ZyXEL

Firmware Release Note

ZyWALL P1

Release 3.64(XJ.4)

Date:	**Aug., 09, 2005**
Author:	**Nash Fan**
Project Leader:	**Tim Tseng**

ZyXEL ZyWALL P1 Standard Version
Release 3.64(XJ.4)
Release Note

Date: Aug. 09, 2005

Supported Platforms:

ZyXEL ZyWALL P1

Versions:

ZyNOS Version: V3.64(XJ.4) | 08/09/2005 09:06:56
BootBase : V1.03 | 05/06/2005

Notes:

1. **Restore to Factory Defaults Setting Requirement: No.**
2. **The setting of ignore triangle route is on in default ROM FILE. Triangle route network topology has potential security crisis. If you are not clear about it, please refer to Appendix for the triangle route issue.**
3. **IKE process in phase 2 will check ID information between system and the peer. If you found that the IPSec connection is failed, please check your settings.**
4. **When firewall turns from "off" to "on", the firewall initialization procedure will disconnect all connections running through the ZyWALL.**
5. **SUA/NAT address loopback feature was enabled on ZyWALL by default, however, if users do not need it, a C/I command "ip nat loopback off" could turn it off.**
6. **When UPnP is on, and then reboot the router, Windows XP will not detect UPnP and refresh "My Network Places→Local Network". Plug in network wire again can solve this problem.**
7. **The default max NAT session number per host is 256.**
8. **If you were using MSN Messenger Voice Communication through ZyWALL UPnP and found voice is blocked by firewall,**
   we suggest you download MSN Messenger 7.0 and try again. This is because we found MSN Messenger 6.2 sometimes fails to
   detect UPnP status when it's starting voice invitation.
9. **In previous 3.64 firmware, the VID value of DPD is not correct. VID change will cause current version doesn't work with the wrong value. Please be sure to connect with devices which has updated VID, or the DPD may not work correctly.**
10. **The default LAN IP and DHCP Client Address are 192.168.167.1 and 192.168.167.33.**

Known Issues:

1. **Sometimes on screen the "Local Area Connection" icon for UPnP disappears. The icon shows again when restarting PC.**
2. **When you use MSN messenger, sometimes you fail to open special applications, such as whiteboard, file transfer and video etc. You have to wait more than 3 minutes and retry these applications.**
3. **System may need to reboot when change the SNMP port number.**
4. **CNM agent has not supported to register to Vantage yet.**

Features:

Modifications in V 3.64(XJ.4) | 08/09/2005
Modify for formal release

Modifications in V3.64(XJ.4)b1 | 08/04/2005

1. [BUG FIX]
   Symptom: Send log mail is very slow.
   Condition:
   1. In "eWC->LOGS->Let Settings", set "E-mail log Settings".
   2. In "eWC->LOGS->View Log", click "Email Log Now".
   3. The mail will be sent after 1~2 minutes. It's too slow.
2. [BUG FIX]
   Symptom: The device shows the "SMTP fail" log continuously.
   Condition:
   1. Enable "System Errors" log and alert mail.
   2. Input an invalid site in Mail Server of Log Settings.
   3. Fill other mail related fields of Log Settings.
   4. The system will generate the "SMTP fail (Cannot connect to SMTP server ...)" continuously.
3. [BUG FIX]
   Symptom: VPN tunnel cannot be built if the reveived IKE packet is fragmented.
   Condition:
   (1) Set IKE rule which authentication key is certificate with 2048 bit key length.
   (2) Set encryption algorithm of the IKE rule as AES.
   (3) Set the ipsec rule.
   (4) Set a environment which will fragment the IKE packet.
   (5) Dial the tunnel.
   (6) The tunnel cannot be built.
4. [BUG FIX] 050601011
   Symptom: VPN tunnel can be built up without authentication, which configures authentication by router.
   Condition:
   1. Configure a VPN IKE rule, authenticatin use router.
   2. And Configure a IPSEC rule, choose Nail-up.
   3. The Tunnel will be built up automatically without authentication. It is wrong.

Modifications in V 3.64(XJ.3) | 07/01/2005
Modify for formal release

Modifications in V3.64(XJ.3)b1 | 06/16/2005
1. [BUG FIX]
Symptom: Router crash.
Condition:
(1) Use router for a long time.
(2) Sometimes Router will crash and the console shows
"Common TOS: Free queue session number > max session number..
\tos.c:960 sysreset()".
2. [BUG FIX]
Symptom: IPSec input idle timer does not work correctly.
Condition:
Topology:
PC1-ZWA--Intranet--ZWB-PC2
Add normal VPN rule in both side.
(1) In ZWB, set "Input Idle Timeout" as "30" seconds.
(2) Dial the tunnel up, there is no traffic in the tunnel.
(3) In ZWB, SMT 24.8, type "ipsec sho sa", the "input idle count" in "INBOUND" will be decreasing, it works correctly.
(4) Now, In PC1, ping PC2 from PC1 with one packet then stop the traffic in the tunnel.
(5) In ZWB, SMT 24.8, type "ipsec sho sa", the "input idle count" in "INBOUND" stay unchanged.
(6) The input idle timeout mechanism will not work anymore.
3. [BUG FIX]
Symptom: Output idle timer doesn't work correctly.
Condition:
PC1--(L)ZWP1(W)--Intranet--(W)Router(L)--PC2
(1) ZWP1 and Router had established VPN tunnel.
(2) Output idle timer=120 secs, input idle timer=30 secs.
(3) Unplug the WAN link of Router, make a ICMP echo request to PC2 from PC1.
(4) ZWP1 doesn't send out "are u there" packets to peer gateway after 120 seconds.

Modifications in V 3.64(XJ.2) | 06/08/2005
Modify for formal release

Modifications in V 3.64(XJ.2)b2 | 05/31/2005
1. [BUG FIX]
Symptom: VPN Authenticated By None can't be trigger dial.
Condition:
PC A -- ZWP1 ---- PQA --- ZW70 -- PC B
1. In eWC add VPN rule, in IKE rule Authenticated By select "None" and make sure this rule can be build up
2. Use Dos command "ping 192.168.1.33"(PC B IP), tunnel should be up, but it not.
2. [BUG FIX]

Symptom: VPN Authenticated By None still need input username and password.
Condition:
PC A -- ZWP1 ---- PQA --- ZW70 -- PC B
1. In eWC add VPN rule, in IKE rule Authenticated By select "None".
2. Logout GUI, and at VPN page, dial it, it still want user input username and password.

Modifications in V 3.64(XJ.2)b1 | 05/25/2005

1. [BUG FIX] 050502014
Symptom: Modification to exisiting WANtoWAN rule (with IKE and BOOTP) can not work
Condition:
In the example, use SSH
1) Change SSH port to 2222 in Remote MGMT.
2) Go to WAN to WAN / ZyWALL and create a custom service, TCP/UP 2222.
3) Add the rule in the default rule that has IKE and Bootp.
4) Try to connect with Putty or other prefered SSH client. It doesn't work
5) Now add the standard SSH (or any other predefined TCP rule) service to the same firewall rule. It works.
2. [BUG FIX] 050502038
Symptom: Daylight Saving problem: Current Time is faster 2 hours than Taiwan during daylight saving.
Condition:
1. Restore default romfile.
2. Go to eWC->Maintenance->TimeAndDate.
and the problem happened only when
3. Apply the "Time Zone" = "(GMT+08:00)", activate "Enable Daylight Saving" and set the date range include the current time.
4. Click the "Apply" button and the page will be refreshed.
5. The current time is faster 2 hours than Taiwan, it should be faster 1 hour only.
3. [BUG FIX]
Symptom: Router crash.
Condition:
(1) Turn on firewall.
(2) Sometimes router will crash when suffer attack.
4. [BUG FIX] 050311673
Symptom: When the VPN tunnel did not receive packet for sometime, the log is unclear.
Condition:
Topology:
PCA(192.168.167.33)---ZWP1--- (VPN) --- ZW5---PCB(192.168.1.33)
1. For ZWP1, set output timer and input timer in VPN global setting.
2. Add a IKE rule, and IPSec policy for ZW5, PCB.
3. Configure ZW5, add a IKE rule, and IPSEC policy for ZWP1, PCA.
4. Build this tunnel, do not send packet through this tunnel.
5. After last sending packet for output time, ZW5 do not receive packet, it will

send R_U_THERE packet to ZWP1, but ZWP1 log shows NOTFY:UNKNOW(36136) and NOTFY:UNKNOW(36137), this message is unclear.

6. After last receiving packet for input timer, ZW5 do not receive packet, the same situation will happen.

5. [BUG FIX] 050505207
   Symptom: Resynchronize in Time Setting page does not work.
   Condition:
   1. restore default romfile
   2. login eWC and enter Time setting page.
   3. after 1 day, there is no time resynchronization log.
6. [FEATURE CHANGE]
   When edit a firewall rule, the source IP and destination IP rule numbers are limited to 20.
7. [FEATURE CHANGE]
   At the beginning of router restart, the pingcheck is disabled.

8. [ENHANCEMENT]
   VPN authentication type add None for without authentication.

Modifications in V 3.64(XJ.1) | 05/12/2005
Modify for formal release

Modifications in V 3.64(XJ.1) b1 | 05/06/2005
1. [EHNANCEMENT]
   Add IP information for my IP address and Secure Gateway address. In CI command, "ipsec ikeDisp #" will show IKE rule configuration. When my IP address or secure gateway address is domain name, the resolved IP will show after domain name.
2. [BUG FIX]
   Symptom When users remotely manage the ZyWALL via a PPTP connection, a strange firewall session (between PPTP server and PPTP client) timeout log may be observed.
   Condition:
   (1) Configure the ZyWALL's WAN port to use PPTP encapsulation.
   (2) Remotely login eWC (http/https) via the PPTP connection.
   (3) After a few minutes, check the centralized logs or syslogs, you will observe a sequence of firewall logs of http/https session timeout.
3. [BUG FIX] 050214272
   Symptom: For firewall ACL schedule, if two rules have the same policies except "schedule", only the first rule will work.
   Condition:
   (1) Set two firewall rules have same policies except schedule.
   (2) Only the first rule will work.
4. [BUG FIX]
   Symptom: Netbios packet cannot pass through VPN tunnel .
   Condition:
   (1) Configure a VPN tunnel as follows:
      1.1 local subnet mask is 192.168.1.1/255.255.0.0.
      1.2 remote subnet mask is 192.169.1.1/255.255.0.0.

1.3 Enable ”Netbois pass through” in local and remote gateway.

1.4 PC A(Local)------ZyWALLA------ZyWALLB---PC B(Remote)192.168.1.1/16 192.169.1.1/16

(2) Establish the VPN tunnel.

(3) In PC A, Search PC B’s computer name.

(4) PC A will send a broadcast packet to search PC B.

(5) ZyWALL A will change destination IP address from 192.168.255.255 to 192.169.255.255 and send to ZyWALL B after encryption. Horever, ZyWALL A should adjust the UDP checksum but it didn’t.

(6) PCB will drop the received broadcast UDP pcket from PC A due to error UDP checksum.

5. [BUG FIX] 050214274
   Symptom: VPN My IP Addr will resolving fail
   Condition:
   (1) Add a VPN rule and My IP Address and Remote Gateway Address are domain type.
   (2) Click Dial button, it will fail to build tunnel first time (second time is ok)
   (3) Check log will display “Cannot resolve My IP Addr for rule xxx”
6. [BUG FIX]
   Symptom: Max. Concurrent Sessions Per Host problem.
   Condition:
   (1) In eWC->NAT , change Max. Concurrent Sessions Per Host to 300
   (2) Use ipscan tool to make session
   (3) Log show “192.168.1.33 exceeds the max. number of session per host! “ when exceeds the max. number of session per host, but Max. Concurrent Sessions Per Host (Historical high since last startup: 286) ,it’s not reach 300
7. [BUG FIX] 050301066
   Symptom: Remote gateway Address can’t configure as domain type when ipsec Nail-Up option is on.
   Condition:
   (1) Add a VPN rule(Static rule) with Remote gateway Address set as domain type.
   (2) In Ipsec rule, enable Nail-Up option.
   (3) Return to IKE rule page, change some fields and click Apply. The Status will show “This ipsec rule bounds to dynamic IKE rule. Please inactive nail up.” and it can’t be saved.
8. [BUG FIX]
   Symptom: Router crash when recieve UDP packets which comes from TfGen.
   Condition:
   (1) Restore default rom file.
   (2) In WAN side, place a PC and open TfGen tool to send packets to router's WAN.
   (3) The TfGen's setting in my PC is: Ultilization: 4kbps, Destion: 192.168.70.34, Port: 500.
9. [BUG FIX]
   Symptom: DNS inverse query causes system crash.
   Condition:
   (1) Set A PC on the device LAN site.
   (2) The DNS server of the PC sets to the device.
   (3) The PC sends DNS inverse query continually, the device will crash sometimes.
10. [BUG FIX]
    Symptom: DDNS update failed
    (1) dial PPPoE and obtain dynamic IP

(2) configure DDNS and make sure DDNS name is updated with new dynamic IP
(3) turn on “sys ddns debug 1”
(4) use scheduler to force down interface for 1 min.
(5) re-dial PPPoE (nail-up) and obtain dynamic IP
(6) saw the DDNS debug log showed failed message.

11. [BUG FIX]
    Symptom: Responder receive duplicate package when VPN tunnel established
    Condition:
    (1) At Initiator edit one VPN rule and Extended Authentication=enable=client mode
    (2) At responder edit one VPN rule and Extended Authentication=enable=server mode
    (3) when VPN tunnel established ,Responder log show “Rule[IKE1] receives duplicate packet”
12. [BUG FIX] 050304284
    Symptom: There is no log for replay packets
    Condition:
    (1) Enable ”Anti-Replay” function.
    (2) Sniffer an ESP packet and replay it.
    (3) This ESP packet will be dropped by there is no log.
    (4) There should be log to show this action.
13. [BUG FIX]
    Symptom: DNS inverse query causes memory leak.
    Condition:
    (1) Set A PC on the ZyWALL LAN site.
    (2) The DNS server of the PC sets to the ZyWALL.
    (3) The PC sends DNS inverse query continually (ex: 140.113.23.1), the system will generate memory leak.
14. [BUG FIX]
    Symptom: "Gateway Domain Name Update Timer" in eWC --> VPN --> Global Setting didn't work.
    Condition:
    (1) Set one IKE rule which secured gateway address is domain name.
    (2) Set "Gateway Domain Name Update Timer" to 15 minutes and apply.
    (3) System will not update secured gateway domain name according to the setting unless system reboot.
15. [BUG FIX]
    Symptom: Resolving a domain name which start with number (for example 4youcard.com) will fail.
    Condition: CI command "ip ping 4youcard.com" and it will fail.
16. [BUG FIX]
    Symptom: Router will crash when receive an unrecognizable DNS response
    Condition:
    Environment:
    PC(192.168.1.33)-----(192.168.1.1)ZW70---Internet
    (1) Set ZW70's system DNS server as "164.67.128.1"
    (2) From PC, send a DNS query to ZW70. The DNS format is as following:
    cf 07 01 00 00 01 00 00 00 00 00 00 04 75 63 6c
    61 03 65 64 75 00 00 ff 00 01
    (3) ZW70 will relay the DNS query to "164.67.128.1".

(4) ZW70 will crash after receive DNS response from "164.67.128.1"

17. [BUG FIX]
    Symptom: VPN tunnel can't be up with dynamic rule.
    Condition:
    Initiator: One IKE with one policy. And in policy, local ID type = Subnet. Dest ID type = Subnet.
    Responder: One dynamic IKE with two policies:
    (1) Policy 1: Encryption is wrong. Local ID type = Subnet. Local starting IP Address is wrong
    (2) Policy 2: All settigs are correct.
18. [BUG FIX]
    Symptom: Modification to exisiting WANtoWAN rule (with IKE and BOOTP) can not work
    Condition:
    In the example, use SSH
    (1) Change SSH port to 2222 in Remote MGMT.
    (2) Go to WAN to WAN / ZyWALL and create a custom service, TCP/UP 2222.
    (3) Add the rule in the default rule that has IKE and Bootp. <===
    (4) Try to connect with Putty or other prefered SSH client. ===> doesn't work
    (5) Now add the standard SSH (or any other predefined TCP rule) service to the same firewall rule. It to work

Modifications in V 3.64(XJ.0) C0 | 02/21/2005
Modify for formal release

Modifications in V 3.64(XJ.0) b6 | 02/16/2005

1. **[BUG FIX] 050214276**
   Symptom: VPN lack of Nail-Up option
   Condition:
   (1) ZWP1 lacks Nail-Up option In eWC>VPN>Network policy>Edit.

2. **[BUG FIX] 050214273**
   Symptom: Firewall can't pull Any(ICMP) from Available Service to Selected Service
   Condition:
   (1) Add a Firewall ACL rule.
   (2) Select service Any (ICMP) and click >> button. You will see that "Any (ICMP)" can't be moved to Selected Service

Modifications in V 3.64(XJ.0) b5 | 02/03/2005

3. **[BUG FIX] 050201025**
   Symptom: H323 voice will be block
   Condition:
   PC A – ZWP1 A – ZWP1 B – PC B
   (3) Enable ALG_H323, add firewall rule W to L forward H323 1720 port, and NAT port fording to PC A and B
   (4) Use OpenH323 application tool
   (5) PC A call PC B, then PC B can't receive voice. PC A is ok
   (6) PC B call PC A, then PC A can't receive voice. PC B is ok
4. **[BUG FIX] 050201026**

Symptom : Help page description error
Condition:
(1) On eWC LAN/LAN, help page should not mention “Relay”

5. **[BUG FIX] 050201028**
   Symptom : Change ISP after first time get IP, traffic can’t go out
   Condition:
   (1) Device reset default rom file
   (2) Change WAN ISP from Ethernet to PPPoE /PPTP, and after first get IP, all traffic can’t go out until system reboot.
   (3) Even use Ethernet, dynamic change to static IP, all traffic can’t go out.
6. **[BUG FIX] 050201029**
   Symptom: DHCP client does not follow RFC 2131
   Condition:
   (1) DHCP client does not follow RFC 2131 on rebinding request. According to RFC, it should be broadcast where our device is send unicast.
7. **[BUG FIX]**
   Symptom: DPD vendor ID is not correct.
   Condition:
   VID value of DPD is not compatible with RFC3706.
8. **[Feature Change]**
   WAS: The second datagram will use the last 8 octets of the first datagram as IV. This may cause IV "predictable".
   IS: All datagrams will use random IV to make IV unpredictable.
9. **[BUG FIX]**
   Symptom: Unplug the physical WAN link, the VPN tunnel should be deleted.
   Condition:
   (1) Go to eWC>VPN>VPN Rules (IKE) dial a VPN tunnel.
   (2) Unplug the physical WAN link, the VPN tunnel will be deleted after 10 secs.

Modifications in V 3.64(XJ.0) b4 | 01/31/2005

1. **[BUG FIX] 041214721**
   Symptom: Maintenance/Configuration description error
   Condition:
   (1) On eWC/Maintenance/Configuration/Back to Factory Defaults, LAN IP address should be 192.168.167.1 instead of 192.168.1.1
2. **[BUG FIX]**
   Symptom: The ZyWALL should synchronize with the timeservers after WAN link is up
   Condition:
   (2) Go to eWC>MAINTENANCE>Time and Date.
   (3) Set Time server address as ”a.ntp.alphazed.net” and save
   (4) Unplug the WAN from ZWP1 and reboot the ZyWALL. After rebooting, you can see a log the ”Failed to synchronize with NTP server: a.ntp.alphazed.net” but the WAN link is not up.
   (5) The ZyWALL should synchronize with the timeservers after WAN link is up.
3. **[BUG FIX]**
   Symptom: The new connected PC cannot get an IP from ZWP1.
   Condition:
   (1) Reboot the ZyWALL P1.
   (2) PC connects LAN port of ZWP1 and gets IP.
   (3) Unplug the cable of LAN of ZWP1.
   (4) Another PC connects LAN port of ZWP1 and gets IP.
   (5) The new connected PC cannot get dhcp client IP from ZWP1.
4. **[BUG FIX]**
   Symptom: Enter special url will cause device crash.
   Condition:
   (1) Form LAN site, enter http://192.168.167.1/Forms/rpAuth_1?ZyXEL%20ZyWALL%20Series<script>top.location.pathname=%20""</script> on browser, the device will crash.
5. **[BUG FIX]**
   Symptom: SIP P2002 voice communication failed.
   Condition:
   (1) P2002A-(L)ZWP1(W)----Internet(SIP server)---(W) ZWP1 (L)----P2002 B
   (2) Both ZyWALL reset to default romfile.
   (3) Using CI command, both type “ip alg enable ALG_SIP” to enable SIP ALG.
   (4) P2002 A make a phone call to P2002 B, voice communication works fine.
   (5) Terminate the phone call,then P2002 B make a phone call to P2002 A, voice communication fail. Fail status: P2002 A can hear voice, but P2002 B can't.
6. **[BUG FIX]**
   Symptom: When user unplugs PC A from the LAN of ZWP1, the tunnel cannot be deleted.
   Condition:
   (1) Build a VPN tunnel PC A--(L)ZWP1 A(W)--(W)ZWP1 B(L)-- PC B.
   (2) Unplug a PC A from the LAN of ZWP1.
   (3) ZWP1 should delete the tunnel.
7. **[Feature Change]**
   Change default romfile setting value for IPSec timers:

Output Idle Timer = 120 (sec)
Input Idle Timer = 0 (sec)
Gateway Domain Name Update Timer = 5 (min)

Modifications in V 3.64(XJ.0) b3 | 01/25/2005

10. [BUG FIX] 041214721
Symptom: Use IXIA create session cause ZWP1 crash
Condition:
(1) Use IXIA to create 2048 sessions and run about 1 minute, device crashes.

11. [Enhancement] 041214722
Anti-Probing default setting should be LAN&WAN

12. [BUG FIX] 041214723
Symptom: LAN description does not match
Condition:
(1) On eWC>LAN>LAN, "IP Address" is 192.168.2.1, "IP Subnet Mask" is 255.255.255.254, "DHCP" is Server, "DHCP Client Address" is 192.168.2.2.
(2) Status will show "Invalid DHCP starting Address", it should show "Invalid DHCP Client Address"

13. [ENHANCEMENT] 041214724
Cache the data in eWC>LAN when users change the options in "DNS Servers Assigned by DHCP Server".

14. [Enhancement] 041214726
Adjust Max. Concurrent Sessions Per Host to 256

15. [ENHANCEMENT] 041217862
Add ”Authentication For Activating VPN” related fields on VPN wizard

16. [ENHANCEMENT] 041217863
Add an active checkbox for ipsec rule on VPN wizard.

17. [BUG FIX] 041221074
Symptom: Configure WAN page, and WAN priority will become 1
Condition:
(1) In "eWC>WAN>General", set WAN1 priority to 5.
(2) In "eWC>WAN>WAN", set encapsulation type to PPTP or PPPoE.
(3) Go to "eWC>WAN>General", WAN's priority will become 1.

18. [BUG FIX] 041224260
Symptom: The device uploads files from ftp server is very slow with PPTP connection.
Condition:
(1) Set WAN encapsulation is PPTP.
(2) Set the WAN bandwidth is about 1M bits.
(3) Upload files from LAN to WAN.
(4) The upload speed is very slow and the connection will be dropped by timeout after some minutes.

19. [BUG FIX] 041227307
Symptom: After 48 hours, VPN stress test with FTP is crashed.
Condition:
(1) Create a VPN rule with DES encryption
(2) Do VPN stress test with FTP
(3) After 48 hours, device crashes.

20. [BUG FIX] 041227310

Symptom: Enhance the VPN error description.

Condition:

(1) On eWC VPN, add a IKE rule Dynamic rule (Remote Gateway Address is 0.0.0.0)

(2) Add a Ipsec rule, and fill some value instead of 0.0.0.0 in "Remote Network" fields.

(3) Status will show "This policy cannot bound to the dynamic rule"

(4) User may not know where is wrong.

21. [BUG FIX] 041227311

Symptom: eWC/VPN/Global Setting/Gateway Domain Name Update Timer does not work appropriately

Condition:

(1) Set eWC/VPN/Global Setting/Gateway Domain Name Update Timer=1
IKE do not update gateway domain name every 1 minute

22. [BUG FIX]

Symptom: Enter special url will cause device crash.

Condition:

(6) Form LAN site, enter http://192.168.1.1/Forms/rpAuth_1?ZyXEL%20ZyWALL%20Series<script>top.location.pathname=%20""</script> on browser, the device will crash.

23. [FEATURE CHANGE]

Enhance Gateway Domain Name Update Timer.
If 'Gateway Domain Name Update Timer' is enabled.
The ZyWALL will resolve the IP from a VPN gateway policy whose IKE remote gateway is domain name type in every cycle. If the ZyWALL finds that the new remote gateway IP is different from the old one (which is used by tunnel now), the ZyWALL will delete this tunnel.

24. [BUG FIX]

Symptom: Save a legal VPN gateway policy but the ZyWALL shows an error message

Condition:

(1) GO to eWC>VPN>GATEWAY POLICY – EDIT

(2) Save a GATEWAY POLICY whose
name = GW, My Address = www.abc.com.tw, Remote Gateway Address = www.cde.com.tw
and Pre-Shared Key = 12345678

(3) GO to eWC>VPN>NETWORK POLICY – EDIT

(4) Save a NETWORK POLICY whose
name = NW, Active = Yes, Starting IP Address = 192.168.1.33, Starting IP Address = 192.168.2.33
and Pre-Shared Key = 12345678

(5) Go back to eWC>VPN>Rules and edit rule "GW" and set its My Address as 0.0.0.0, then save

(6) The ZyWALL shows a error message "This IKE rule has static policy rules.", but it should not.

25. [BUG FIX]

Symptom: The centralized log shows the strange DHCP entry with hex IP address.

Condition:

(1) The device enables LAN DHCP server.

(2) A PC is set on device LAN site with dynamic IP and no system hostname.
(3) The PC sends DHCP request to device.
(4) The device will show the strange log message have the hex IP address. (Ex: 101 01/15/ 2005 10:15:50 DHCP server assigns 0xa0a01e6 to 00:0E:08:AA: B6:B3)

26. [BUG FIX]

Symptom: There are no logs in eWC>Logs>Log Settings when SMTP authentication fail
Condition:
(1) Go to eWC>Logs>Log Settings. Configure a wrong Mail Server/Send Log to/Send Alerts to/User Name of SMTP Authentication/Password of SMTP Authentication and save.
(2) Go to eWC>Logs>View Log. There are no logs about SMTP Auth failures/SMTP failures.
(3) If the configuration is correct. There is also no log to tell users that the result is successful.

27. [BUG FIX]

Symptom: WAN Link up is before sync with Time server.
Condition:
(1) Go to eWC>MAINTENANCE>Time and Date.
(2) Set Time server address as ”a.ntp.alphazed.net” and save.
(3) Reboot the ZyWALL. After rebooting, you can see a log the ”Failed to synchronize with NTP server: a.ntp.alphazed.net” which is before the log ”WAN connection is up in eWC>Logs>View Log”
(4) The ZyWALL should synchronize with the time servers after WAN link is up

28. [ENHANCMENT]

Add IKE and IPSec logs for ICSA certificate.
(1) There will be log when PSK mismatches.
(2) When IPSec packet authentication fails, there will be a log.
(3) When system receives a repeated packet, there will be a log.

29. [BUG FIX]

Symptom: ID mismatch while using subject name as ID
Condition:
(1) Use certification as authentication method.
(2) Set phase 1 ID as subject name
(3) During IKE negotiation, its.

30. [ENHANCEMENT]

(1) Add the switch of NAT AOL alg.
(2) CI command: "ip nat service aol [on|off]"

31. [BUG FIX]

Symptom: PPTP static IP pop-up mask "My IP Subnet Mask" is wrong
Condition:
(1) Go to eWC>WAN>WAN1.
(2) Set encapsulation type as PPTP.
(3) Key-in My IP Address as 192.168.65.54.
(4) "My IP Subnet Mask" will pop up 255.0.0.0, it is wrong, it should be 255.255.255.0.

32. [BUG FIX] 050112805

Symptom: VPN tunnel can be established but traffic cannot go through tunnel.
Condition:

(1) PC1 -- ZyWALL -- Any Router/Internet -- ZyWALL -- PC2
(2) Configure corresponding VPN setting in both ZyWALLs.
(3) Dial VPN tunnel
(4) After tunnel established, PC1 cannot ping PC2 vice versa.

33. [FEATURE CHANGE]

Enhance Gateway Domain Name Update Timer.
If Gateway Domain Name Update Timer is enabled.
The ZyWALL will resolve the IP from a VPN gateway policy whose IKE remote gateway is domain name type in every cycles. If the ZyWALL finds that the new remote gateway IP is different from the old one(which is used by tunnel now), the ZyWALL will delete this tunnel..

34. [ENHANCEMENT]

Add port information in centralized log message when a NetBIOS packet was blocked

35. [FEATURE CHANGE]

WAS: As a responder, device will not initiate phase 2 SA with peer even it has traffic to pass tunnel.
IS: Device will initiate phase 2 SA if it has traffic to pass tunnel. NOTE: Reproduce procedure is as followed:
(1) The tunnel has been created and device's LAN side PC still ping other side pc via the VPN tunnel.
(2) Reboot peer VPN gateway and device doesn't know peer has rebooted.
(3) After peer gateway start up, it still receives ESP packet from device.
(4) Peer gateway will create phase one IKE with device successful and then send IC notification in an independent information packet to device.
(5) However after the IC packet, the peer gateway stops to send quick mode packets because it has no traffic to transmit.
(6) Device has traffic to transmit so it will start send quick mode and build up the tunnel.

36. [ENHANCEMENT]

Add SIP protocol in service list in firewall rule edit page.

37. [BUG FIX]

Symptom: We must repeat the dialing twice for building VPN up when using NAT-T.
Condition: Topology
PC1-(LAN)ZWP1_1(WAN)=(WAN)ZW5_NAT_Router(LAN)-(WAN) ZWP1_2(LAN) - PC2
(1) In ZWP1-1, we created one IKE with two IPSec rules, and it has the same destination and NAT-T on.
(2) In ZWP1-2, we created one IKE with two IPSec rules to correspond with ZWP1-1.
(3) Dial the first tunnel up, then dial the other tunnel and it will be failed.
(4) Dial the tunnel that just failed again, it will success.

38. [FEATURE CHANGE]

Phase 1 SA process changed for Initial Contact payload.
WAS: After receiving an Initial Contact payload, phase 2 SA will be deleted immediately, but phase 1 SA will remain for a certain interval.
IS: After receiving an Initial Contact payload, both phase 2 SA and phase 1 SA will be deleted immediately.

39. [BUG FIX]

Symptom: The new connected PC cannot get an IP from ZWP1.

Condition:
1. Reboot the ZyWALL P1.
2. PC connects LAN port of ZWP1 and gets IP.
3. Unplug the cable of LAN of ZWP1.
4. Another PC connects LAN port of ZWP1 and gets IP.
5. The new connected PC cannot get dhcp client IP from ZWP1.

40. [BUG FIX]
Symptom: There are no logs in eWC>Logs>Log Settings when SMTP authentication fail.
Condition:
(1) Go to eWC>Logs>Log Settings. Configure a wrong Mail Server/Send Log to/Send Alerts to/ User Name of SMTP Authentication/Password of SMTP Authentication and save.
(2) Go to eWC>Logs>View Log. There are no logs about SMTP Auth failures/SMTP failures.
(3) If the configuration is correct. There is also no log to tell users that the result is successful.

41. [FEATURE CHANGE]
WAS: As a responder, device cannot create tunnel with Eicon and Sidewinder successfully when the requests are from peer at the same time.

IS: In same phase1 (SA), device won't handle two phase2 rule packets at the same time. One tunnel will be established and the other one has to wait until the earlier one finish quick mode.

NOTE: Reproduce procedure is as followed:

(1) Both systems are set-up with 2 subnets referred to as rule1
(2) and rule2.
(3) Both rule1 and rule2 use the same Phase 1 setting.
(4) Tunnels can be established from ZW35 for both subnets with no problems.
(5) Tunnels established from Eicon or Sidewinder side at the same Time will fail.
(6) The log on ZyWALL will show "[HASH]: Rule [rule name] Phase-2 hash mismatch". Console logging shows "Quick Mode processing failed".

42. [ENHANCEMENT]
Remove clear log button in eWC>Basic Mode>Logs>View Log

43. [FEATURE CHANGE]
Set ipsec swIgnoreOverlapIp is off by default

44. [ENHANCEMENT] 040924953
Symptom: The PPTP connection between a ZyXEL router and a Thomson SpeedTouch DSL modem may be reset after the ZyXEL router transmits a _large_quantity_ of packets.
Condition:
(1) Connect a ZyXEL router to a Thomson SpeedTouch DSL modem.
(2) Configure the router to establish a PPTP connection to the modem.

(3) Have the router transmit a _large_quantity_ of packets via the modem.

(4) Check for any sign of PPTP disconnection. (The PPTP connection suffers a risk of drop for around every 65536 packets transmitted by the router.)

45. [ENHANCEMENT]

Change the default LAN IP to 169.254.1.1 and DHCP Client Address to 169.254.1.33 for ZyWALL P1.

46. [ENHANCEMENT]

Add a log "The DHCP-assigned LAN IP X.X.X.X is in conflict with the WAN subnet."

Note: The log is consolidated by the two conflict interfaces and the assigned IP.

47. [BUG FIX]

Symptom: SIP WiFi-Phone's voice communication failed.

Condition:

(4) Use fellowing topology to test. P2002 A-(L)ZWP1(W)----Internet(SIP server)---(W) ZWP1 (L)---- P2002

(5) Both zywall reset to default romfile.

(6) Using CI command, both type "ip alg enable ALG_SIP¨ to enable SIP ALG.

(7) P2002 A make a phone call to P2002 B, voice communication works fine.

(8) Terminate the phone call,then P2002 B make a phone call to P2002 A, voice communication fail. Fail status: P2002 A can hear voice, but P2002 B can't.

Modifications in V 3.64(XJ.0) b2 | 12/10/2004

1. **[BUG FIX]**
   Symptom: Dynamic DNS fail to update IP in special condition.
   Condition:
   (1) Restore default ROM file.
   (2) Edit one DDNS rule in Rule 2 (or 3-5)
   (3) WAN1's encapsulation is Ethernet; the router gets IP and DDNS updates successfully.
   (4) Change WAN1's encapsulation to PPPoE or PPTP, after the router gets IP successfully, the DDNS works exceptionally.
2. **[ENHANCEMENT]**
   When we receive a non-encrypt initial content payload in IKE, we will ignore it.
3. **[BUG FIX]**
   Symptom: Strings are be hided
   Condition:
   (1) Use CI command
   (2) ipsec ikeE 1
   (3) ipsec ikeC x user 01234567890123456789012345678 90
   (4) ipsec ikeC x pass 01234567890123456789012345678 90
   (5) ipsec ikeS
   (6) ipsec ikeD 1
   (7) We see the password is '01'
4. **[BUG FIX]**
   Symptom: VPN cannot work correctly when the router uses AES encryption and Key Length 192,256.
   Condition:
   (1) Create VPN tunnel by 2 ZyWALL P1, set the encryption algorithm with 'AES' and Encryption Key Length with '192' or '256'
   (2) The tunnel can be built up, but the traffic cannot pass through, the router will show 'IPSec ESP process failed'.
5. **[ENHANCEMENT]**
   There should be more information about the current NAT port usage for a specific WAN.
   CI command: ip nat natTable [iface]
6. **[BUG FIX]**
   Symptom: Go to eWC>WIZARD - Internet Access and click web help, the ZyWALL will show a invalid javascript pop up window Condition:
   (1) Go to eWC>WIZARD - Internet Access and click web help
   (2) The ZyWALL will show a invalid JavaScript pop up window
7. **[BUG FIX]**
   Symptom: Go to eWC>VPN>Activation. If there is no ipsec rule and clicks the 'apply' button, ZWP1 will show an error message "Read ipsec rule fail". It's not clear for user.
   Condition:
   (3) Go to eWC>VPN>Activation.
   (4) Make there is no ipsec rule in the ZWP1 and click the 'apply' button.
   (5) The ZWP1 will show a error message "Read ipsec rule fail".
8. **[ENHANCEMENT]**
   Modify DDNS client in the single is consistent with multiple wan DDNS client. So that each DDNS host will owns its update option, ex: wildcard, offline... separately.

9. [ENHANCEMENT]
Modify DNS GUI for single WAN.
10. [BUG FIX]
Symptom: The CI command "ipsec ipsecDisplay" shows the incorrect "Bound IKE" number.
Condition:
(6) Use CI command, type "ipsec ipsecAdd".
(7) "ipsec ipsecDisplay", a new created ipsec rule should have "9999" as it's "Bound IKE" number, but it shows "0".
11. [BUG FIX]
Symptom: The boundry check of CI command "ipsec ikeConfig myIpAddr" is wrong.
Condition:
(8) Use CI command, type "ipsec ikeAdd".
(9) "ipsec ikeConfig myIpAddr 12345678901234568790123456789012", this command will be accepted, the length of myIpAddr should be 31 (It's 31 in eWC).
12. [BUG FIX]
Symptom: The output of CI command "ipsec ipsecDisplay" should be re-layouted.
Condition:
(10) Add an ipsec rule "ipsec ipsecAdd", fill the name with "1234567890123456789012345678901".
(11) The output of "ipsec ispecDisplay" in working buffer is messy (or is hidden).
13. [BUG FIX]
Symptom: The output of CI command "ipsec ikeDisplay" should be re-layouted.
Condition:
(12) Add an ike rule "ipsec ikeAdd", fill the My IP Address with "12345678901234567890123456789012" and Secure Gateway Addr with "12345678901234567890123456789012", save the rule.
(13) "ipsec ikeDisplay" the data shown in working buffer is messy.
14. [BUG FIX]
Symptom: Saving non-active ipsec rule by CI command should not check local and remote IP address.
Condition:
(14) Use CI command "ipsec ipsecAdd"
(15) "ipsec ipsecConfig test"
(16) "ipsec ipsecSave", it can't be saved and will show warning message "The local and remote starting IP address can't both be 0.0.0.0."
15. [ENHANCEMNET]
Add payload information in IKE LOG. Besides reason, we also show which payload caused the IKE LOG.
16. [BUG FIX]
Symptom: Peer ID content is larger than 31 characters
Condition:
(17) Use CI command ipsec ikeE 1
(18) ipsec ikeC peer 1
(19) ipsec ikeC peerIdC 01234567890123456789012345678901 23(which has 34 characters)
(20) ipsec ikeS

(21) ipsec ikeD 1 and we can see peer ID content has 32 characters

17. [BUG FIX]

Symptom: IPSec CI command has a problem about boundary check.

Condition:

(22) Use CI command ipsec ikeAdd

(23) ipsec ikeConfig peerIdType 1 (or ipsec ikeConfig peerIdType 2)

(24) ipsec ikeConfig peerIdContent 123456789012345678901234567890123 (The maximum number of characters/digits is 31, but it does not check). However, ipsec ikeConfig lcIdContent , this command will do the check.

18. [BUG FIX]

Symptom: Packets which size is (1419~1426) can't pass through VPN tunnel.

Condition:

(25) Create a VPN tunnel (Encryption Algorithm = AES or 3DES).

(26) Generate a ping packet (size is from 1419 to 1426) and we can't get any response from the remote host through tunnel.

19. [ENHANCEMENT]

In GUI>WAN, add "Authentication Type" field.

20. [BUG FIX]

Symptom: Static Rout error message is vague

Condition:

(27) Use CI/eWC to add and enable a new static route entry with a gateway that is not on the same network segment as the device's LAN, WAN port.

(28) When applying to save, a warning "The new routing entry can not be added" appears. This warning message is vague. Users cannot determine what goes wrong from the message.

21. [ENHANCEMENT]

Support IXP 422 CPU with DES internal crypto engine on ZyWALL P1.

22. [BUG FIX]

Symptom: IPSec 1.1D CI command "ipsec ikeConfig peerIdContent" has length-checking problem.

Condition:

(29) Use CI command, add an ike rule.

(30) Change the authentication method to RSASignature.

(31) Change the peer ID type to "DNS" or "Email".

(32) Fill the peer ID content with "123456789012345687901234568790123"

(33) Save the ike rule, the router will show warning message, "The maximum ID Content length of DNS or Email is 32 characters."

(34) The content we type is 32 characters, but it failed to save.

23. [BUG FIX]

Symptom: IPSec CI command "ipsec ipsecConfig saIndex" should be modified.

Condition:

(35) Use CI command, type "ipsec ipsecConfig saIndex xxxx".

(36) The router will accept this command, and set the saIndex with "0" without any warning message.

24. [BUG FIX]

Symptom: The hint of CI command "ipsec ipsecConfig activeProtocol" is wrong.

Condition:

(37) Use CI command, type "ipsec ipsecConfig activeProtocol".
(38) The router will show the hint "Usage: ipsec ipsecConfig ike activeProtocol <0:AH | 1:ESP>"
(39) The string "ike" should be removed.

25. [BUG FIX]

Symptom: "ipsec ipsecConfig lcPortStart" and "ipsec ipsecConfig rmPortStart" should be modified.
Condition:
(40) Use CI command, type "ipsec ipsecConfig lcPortStart xxxx".
(41) The router will accept this command, and set the Local Port Start (Remote Port Start) with "0" without any warning message.

26. [BUG FIX]

Symptom: VPN tunnel built failed.
Condition: PC1—ZWP1—ZWP1--PC2
(42) Create a pair of VPN rules and dial it up (Active protocol is ESP)
(43) Change the VPN tunnel from "ESP" to "AH".
(44) Dial the tunnel again but the tunnel can't be built up.

27. [FEATURE CHANGE]

ZyWall P1 can use packet-triggered tunnel after VPN activation done in the first time.

28. [BUG FIX]

Symptom: VPN LED didn't light up when tunnel is connected.
Condition:
(45) Setup IPSEC policy for VPN connection.
(46) Activate VPN connection.
(47) When tunnel is up, VPN LED do not light up.

29. [BUG FIX]

Symptom: For ZWP1, on eWC/Maintenance/Time&Date, after manually setup new time/date and reboot, the time/date cannot save to DUT.
Condition:
(48) On eWC/Maintenance/Time&Date, after manual setup new time/date and reboot, the time/date cannot save to DUT.

30. [BUG FIX]

Symptom: The log of DDNS should be improved.
Condition:
The log for DDNS update is like "DDNS update IP: 172.21.1.25 successfully", we can have at most 5 DDNS records in our router. In the log we can't know which record is updated. The log should be "DDNS update IP: 172.21.1.25 (host 3) successfully"

31. [BUG FIX]

Symptom: DDNS log description not clear.
Condition:
(49) Set DDNS and update IP address, then check log only show "DDNS update IP: 192.168.11.150 successfully"
(50) Can it add what domain update successful, like as "aaa.dyndns.tv update IP: 192.168.11.150 successfully"

32. [BUG FIX]

Symptom: When we use PPTP or PPPoE, WAN IP will not drop immediately.
Condition:

(51) Go to eWC/WAN/WAN
(52) Set WAN as PPTP or PPPoE and save.
(53) Go to eWC/Home, you can see the WAN IP will not update immediately.

33. [BUG FIX]
Symptom: Router crash while editing an active VPN rule.
Condition:
(54) Create a VPN tunnel and dial it up.
(55) Use CI command, ipsec ipsecEdit 1, ipsec ipsecSave.
(56) The system crash.

34. [BUG FIX]
Symptom: System reset after ping.
Condition:
(57) Let router's LAN is DHCP server mode. Suppose router's LAN IP is 192.168.1.1.
(58) PC in LAN side and gets IP from router. Suppose PC's LAN IP is 192.168.1.33.
(59) Turn on UPnP and all related check box. (Make sure that you have turn on UPnP service in your PC).
(60) PC keeps ping 192.168.1.1.
(61) Change router's LAN to 192.168.2.1, IP pool start IP address = 192.168.2.33 (router is Still in DHCP server mode).
(62) Now PC cannot PING to router anymore. After few seconds, router will crash.

35. [ENHANCEMENT]
Remove DHCP relay setting in eWC and CI command

36. [ENHANCEMENT]
(63) Add the SA monitor in Basic Mode on ZWP1.
(64) Remove 'Authentication Type' in wizard.

37. [BUG FIX] Symptom: In VPN wizard, when users configure the My WAN IP as DNS type which can't be shown correctly in summary page. Condition:
(65) Go to VPN wizard
(66) When users configure the My WAN IP as domain name type which can't be shown correctly in eWC>VPN wizard>Summary page. The incorrect information is '0.0.0.0'

38. [ENHANCEMENT]
Add a log page in ZyWALL P1's basic mode for users to check what happens in the ZyWALL.

39. [BUG FIX]
Symptom:ZyWALL P1 will go to the wrong web page when users login eWC from WAN.
Condition:
(67) Login eWC by WAN and select static ip.
(68) Save the configurations in eWC>WAN>WAN.
(69) Then click any hyperlink in eWC.
(70) The ZyWALL will logout.

Modifications in V 3.64(XJ.0) b1 | 11/18/2004
1. First release.

Appendix 1 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.

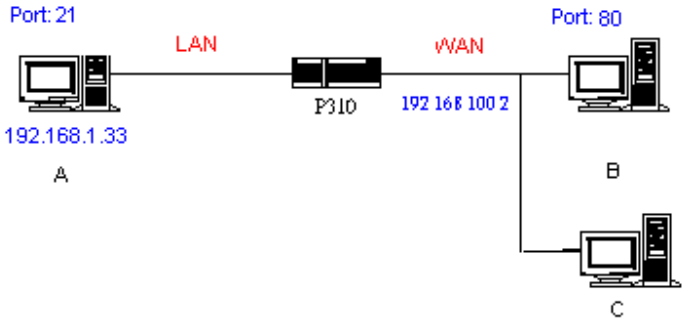
These triggered events can be timed so that they erase the port mapping as soon as they are done with the data transfer, so that the port mapping can be triggered by another Client computer. This gives the *illusion* that multiple computers can use the same port mapping at the same time, but the computers 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 2 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 3 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 4 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.

Command Class List Table		
System Related Command	Exit Command	Ethernet Related Command
Configuration Related Command	IP Related Command	Firewall Related Command
New IPSec Related Command	Certificate Management (PKI) Command	

System Related Command Home

Command				Description
sys				
	adjtime			retrive date and time from Internet
			display	display cbuf static
	callhist			
		display		display call history
		remove	<index>	remove entry from call history
	countrycode		[countrycode]	set country code
	date		[year month date]	set/display date
	domainnam e			display domain name
	edit		<filename>	edit a text file
	extraphnum			maintain extra phone numbers for outcalls
		add	<set 1-3> <1st phone num> [2nd phone num]	add extra phone numbers
		display		display extra phone numbers
		node	<num>	set all extend phone number to remote node <num>
		remove	<set 1-3>	remove extra phone numbers
		reset		reset flag and mask
	feature			display feature bit
	hostname		[hostname]	display system hostname
	logs			
		category		
			access [0:none/1:log/2:alert/3:b oth]	record the access control logs
			attack [0:none/1:log/2:alert/3:b oth]	record and alert the firewall attack logs
			display	display the category setting
			error [0:none/1:log/2:alert/3:b oth]	record and alert the system error logs
			ipsec [0:none/1:log/2:alert/3:b oth]	record the access control logs
			ike [0:none/1:log/2:alert/3:b oth]	record the access control 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:b oth]	record the pki logs
			tcpreset [0:none/1:log]	record the tcp reset logs

			upnp [0:none/1:log]	record upnp logs
		clear		clear log
		display	[access|attack|error|ipsec|ike|javablocked|mten|packetfilter|pki|tcpreset|urlblocked|urlforward]	display all logs or specify category logs
		errlog		
			clear	display log error
			disp	clear log error
			online	turn on/off error log online display
		load		load the log setting buffer
		mail		
			alertAddr [mail address]	send alerts to this mail address
			display	display mail setting
			logAddr [mail address]	send logs to this mail address
			schedule display	display mail schedule
			schedule hour [0-23]	hour time to send the logs
			schedule minute [0-59]	minute time to send the logs
			schedule policy [0:full/1:hourly/2:daily/3:weekly/4:none]	mail schedule policy
			schedule week [0:sun/1:mon/2:tue/3:wed/4:thu/5:fri/6:sat]	weekly time to send the logs
			server [domainName/IP]	mail server to send the logs
			subject [mail subject]	mail subject
		save		save the log setting buffer
		syslog		
			active [0:no/1:yes]	active to enable unix syslog
			display	display syslog setting
			facility [Local ID(1-7)]	log the messages to different files
			server [domainName/IP]	syslog server to send the logs
…..		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
		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
	pwderrtm		[minute]	Set or display the password error blocking timeout value.
	rn			
		load	<entry no.>	load remote node information
		disp	<entry no.>(0:working	display remote node information

			buffer)	
		nat	<none|sua|full_feature>	config remote node nat
		nailup	<no|yes>	config remote node nailup
		mtu	<value>	set remote node mtu
		save	[entry no.]	save remote node information
	stdio		[second]	change terminal timeout value
	time		[hour [min [sec]]]	display/set system time
	tos			
		display		display all runtime TOS
		listPerHost		display all host session count
		debug	[on|off]	turn on or off TOS debug message
		sessPerHost	<number>	configure session per host value
		timeout		
			display	display all TOS timeout information
			icmp <idle timeout>	set idle timeout value
			igmp <idle timeout>	set idle timeout value
			tcpsyn <idle timeout>	set idle timeout value
			tcp <idle timeout>	set idle timeout value
			tcpfin <idle timeout>	set idle timeout value
			udp <idle timeout>	set idle timeout value
			gre <idle timeout>	set idle timeout value
			esp <idle timeout>	set idle timeout value
			ah <idle timeout>	set idle timeout value
			other <idle timeout>	set idle timeout value
		tempTOSDisplay		display temporal TOS records.
		tempTOSTimeout	[timeout value]	set/display temporal timeout value
	trcdisp	parse, brief, disp		monitor packets
	trclog			
	trcpacket			
	syslog			
		server	[destIP]	set syslog server IP address
		facility	<FacilityNo>	set syslog facility
		type	[type]	set/display syslog type flag
		mode	[on|off]	set syslog mode
	version			display RAS code and driver version
	view		<filename>	view a text file
	wdog			
		switch	[on|off]	set on/off wdog
		cnt	[value]	display watchdog counts value: 0-34463
	romreset			restore default romfile
		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
	socket			display system socket information
	filter			
		netbios		
			disp	display netbios filter status
			config <0:Between LAN and WAN, 3:IPSec passthrough, 4:Trigger Dial> <on|off>	config netbios filter
	roadrunner			
		debug	<level>	enable/disable roadrunner service 0: diable <default> 1: enable
		display	<iface name>	display roadrunner information iface-name: enif0, wanif0
		restart	<iface name>	restart roadrunner
	ddns			
		debug	<level>	enable/disable ddns service
		display	<iface name>	display ddns information
		restart	<iface name>	restart ddns
		logout	<iface name>	logout ddns
	cpu			
		display		display CPU utilization
	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

Exit Command Home

Command				Description
exit				exit smt menu

Ethernet Related Command

Home

Command				Description
ether				
	config			display LAN configuration information
	driver			
		cnt		
			disp <name>	display ether driver counters
		ioctl	<ch_name>	Useless in this stage.
		status	<ch_name>	see LAN status
	version			see ethernet device type
	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.

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#>
	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 #>
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 |daily | weekly>		Edit email schedule when log is full or per hour, day, week.
			day <sunday | monday | tuesday | wednesday | thursday | friday | saturday>		Edit the day to send the log when the email policy is set to Weekly
			hour <0~23>		Edit the hour to send the log when the email policy is set to daily or weekly
			minute <0~59>		Edit the minute to send to log when the email policy is set to daily or weekly
			Subject <mail subject>		Edit the email subject
		attack	send-alert <yes|no>		Activate or deactivate the firewall DoS attacks notification emails
			block <yes|no>		Yes: Block the traffic when exceeds the tcp-max-incomplete threshold
					No: Delete the oldest half-open session when exceeds the tcp-max-incomplete threshold
			block-minute <0~255>		Only valid when sets 'Block' to yes. The unit is minute
			minute-high <0~255>		The threshold to start to delete the old half-opened sessions to minute-low
			minute-low <0~255>		The threshold to stop deleting the old half-opened session
			max-incomplete-high <0~255>		The threshold to start to delete the old half-opened sessions to max-incomplete-low
			max-incomplete-low <0~255>		The threshold to stop deleting the half-opened session
			tcp-max-incomp		The threshold to start executing

			lete <0~255>		the block field
		set <set#>	name <desired name>		Edit the name for a set
			default-permit <forward|block>		Edit whether a packet is dropped or allowed when it does not match the default set
			icmp-timeout <seconds>		Edit the timeout for an idle ICMP session before it is terminated
			udp-idle-timeout <seconds>		Edit the timeout for an idle UDP session before it is terminated
			connection-timeout <seconds>		Edit the wait time for the SYN TCP sessions before it is terminated
			fin-wait-timeout <seconds>		Edit the wait time for FIN in concluding a TCP session before it is terminated
			tcp-idle-timeout <seconds>		Edit the timeout for an idle TCP session before it is terminated
			pnc <yes|no>		PNC is allowed when 'yes' is set even there is a rule to block PNC
			log <yes|no>		Switch on/off sending the log for matching the default permit
			logone <yes|no>		Switch on/off for one packet that create just one log message.
			rule <rule#>	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 address>	Select and edit a source address range of a packet which complies to this rule.

				destaddr-single <ip address>	Select and edit a destination address of a packet which complies to this rule
				destaddr-subnet <ip address> <subnet mask>	Select and edit a destination address and subnet mask if a packet which complies to this rule.
				destaddr-range <start ip address> <end ip address>	Select and edit a destination address range of a packet which complies to this rule.
				tcp destport-single <port#>	Select and edit the destination port of a packet which comply to this rule. For non-consecutive port numbers, the user may repeat this command line to enter the multiple port numbers.
				tcp destport-range <start port#> <end port#>	Select and edit a destination port range of a packet which comply to this rule.
				udp destport-single <port#>	Select and edit the destination port of a packet which comply to this rule. For non-consecutive port numbers, users may repeat this command line to enter the multiple port numbers.
				udp destport-range <start port#> <end port#>	Select and edit a destination port range of a packet which comply to this rule.
				desport-custom <desired custom port name>	Type in the desired 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
delete	firewall	e-mail			Remove all email alert settings
		attack			Reset all alert settings to defaults
		set <set#>			Remove a specified set from the firewall configuration
		set <set#>	rule <rule#>		Remove a specified rule in a set from the firewall configuration
insert	firewall	e-mail			Insert email alert settings
		attack			Insert attack alert settings
		set <set#>			Insert a specified rule set to the firewall configuration
		set <set#>	rule <rule#>		Insert a specified rule in a set to the firewall configuration
cli					Display the choices of command list.

IP Related Command Home

Command	Description

ip				
	address		**[addr]**	**display host ip address**
	alg			
		disp		**Show ALG enable disable status**
		enable	**<ALG_FTP|ALG_H323|ALG_SIP>**	**Enable ALG command**
		disable	**<ALG_FTP|ALG_H323|ALG_SIP>**	**Disable ALG command**
		siptimeout	**<timeout in second> or 0 for no timeout**	**Configure SIP timeout command**
	arp			
		status	**<iface>**	**display ip arp status**
		attpret	**<on|off>**	**Switch receive APR from the different network or not.**
		force	**<on|off>**	**Switch the time out function of the APR.**
	dhcp		**<iface>**	
		client		
			release	**release DHCP client IP**
			renew	**renew DHCP client IP**
			release <entry num>	**release specific entry of the dhcp server pool**
		status	**[option]**	**show dhcp status**
	dns			
		query		
		server	**<primary> [secondary] [third]**	**set dns server**
		stats		
			Clear	**clear dns statistics**
			Disp	**display dns statistics**
		default	**<ip>**	**Set default DNS server**
		system		
			display	**display dns system information**
			edit <0: first|1: second|2: third> <0:from ISP|1:usr-def|2:none> [IP address if choosing 1]	**edit dns record**
	Httpd			
		debug	**[on|off]**	**set http debug flag**
	icmp			
		status		**display icmp statistic counter**
		discovery	**<iface> [on|off]**	**set icmp router discovery flag**
	ifconfig		**[iface] [ipaddr] [broadcast <addr> |mtu <value>|dynamic]**	**configure network interface**
	ping		**<hostid>**	**ping remote host**
	route			
		status	**[if]**	**display routing table**
		add	**<dest_addr|default>[/<bits>]**	**add route**

			<gateway> [<metric>]	
		addiface	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add an entry to the routing table to iface
		drop	<host addr> [/<bits>]	drop a route
	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.
	udp			
		status		display udp status
	rip			
	tcp			
		status	[tcb] [<interval>]	display TCP statistic counters
	telnet		<host> [port]	execute telnet clinet command
	tftp			
	traceroute		<host> [ttl] [wait] [queries]	send probes to trace route of a remote host
	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
	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

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.
		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
	updatePeer Ip			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
	ikeDisplay	<rule #>		Display IKE rule #, if no rule number assigned, this command will show current working buffer. NOTE: If working buffer is null, it will show error messages. Please ADD or EDIT an IKE rule before display.
	ikeAdd			Create a working buffer for IKE rule.
	ikeEdit	<rule #>		Edit an existing IKE rule #
	ikeSave			Save working buffer of IKE rule to romfile.
	ikeList			List all IKE rules
	ikeDelete	<rule #>		Delete IKE rule #
	ikeConfig	name	<string>	Set rule name (max length is 31)
		negotiationMode	<0:Main | 1:Aggressive>	Set negotiation mode
		natTraversal	<Yes| No>	Enable NAT traversal or not.
		multiPro	<Yes|No>	Enable multiple proposals in IKE or not
		lcIdType	<0:IP | 1:DNS | 2:Email>	Set local ID type
		lcIdContent	<string>	Set local ID content
		myIpAddr	<IP address>	Set my IP address
		peerIdType	<0:IP | 1:DNS | 2:Email>	Set peer ID type
		peerIdContent	<string>	Set peer ID content
		secureGwAddr	<IP address | Domain name>	Set secure gateway address or domain name
		authMethod	<0:PreSharedKey | 1:RSASignature | 2:preShare Key+XAUTH | 3:RSASignature+ XAUTH>	Set authentication method in phase 1 in IKE
		preShareKey	<ASCII | 0xHEX>	Set pre shared key in phase 1 in IKE
		certificate	<certificate name>	Set certificate file if using RSA signature as authentication method.

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

		rmAddrType	<0:single | 1:range | 2:subnet>	Set remote address type
		rmAddrStart	<IP>	Set remote start address
		rmAddrEndMask	<IP>	Set remote end address or mask
		rmPortStart	<port>	Set remote start port
		rmPortEnd	<port>	Set remote end port
	policyList			List all IPSec policies
	manualDisplay	<rule #>		Display manual rule #
	manualAdd			Add manual rule
	manualEdit	<rule #>		Edit manual rule #
	manualSave			Save IPSec rules
	manualList			List all IPSec rule
	manualDelete	<rule #>		Delete IPSec rule #
	manualConfig	name	<string>	Set rule name
		active	<Yes | No>	Set active or not
		myIpAddr	<IP address>	Set my IP address
		secureGwAddr	<IP address>	Set secure gateway
		protocol	<1:ICMP | 6:TCP | 17:UDP>	Set protocol
		lcAddrType	<0:single | 1:range | 2:subnet>	Set local address type
		lcAddrStart	<IP>	Set local start address
		lcAddrEndMask	<IP>	Set local end address or mask
		lcPortStart	<port>	Set local start port
		lcPortEnd	<port>	Set local end port
		rmAddrType	<0:single | 1:range | 2:subnet>	Set remote address type
		rmAddrStart	<IP>	Set remote start address
		rmAddrEndMask	<IP>	Set remote end address or mask
		rmPortStart	<port>	Set remote start port
		rmPortEnd	<port>	Set remote end port
		activeProtocol	<0:AH | 1:ESP>	Set active protocol in manual
		ah	encap <0:Tunnel | 1:Transport>	Set encapsulation in ah in manual
			spi <decimal>	Set spi in ah in manual
			authAlgo <0:MD5 | 1:SHA1>	Set authentication algorithm in ah in manual
			authKey <string>	Set authentication key in ah in manual
		esp	encap <0:Tunnel | 1:Transport>	Set encapsulation in esp in manual
			spi <decimal>	Set spi in esp in manual
			encryAlgo <0:Null | 1:DES | 2:3DES>	Set encryption algorithm in esp in manual
			encryKey <string>	Set encryption key in esp in manual
			authAlgo <0:MD5 | 1:SHA1>	Set authentication algorithm in esp in manual
			authKey < string>	Set authentication key in esp in manual
	manualPolicyList			List all manual policy
	swSkipOve		<on|off>	- When a VPN rule with remote range

	rlapIp			**overlaps with local range, the switch decides if a local to local packet should apply this rule.** **- Default value is "off" which means "no skip".**
	adjTcpMss		**<off|auto|user defined value>**	**- After a tunnel is established, system will automatically adjust TCP MSS.** **- After all tunnels are drops, the MSS will adjust to the original value.** **- The default value is auto.**

Firewall Related Command **Home**

Command					**Description**
sys	**Firewall**				
		acl			
			disp		**Display specific ACL set # rule #, or all ACLs.**
		active	**<yes|no>**		**Active firewall or deactivate firewall**
		clear			**Clear firewall log**
		cnt			
			disp		**Display firewall log type and count.**
			clear		**Clear firewall log count.**
		disp			**Display firewall log**
		online			**Set firewall log online.**
		dynamicrule			
		dos			
			smtp		**Set SMTP DoS defender on/off**
			display		**Display SMTP DoS defender setting.**
			ignore		**Set if firewall ignore DoS in lan/wan/dmz/wlan**
		ignore			
			triangle		**Set if firewall ignore triangle route in lan/wan/dmz/wlan**
		schedule			
			load [set # rule #]		**Load firewall ACL schedule by rule.**
			display		**Display ACL schedule in buffer.**
			save		**Save buffer date and update runtime firewall ACL rule.**
			week		
				monday [on/off]	**Set schedule on or off by day – Monday.**
				tuesday [on/off]	**Set schedule on or off by day – Tuesday.**
				wednesday [on/off]	**Set schedule on or off by day – Wednesday.**
				thursday [on/off]	**Set schedule on or off by day – Thursday.**
				friday [on/off]	**Set schedule on or off by day – Friday.**
				saturday [on/off]	**Set schedule on or off by day – Saturday.**
				sunday [on/off]	**Set schedule on or off by day – Sunday.**

				allweek [on/off]	Quick set schedule on or off by week.
			timeOfDay [always/hh:mm]		Set firewall ACL schedule block time of day.

Certificate Management (PKI) Command

Home

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

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

				basic information.
		rename <old name> <new name>		**Rename the specified my certificate. <old name> specifies the name of the certificate to be renamed. <new name> specifies the new name as which the certificate is to be saved.**
		def_selfsigned [name]		**Set the specified self-signed certificate as the default self-signed certificate. [name] specifies the name of the certificate to be set as the default self-signed certificate. If [name] is not specified, the name of the current self-signed certificate is displayed.**
	ca_trusted			
		import <name>		**Import the PEM-encoded certificate from stdin. <name> specifies the name as which the imported CA certificate is to be saved.**
		export <name>		**Export the PEM-encoded certificate to stdout for user to copy and paste. <name> specifies the name of the certificate to be exported.**
		view <name>		**View the information of the specified trusted CA certificate. <name> specifies the name of the certificate to be viewed.**
		verify <name> [timeout]		**Verify the certification path of the specified trusted CA certificate. <name> specifies the name of the certificate to be verified. [timeout] specifies the timeout value in seconds (optional). The default timeout value is 20 seconds.**
		delete <name>		**Delete the specified trusted CA certificate. <name> specifies the name of the certificate to be deleted.**
		list		**List all trusted CA certificate names and basic information.**
		rename <old 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.**

		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.**

Appendix 5 IPSec IP Overlap Support

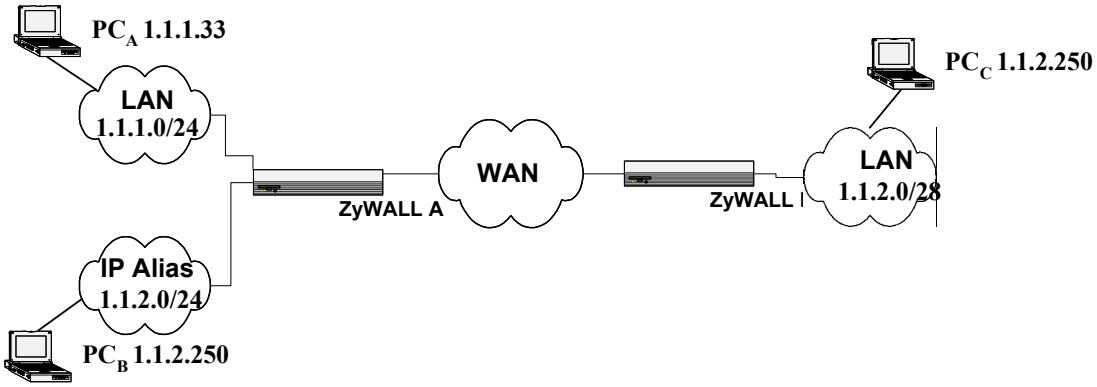


Figure 1

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 6 VPN Local IP Address Limitation

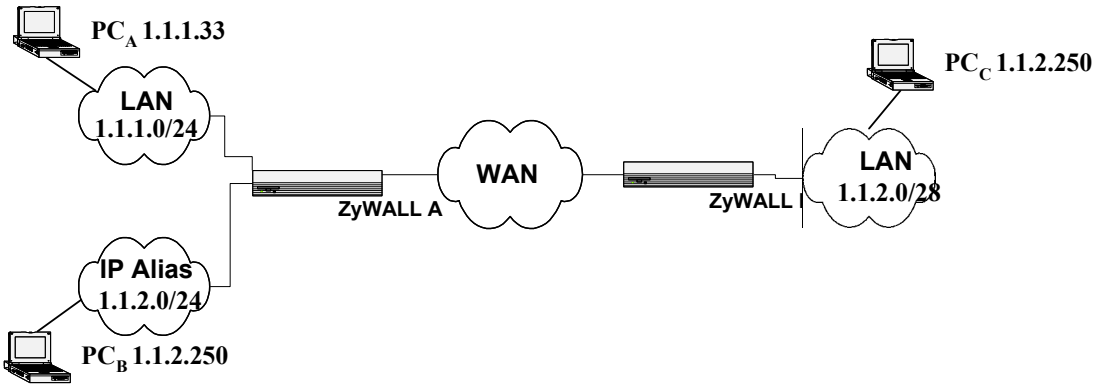


Figure 1

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, a user configures 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 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.