			failback enable <on|off>	Enable or disable “Fail back to primary secure gateway when possible”
			failback interval <number>	Configure the check interval for fail back detection
			failover display	Display current fail over detection method
			failover dpd <on|off>	Enable / disable fail over by DPD
			failover outputIdleTime <on|off>	Enable / disable fail over by output idle timer
			failover pingCheck <on|off>	Enable / disable fail over by ping check
	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
		activeZero	<Yes|No>	Activate the policy for the zero configuration mode
		natActive	<Yes|No>	Activate the NAT over IPSEC function
		natType	<0:One-to-One|1:Many-to-One|2:Many-One-to-One>	Configure the NAT mapping tyoe
		natPrivateStart	<IP>	Configure the NAT over IPSEC private starting address
		natPrivateEnd	<IP>	Configure the NAT over IPSEC private ending address

	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".
	swCfScan		<on|off>	Enable / disable the Content Filter for IPSec packet.
	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.
	ha	pingRetryCnt	<value> (1~10)	Ping retry fail tolerence
		debug	<on|off|runtime|spt>	On: turn on debug message Off: turn on debug message Runtime: show runtime data structure Spt: show SPT record data
	Drop		<policy index>	Drop a active tunnel.
	swSkipPPTP		<on|off>	Enable / disable to skip PPTP packets to go in ipsec tunnel.
	initContactMode		<tunnel | gateway>	Set initial contact mode to base on tunnel or gateway. Change to tunnel mode can support multiple VPN client which located at same NAT router.
	async	active	<on|off>	Enable / disable the asynchronous mode
		utility		Crypto engine utility rate
		queue	<on|off>	Enable / disable the asynchronous queue function
		display		Asynchronous mode function status
		debug	<on|off>	Show asynchronous debug message
	swDevTri		<on|off>	Enable / disable device trigger tunnel

Nortel CI commands

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.
				Remark: Only supported in ZyWALL100
		lan	<on|off>	After a packet is IPSec processed and will be sent to LAN side, this switch is to control if this packet can be applied IPSec again.

				Remark: Command available since 3.50(WA.3)
		wan	<on|off>	After a packet is IPSec processed and will be sent to WAN side, this switch is to control if this packet can be applied IPSec again.
	show_runtime	sa		display runtime phase 1 and phase 2 SA information
		spd		When a dynamic rule accepts a request and a tunnel is established, a runtime SPD is created according to peer local IP address. This command is to show these runtime SPD.
	switch	<on|off>		As long as there exists one active IPSec rule, all packets will run into IPSec process to check SPD. This switch is to control if a packet should do this. If it is turned on, even there exists active IPSec rules, packets will not run IPSec process.
	timer	chk_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
	updatePeerIp			Force system to update IPSec rules which use domain name as the secure gateway IP right away.
	dial	<rule index> <policy index>		Initiate IPSec rule <#> policy <#> from ZyWALL box
	enable	<on|off>		Turn on/off IPSec feature
	display	<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.
	load	<rule #>		Edit an existing IKE rule #
	save			Save working buffer of IKE rule to romfile.
	config	name	<string>	Set rule name (max length is 31)
		active	<Yes|No>	Active the rule or not
		negotiationMode	<0:Main | 1:Aggressive>	Set negotiation mode
		natTraversal	<Yes| No>	Enable NAT traversal or not.
		p1MultiPro	<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:preShareKey+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.
		p1EncryAlgo	<0:DES | 1:3DES | 2:AES>	Set encryption algorithm in phase 1 in IKE
		p1AuthAlgo	<0:MD5 | 1:SHA1>	Set authentication algorithm in phase 1 in IKE
		p1SaLifeTime	<seconds>	Set sa life time in phase 1 in IKE
		keyGroup	<0:DH1 | 1:DH2>	Set key group in phase 1 in IKE
		p2MultiPro	<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
		p2EncryAlgo	<0:Null | 1:DES | 2:3DES | 3:AES>	Set encryption algorithm in IPSec
		p2EncryKeyLen	<0:128 | 1:192 | 2:256>	Set encryption key length in IPSec
		p2AuthAlgo	<0:MD5 | 1:SHA1>	Set authentication algorithm in IPSec
		p2SaLifeTime	<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
	policyConfig	saIndex	<index>	Bind to which IKE rule
		active	<Yes|No>	Active the rule or not
		controlPing	<Yes|No>	Enable control ping 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
	policySave			Save the policy.
	policyList			List all IPSec policies
	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.

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

Bridge Related Command

Home

Command				Description
bridge				
	mode		<1/0> (enable/disable)	turn on/off (1/0) LAN promiscious mode
	block	<ipx | poe | ip | arp | bpdu | unknow>	<on | off>	Block ipx, poe, ip, arp, bpdu, unknown Ethernet frame pass through in bridge 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

HDAP Related Command

Home

Command				Description
hdap				
	debug		[on|off]	set hdap debug flag
	reset			reset hdap

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

				Smask> Sport protocol		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.
	vpnTraffic			<on|off>		Change BWM classifier do classify based on inner protocol header or IPSec header.
	packetBased			<on|off>		Change BWM classifier based on stream based or packet based

Firewall Related Command

Home

Command					Description
sys	Firewall				
		acl			
			disp		Display specific ACL set # rule #, or all ACLs.
			delete		Delete specific ACL set # rule #.
		active	<yes|no>		Active firewall or deactivate firewall
		clear			Clear firewall log
		cnt			
			disp		Display firewall log type and count.
			clear		Clear firewall log count.
		debug			Set firewall debug level.
		disp			Display firewall log
		init			### nothing. ###
		mailsubject			
			disp		Display mail setting which is used to mail alert.
			edit		Edit mail setting.
		online			Set firewall log online.
		pktdump			Dump the 64 bytes of dropped packet by firewall
		tos			
			delete		Delete specific TOS session.
			display		Display TOS sessions.
			status		Display TOS sessions' status.
			dump		Dump TOS.
		tosctrl			
			destination		Display TOS destination hash
			incomplete		Display TOS incomplete List.
		dynamicrule			

			display		Display firewall dynamic rules
			timeout		Set dynamic ACL rule timeout value
		dos			
			smtp		Set SMTP DoS defender on/off
			display		Display SMTP DoS defender setting.
			ignore		Set if firewall ignore DoS in lan/wan1/wan2/dmz/wlan/vpn
		ignore			
			logBroadcast	<from> <to> <on|off>	Set ignore log broadcast flag. The <from> and <to> parameters include lan/wan1/wan2/dmz/wlan/vpn.
			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		
			self_signed <name> <subject> <key> [validity period]	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> specifies the key size. Valid options are

				0, 512, 768, 1024, 1536 and 2048 bits. When 0 is specifed, the default value 1024 is applied. It can also be used to specify an existing key by preceding the key name with a \. Example: \key_17. [validity period] specifies the validity period in years. Valid range is from 1 to 30. The default is 3.
			request <name> <subject> [key]	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] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits. It can also be used to specify an existing key by preceding the key name with a \. Example: \key_17.
			scep_enroll <name> <CA addr> <CA cert> <auth key> <subject> [key]	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] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits. It can also be used to specify an existing key by preceding the key name with a \. Example: \key_17.
			cmp_enroll <name> <CA addr> <CA cert> <auth key> <subject> [key]	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] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits. It can also be used to specify an existing key by preceding the key name with a \. Example: \key_17.
		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.
		http_import <url> <name> [proxyurl]		Import a certificate file from a remote web server as the device’s own certificate. The certificate file must be in one of the following formats: 1) Binary X.509, 2) PEM-encoded X.509, 3) Binary PKCS#7, and 4) PEM-encoded PKCS#7. <url> specifies the location of the certificate to be imported. <name> specifies the name as which the imported certificate is to be saved. [proxyurl] specifies the address and port of an optional HTTP proxy to use. For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist. After the importation, the certification request will automatically be deleted.
		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.
	my_key	create <name> [key size]		Create an RSA key pair. <name> specifies a descriptive name for the generated key pair. [key size] specifies the key size. Valid options are 512, 768, 1024, 1536 and 2048 bits. The default is 1024 bits. Note that key generation may take up to one minute.
		import <name>		Import the PEM-encoded key from stdin. [name] specifies the descriptive name as which the imported key is to be saved.
		export <name>		Export the PEM-encoded key to stdout for user to copy and paste. <name> specifies the name of the key to be exported.
		delete <name>		Delete the specified key. <name> specifies the name of the key to be deleted.
		list		List all my keys and related information.
		rename <old name> <new name>		Rename the specified key. <old name> specifies the name of the key to be renamed. <new name> specifies the new name as which the key is to be saved.
	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.
		http_import <url> <name> [proxyurl]		Import a certificate file from a remote web server as the device's trusted CA. The certificate file must be in one of the following formats: 1) Binary X.509, 2) PEM-encoded X.509, 3) Binary PKCS#7, and 4) PEM-encoded PKCS#7. <url> specifies the location of the certificate to be imported. <name> specifies the name as which the imported certificate is to be saved. [proxyurl] specifies the address and port of an optional HTTP proxy to use.
		export <name>		Export the PEM-encoded certificate to stdout for user to copy and paste. <name> specifies the name of the certificate to be exported.

		view <name>		View the information of the specified trusted CA certificate. <name> specifies the name of the certificate to be viewed.
		verify <name> [timeout]		Verify the certification path of the specified trusted CA certificate. <name> specifies the name of the certificate to be verified. [timeout] specifies the timeout value in seconds (optional). The default timeout value is 20 seconds.
		delete <name>		Delete the specified trusted CA certificate. <name> specifies the name of the certificate to be deleted.
		list		List all trusted CA certificate names and basic information.
		rename <old name> <new name>		Rename the specified trusted CA certificate. <old name> specifies the name of the certificate to be renamed. <new name> specifies the new name as which the certificate is to be saved.
		crl_issuer <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.
		http_import <url> <name> [proxyurl]		Import a certificate file from a remote web server as the device’s trusted remote host. The certificate file must be in one of the following formats: 1) Binary X.509, 2) PEM-encoded X.509, 3) Binary PKCS#7, and 4) PEM-encoded PKCS#7. <url> specifies the location of the certificate to be imported. <name> specifies the name as which the imported certificate is to be saved. [proxyurl] specifies the address and port of an optional HTTP proxy to use.
		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.
		counters		
			display	Display the PKI counters.
			clear	Clear the PKI counters.

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.

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.
		lan-lan	<on|off>		Config the protected interface setting.
		lan-wan	<on|off>		Config the protected interface setting.
		lan-dmz	<on|off>		Config the protected interface setting.
		lan-wan2	<on|off>		Config the protected interface setting.
		lan-wlan	<on|off>		Config the protected interface setting.
		wan-lan	<on|off>		Config the protected interface setting.
		wan-wan	<on|off>		Config the protected interface setting.
		wan-dmz	<on|off>		Config the protected interface setting.
		wan-wan2	<on|off>		Config the protected interface setting.
		wan-wlan	<on|off>		Config the protected interface setting.
		dmz-lan	<on|off>		Config the protected interface setting.
		dmz-wan	<on|off>		Config the protected interface setting.
		dmz-dmz	<on|off>		Config the protected interface setting.
		dmz-wan2	<on|off>		Config the protected interface setting.
		dmz-wlan	<on|off>		Config the protected interface setting.
		wan2-lan	<on|off>		Config the protected interface setting.
		wan2-wan	<on|off>		Config the protected interface setting.
		wan2-dmz	<on|off>		Config the protected interface setting.
		wan2-wan2	<on|off>		Config the protected interface setting.
		wan2-wlan	<on|off>		Config the protected interface setting.
		wlan-lan	<on|off>		Config the protected interface setting.
		wlan-wan	<on|off>		Config the protected interface setting.
		wlan-dmz	<on|off>		Config the protected interface setting.
		wlan-wan2	<on|off>		Config the protected interface setting.
		wlan-wlan	<on|off>		Config the protected interface setting.
	save				Save the enable setting and the protected

					interface setting
	clean				Clean all the IDP matrix configurations.
	commonDebug				The debug command for IDP/Anti-Virus/Anti-Spam
		display			Show the debug setting for IDP/Anti-Virus/Anti-Spam
		tos	<on|off>		Set the tos debug flag for IDP/Anti-Virus/Anti-Spam
		ipfrag	<on|off>		Set the ipfrag flag for IDP/Anti-Virus/Anti-Spam
		tcpasm	<on|off>		Set the tcpasm debug flag for IDP/Anti-Virus/Anti-Spam
		tcpprocess	<on|off>		Set the tcpprocess debug flag for IDP/Anti-Virus/Anti-Spam
		l7process	<on|off>		Set the l7process debug flag for IDP/Anti-Virus/Anti-Spam
		autoupdate	<on|off>		Set the autoupdate debug flag for the IDP/Anti-Virus signature autoupdate
		reengine	<on|off>		Set the reengine debug flag for the IDP/Anti-Virus SW/HW search engine
		bwengine	<on|off>		Set the bwengine debug flag for IDP backend process
		reLibDbg	<on|off>		Set the reLibDbg debug flag for the Lionic resoft library
		showIaCb			Show the runtime debug information for IDP/Anti-Virus
		showMemUseInfo			Show the memory usage information for IDP/Anti-Virus
	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
		displayMinute			Display the current update minute setting
		configMinute	[00-59]		Config the current update minute 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
		clearFullSig			Clear the full version signature file from the flash
		clearDeltaSig			Clear the delta version 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
		overZipSession	[0:Block| 1:Forward]		Forward session when the session number is over the maximum ZIP sessions.
		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
			lan-lan	<on|off>	Config the protected interface setting
			lan-wan	<on|off>	Config the protected interface setting
			lan-dmz	<on|off>	Config the protected interface setting
			lan-wan2	<on|off>	Config the protected interface setting
			lan-wlan	<on|off>	Config the protected interface setting
			wan -lan	<on|off>	Config the protected interface setting
			wan -wan	<on|off>	Config the protected interface setting
			wan -dmz	<on|off>	Config the protected interface setting
			wan -wan2	<on|off>	Config the protected interface setting
			wan -wlan	<on|off>	Config the protected interface setting
			dmz -lan	<on|off>	Config the protected interface setting
			dmz -wan	<on|off>	Config the protected interface setting
			dmz -dmz	<on|off>	Config the protected interface setting
			dmz -wan2	<on|off>	Config the protected interface setting

			dmz -wlan	<on|off>	Config the protected interface setting
			wan2 -lan	<on|off>	Config the protected interface setting
			wan2-wan	<on|off>	Config the protected interface setting
			wan2-dmz	<on|off>	Config the protected interface setting
			wan2-wan2	<on|off>	Config the protected interface setting
			wan2-wlan	<on|off>	Config the protected interface setting
			wlan -lan	<on|off>	Config the protected interface setting
			wlan -wan	<on|off>	Config the protected interface setting
			wlan -dmz	<on|off>	Config the protected interface setting
			wlan -wan2	<on|off>	Config the protected interface setting
			wlan -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
			lan-lan	<on|off>	Config the protected interface setting
			lan-wan	<on|off>	Config the protected interface setting
			lan-dmz	<on|off>	Config the protected interface setting
			lan-wan2	<on|off>	Config the protected interface setting
			lan-wlan	<on|off>	Config the protected interface setting
			wan -lan	<on|off>	Config the protected interface setting
			wan -wan	<on|off>	Config the protected interface setting
			wan -dmz	<on|off>	Config the protected interface setting
			wan -wan2	<on|off>	Config the protected interface setting
			wan -wlan	<on|off>	Config the protected interface setting
			dmz -lan	<on|off>	Config the protected interface setting
			dmz -wan	<on|off>	Config the protected interface setting
			dmz -dmz	<on|off>	Config the protected interface setting
			dmz -wan2	<on|off>	Config the protected interface setting
			dmz -wlan	<on|off>	Config the protected interface setting
			wan2 -lan	<on|off>	Config the protected interface setting
			wan2-wan	<on|off>	Config the protected interface setting
			wan2-dmz	<on|off>	Config the protected interface setting
			wan2-wan2	<on|off>	Config the protected interface setting
			wan2-wlan	<on|off>	Config the protected interface setting
			wlan -lan	<on|off>	Config the protected interface setting
			wlan -wan	<on|off>	Config the protected interface setting
			wlan -dmz	<on|off>	Config the protected interface setting
			wlan -wan2	<on|off>	Config the protected interface setting
			wlan -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
			lan-lan	<on|off>	Config the protected interface setting
			lan-wan	<on|off>	Config the protected interface setting
			lan-dmz	<on|off>	Config the protected interface setting
			lan-wan2	<on|off>	Config the protected interface setting
			lan-wlan	<on|off>	Config the protected interface setting
			wan -lan	<on|off>	Config the protected interface setting
			wan -wan	<on|off>	Config the protected interface setting
			wan -dmz	<on|off>	Config the protected interface setting
			wan -wan2	<on|off>	Config the protected interface setting
			wan -wlan	<on|off>	Config the protected interface setting
			dmz -lan	<on|off>	Config the protected interface setting
			dmz -wan	<on|off>	Config the protected interface setting
			dmz -dmz	<on|off>	Config the protected interface setting
			dmz -wan2	<on|off>	Config the protected interface setting
			dmz -wlan	<on|off>	Config the protected interface setting
			wan2 -lan	<on|off>	Config the protected interface setting
			wan2-wan	<on|off>	Config the protected interface setting
			wan2-dmz	<on|off>	Config the protected interface setting
			wan2-wan2	<on|off>	Config the protected interface setting
			wan2-wlan	<on|off>	Config the protected interface setting
			wlan -lan	<on|off>	Config the protected interface setting
			wlan -wan	<on|off>	Config the protected interface setting
			wlan -dmz	<on|off>	Config the protected interface setting
			wlan -wan2	<on|off>	Config the protected interface setting
			wlan -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
			lan-lan	<on|off>	Config the protected interface setting
			lan-wan	<on|off>	Config the protected interface setting
			lan-dmz	<on|off>	Config the protected interface setting
			lan-wan2	<on|off>	Config the protected interface setting
			lan-wlan	<on|off>	Config the protected interface setting
			wan -lan	<on|off>	Config the protected interface setting
			wan -wan	<on|off>	Config the protected interface setting
			wan -dmz	<on|off>	Config the protected interface setting
			wan -wan2	<on|off>	Config the protected interface setting
			wan -wlan	<on|off>	Config the protected interface setting
			dmz -lan	<on|off>	Config the protected interface setting

			dmz -wan	<on|off>	Config the protected interface setting
			dmz -dmz	<on|off>	Config the protected interface setting
			dmz -wan2	<on|off>	Config the protected interface setting
			dmz -wlan	<on|off>	Config the protected interface setting
			wan2 -lan	<on|off>	Config the protected interface setting
			wan2-wan	<on|off>	Config the protected interface setting
			wan2-dmz	<on|off>	Config the protected interface setting
			wan2-wan2	<on|off>	Config the protected interface setting
			wan2-wlan	<on|off>	Config the protected interface setting
			wlan -lan	<on|off>	Config the protected interface setting
			wlan -wan	<on|off>	Config the protected interface setting
			wlan -dmz	<on|off>	Config the protected interface setting
			wlan -wan2	<on|off>	Config the protected interface setting
			wlan -wlan	<on|off>	Config the protected interface setting
	save				Save the anti-virus setting
	clean				Clean all the AV matrix configurations.
	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
		displayMinute			Display the current update minute setting
		configMinute	[00-59]		Config the current update minute 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
	commonDebug				The debug command for IDP/Anti-Virus/Anti-Spam
		display			Show the debug setting for IDP/Anti-Virus/Anti-Spam
		Tos	<on|off>		Set the tos debug flag for IDP/Anti-Virus/Anti-Spam
		ipfrag	<on|off>		Set the ipfrag flag for IDP/Anti-Virus/Anti-Spam
		tcpasm	<on|off>		Set the tcpasm debug flag for IDP/Anti-Virus/Anti-Spam
		tcpprocess	<on|off>		Set the tcpprocess debug flag for IDP/Anti-Virus/Anti-Spam
		l7process	<on|off>		Set the l7process debug flag for IDP/Anti-Virus/Anti-Spam
		autoupdate	<on|off>		Set the autoupdate debug flag for the IDP/Anti-Virus signature autoupdate
		reengine	<on|off>		Set the reengine debug flag for the

					IDP/Anti-Virus SW/HW search engine
		bwengine	<on|off>		Set the bwengine debug flag for IDP backend process
		reLibDbg	<on|off>		Set the reLibDbg debug flag for the Lionic resoft library
		showIaCb			Show the runtime debug information for IDP/Anti-Virus
		showMemUseInfo			Show the memory usage information for IDP/Anti-Virus
	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
	listFullRef				List the virus reference table of the full version signature
	listDeltaRef				List the virus reference table of the delta version signature
	debug				The debug flag for the anti-virus
		display			Display the debug flag setting
		smtppop3	<on|off>		The debug flag for the SMTP/POP3 attachment process
		ftpdata	<on|off>		The debug flag for the FTPDATA process
		http	<on|off>		The debug flag for the HTTP process
		decompress	<on|off>		The debug flag for the decompress on the fly
		maildecode	<on|off>		The debug flag for the uuencode/base64 decode process
		mailinsertion	<on|off>		The debug flag for the mail text insertion process
	zipUnsupport	[0/1]			0: Pass through 1: Destroy

Anti-Spam Command

Home

Command					Description
as					Anti-Spam CI commands
	asAction	[0|1]			Forward/Block exceeding mails sessions.
	cleanServerList	[index | all]			Delete one or all rating servers from the server list.
	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.
		runtimedata	<all|black|white>	[all|ip|mime|email|subject]	Display runtime data for anti-spam ACL structure.
	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.
	fill				Fill the white/black list.
		blackRule			Fill the black list.
			ip	<start IP address>	Fill the black list with IP filter.
			email		Fill the black list with Email filter.
			mime		Fill the black list with MIME filter.
		blackRule			Fill the white list.
			ip	<start IP	Fill the white list with IP filter.

				address>	
			email		Fill the white list with Email filter.
			mime		Fill the white list with MIME filter.
	freeSession				Free all mail ssessions.
	getServerList	<Y:Yes|N:No>			Send server list request manually.
	dir	<lan|wan1|dmz|wan2|wlan>	<lan|wan1|dmz|wan2|wlan>	<on|off>	Enable or disable on direction of Anti Spam
	scoreTimeout	<timeout value>			Set the AS score query timeout value.
	xtag	<tag><content>			Set xtag and content

Wireless Related Command

Home

Command				Description
wlan				
	active		<1:on| 0:off>	Active the wireless card
	association			Show Association List
	chid		<RF Channel ID>	Set the RF Channel ID
	essid		<ESSID>	Set the wireless AP SSID
	fraThreshold		<256~2346>	Set the fragmentation threshold
	iapp			Show the IAPP information
	outputpower		<0..4>	Set the output power level
	radio		<1:B | 2:G | 3:B+G | 4:A>	Set the wireless radio mode
	rtsThreshold		<256~2346>	Set the RTS/CTS threshold
	removeSTA		<MAC address>	Remove the station
	reset			Reset wireless module
	scan			Scan environment and get a recommand RF channel
	ssidprofile			
		set	<SSID Profile name1> [SSID Profile name2] …	Enable the SSID Profile
		show		Show current active SSID
	version			Show wireless driver version
	showBandInfo			Show current band information
	counter			Show driver's statistics
	sptShow			Show SPT configuration
	displaySetting			Show runtime setting
	displayStats			Show device and driver status
	packet		[DA MAC] [size] [number] [interval] [DSCP] [DA UDP Port] [Chan ID]	Create testing packet to send

	level		[Debug level]	Set the debug level
	qscanSet			Set which device to scan
	qscanGet			Get SSID in this environment
	magicProfile			Set the profile to specified configuration.
	qsetmacf		[action] [No. N] [MAC Addr]	Set the MAC filter record.
	superset		<VAP> <FF> <CB>	Enable Atheros super mode flag.
	rfdiv		<1:on | 0:off>	Enable/Disable diversity
wcfg				
	ssid	[1...8]		
			name <name>	Set profile name
			ssid <ssid>	Set profile SSID
			hidenssid <enable | disable>	Enable/Disable Hide SSID
			security <security profile name>	Link to which security profile.
			macfilter <enable | disable>	Enable/Disable MAC Filter function
			clear	Set the profile to default value
			save	Save this profile configuration
			show	Show this profile configuration
		display		Display runtime ssid profile buffer
		spdisplay		Display all ssid SPD configuration
		saveall		Save all runtime ssid buffer to SPD.
	security	[1...8]		
			name <name>	Set profile name
			mode <none | wep | 8021x-only | 8021x-static64 | 8021x-static128 | wpa | wpapsk | wpa2 | wpa2mix | wpa2psk | wpa2pskmix	Set the security mode.
			wep keysize [64 | 128 | 152] [ascii | hex]	Set the WEP key length
			wep auth [shared | auto]	Set the WEP authentication
			wep key1 <key>	Set the WEP key1
			wep key2 <key>	Set the WEP key2
			wep key3 <key>	Set the WEP key3
			wep key4 <key>	Set the WEP key4
			wep keyindex	Set the default WEP key
			reauthtime [value]	Timer for key re-authentication
			idletime [value]	Idle time before force de-association
			groupkeytime [value]	Time for group key update
			passphrase [value]	Set passphrase for security mode wpapsk, wpa2psk, and wpa2pskmix. Length is 8~63
			clear	Set the profile to default value
			save	Save this profile configuration
			show	Show this profile configuration
		display		Display runtime security profile buffer
		spdisplay		Display all security SPD configuration
		saveall		Save all runtime security buffer to SPD.