ZyXEL

Firmware Release Note

ZyWALL 50

Release 3.52(WC.0)

Date: **Mar, 4, 2003**
Author: **Neil Cheng**

ZyXEL ZyWALL 50 Standard Version 3.52(WC.0) Release Note

Date: Mar 4, 2003

Supported Platforms:

ZyXEL ZyWALL 50

Versions:

ZyNOS Version: V3.52(WC.0) | 03/04/2003 14:47:02
Bootbase Version: V1.04 | 09/11/2001 15:20:23

Note:

1. 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.
2. Using Web to configure VPN, the phase 1 algorithms have been fixed to DES + MD5. If other algorithms are preferred, please use ADVANCE page to configure them.
3. When firewall turns from "off" to "on", the firewall initialization procedure will disconnect all connections running through the ZyWALL.
4. Please refer to Appendix 5 for the triangle route issue.
5. After upgrading the firmware, the DHCP client and IKE feature may fail. This is because new firewall has four sets and the previous one had only two sets. In the previous firmware, IKE and BOOTP_CLIENT protocol was placed on WAN-to-LAN set. However, in the new design, they should be put in WAN-to-WAN / ZyWALL set. Please move them to the correct set manually or restore default romfile to make this changed.
6. Keep-alive feature only works when both peers turn on the keep-alive switch.

Known Issues:

1. Symptom: After system boot up, static route cannot set into routing table.
   Condition: If gateway in static route belongs to WAN interface, static route node will not add in routing table and have no function after ZyWALL reboot. So, users need to reactive static route rule to enable this function.
2. eWC→WAN IP has bugs when WAN→ISP is PPPoE or PPTP. Leaving some values in remote IP or remote masks for WAN→IP and then switch to dynamic IP, ZyWALL cannot dial anymore.
3. When Peer ID content is blank when its ID type is IP and the secure gateway address is 0.0.0.0, the rule will be chosen when incoming packets' ID type is IP. This is because ZyWALL only check ID type when this rule's ID content is blank and ID type is IP. We will modify it in the future.
4. Content filter can block cookies but have no log. Log of cookies will be added in next release.
5. E-mail alert will work when you fill both log and alert E-mail addresses. This will fix in the next release.
6. Sometimes the applications bound in MSN can't create connection, when this happened please wait

about 3 minutes (for session timeout) and try again.

7. Setting time server as none in eWC will show an error message, but this will not affect the functionality. The page can not refresh after users apply.

Features:

Modification in V3.52(WC.0)b6 | 2/19/2003

1. [BUG FIX] Symptom: MSN messenger can't initial applications bound in MSN like whiteboard, file transfer and etc. when firewall is enable.
   Condition: Firewall can't parse the information send by MSN server and create connection to remote computer.
2. [BUG FIX] Symptom: The custom port is allowed to be deleted even though it is used by other firewall rules.
   Condition: Once it is deleted, the firewall will change to allow Any (TCP) and Any (UDP) and result in a security problem.

Modification in V3.52(WC.0)b5 | 1/22/2003

1. [FEATURE CHANGE] When phase 1 ID type is IP and content is blank or 0.0.0.0, ZyWALL will use WAN IP or Secure gateway address as content. In the previous design, only blank content will do. Please refer to appendix for more details.
2. [BUG FIX] Symptom: When phase 1 ID type is IP, tunnel cannot be built.
   Condition:
   (1) Set MyIP 0.0.0.0
   (2) Set My ID Type as IP
   (3) Leave My ID content blank
   (4) During IKE, ZyWALL will use 0.0.0.0 as ID content. However it should be WAN IP.

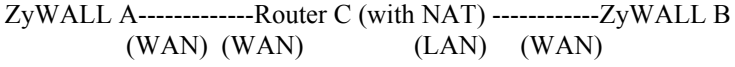
Modification in V3.52(WC.0)b4 | 1/8/2003

1. [ENHANCEMENT] Add IPSec NAT traversal support. It only supports ESP tunnel and ESP transport when key management is IKE. No manual key support for IPSec NAT traversal.
2. [ENHANCEMENT] Add centralized logs for phase 1 ID (FQDN). When ID check fails during IKE phase 1, LOG will show the incoming ID type and content for reference.
3. [FEATURE CHANGE] LAN DHCP server pool size can be 1.
   NOTE: When the pool size is 1, LAN IP cannot be the same as Client IP Pool Starting Address.
4. [FEATURE CHANGE] Centralize Log GUI color defines. Log message with black color is normal and red color for alert, attack and error messages.
5. [BUG FIX] Symptom: Receiving hotmail mail will cause system crash.
   Condition: Enable Block Cookies and Receiving hotmail mail and cause system crash.
6. [BUG FIX] Symptom: "Don't block Java/ActiveX/Cookies/Web Proxy to Trusted Domain sites" sometimes cannot work.
   Condition: Enable "Filter List Customization" and "Don't block Java/ActiveX/Cookies/Web Proxy to Trusted Domain sites" but the web pages that contains Java/ActiveX/Cookies and Web Proxy components still be blocked by ZyWALL.
7. [BUG FIX] Symptom: When "ipsec switch" is off, "ipsec dial" still works.
   Condition: If user uses command "ipsec switch off" to turn off IPSec, "dial" still works.
8. [BUG FIX] Symptom: Can't build tunnel successfully with IPSec without FQDN.
   Condition: With the firmware without FQDN, IPSec can't build tunnel successfully by setting IP in FQDN ID type.
9. [BUG FIX] Symptom: If firewall turns on, traffic redirect can not switch back the original Internet connection.
   Condition: This problem only happens when the traffic redirect gateway is not on WAN.

If the default Internet connection fails, router will switch routing to traffic redirect gateway. When firewall turns on and the original connection recovers, the routing can not switch back.

Modification in V3.52(WC.0)b3 | 12/19/2002

1. [ENHANCEMENT] Add CI commands to configure IPSec rules. Please refer CI command list.
2. [ENHANCEMENT] The subject of email for the logs can be configured by CI command "sys logs mail subject".
3. [ENHANCEMENT] Add Stdio Timeout Mechanism. Let users can specify ZyWALL management session (either via the web configuration or SMT) idle timeout value.
4. [ENHANCEMENT] Add Static IP by MAC address with DHCP client address assignment.
5. [ENHANCEMENT] Show the reason of forward/block by content filter in the centralized log message.
6. [ENHANCEMENT] Add a retype password confirmation mechanism for PPTP and PPPoE setup in smt menu 4 and 11.
7. [ENHANCEMENT] Add full path + file name check for keyword blocking.
8. [ENHANCEMENT] The system can send an alert mail of “Access Control”, “Blocked JAVA etc”, “IPSec”, and “IKE” categories.
9. [ENHANCEMENT] Add new centralized log category – IKE. And add CI command “sys logs category ike” to set it, “sys logs display ike” to display it.
10. [FEATURE CHANGE] Wording change for firewall log messages. For example: "set:1" will be "L to W" means packet from LAN to WAN.
11. [FEATURE CHANGE] The log of remote management is moved from error log to centralized log. Its category is “Access Control”.
12. [FEATURE CHANGE] In VPN configuration, local / remote IP start field can accept 0.0.0.0.
13. [FEATURE CHANGE] Make hard-coded NetBIOS CI commands visible by users.
14. [FEATURE CHANGE] Sometimes user will get some default policy log without set, because other processes like NAT drop these packets or bypass firewall. We replace the default policy description with its actual reason in centralize log.
15. [FEATURE CHANGE] Remove default port definition for AIM, ICQ and MSN messenger in firewall.
16. [BUG FIX] Symptom: When our router exchanges system information through NetBIOS, it may crash.
    Condition: When router send NetBIOS broadcast and found a new name needed to be added. The name list initials with NULL will cause adder function crash our ZyWALL.
17. [BUG FIX] Symptom: Content filtering will block keyword that contains *.html.
    Condition: Use "ip urlfilter customize actionFlag act5 enable" to enable the full path setting. Then add “.html” for keyword blocking. Content filtering will block website that contains *.html.
18. [BUG FIX] Symptom: The keyword blocking does not work.
    Condition: Use browser to access the URL that set in the keyword blocking, the packets will be still allowed to pass after enable the full path check.
19. [BUG FIX] Symptom: Firewall logs duplicate ICMP type 3 code 3 which reply by itself.
    Condition: When router receives a unknow UDP service packet, it reply ICMP port unreachable and firewall logs this packet twice.
20. [BUG FIX] Symptom & Condition: During IKE phase 1 negotiation, if ZyWALL receives a Notify DEL payload, it may crash. Reason & Solution: It's a NULL pointer problem which we should check if the DEL payload is sent to a valid SA.
21. [BUG FIX] Symptom: While access http://www.gamespy.com/articles/ and http://groups.yahoo.com system will crash.
    Condition: System crashes when access http://www.gamespy.com/articles/ or when survey/read the forums via http://groups.yahoo.com.
22. [BUG FIX] Symptom: When ID type is IP, VPN tunnel can not established if passing through another router with NAT.
    Condition: Take the figure below as the example:



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

23. [BUG FIX] Symptom: The router will block the trusted domain URL.
    Condition: 1. Enable filter list customization & Disable all web traffic except for Trusted Domains.
    2. Add mypathways.deere.com in the trusted domain and go to this URL.
    3. Login the page.
24. [BUG FIX] Symptom: The PPPOE or PPTP address can be set within the range of LAN subnet.
    Condition: When using smt menu 4 or 11, choose the pppoe or pptp encapsulation, set the IP address within the range of LAN subnet and then save the configuration.
25. [BUG FIX] Symptom: Content filter will block the web site that matches the trusted domain setting.
    Condition: When web site is both in the cybernot filter list and the trusted domain list, the content filter will block the web site.
26. [BUG FIX] Symptom: Can not download cybernot list.
    Condition: On the "Advanced"->"content filter"->"list update" web page, user presses "download now" to download the cybernot list.
27. [BUG FIX] Symptom: Weird ICMP packet logs are generated.
    Condition: When user sends a large echo packet through the firewall, there are many weird ICMP packet logs to be generated. Sometimes the type and code of that ICMP log show undefined number, and the message shows "Unsupported/out-of-order ICMP".
28. [BUG FIX]Symptom: System halts when both firewall and syslog turn on.
    Condition: When syslog server daemon stops or syslog server host does not exist, the syslog packets explode and firewall generates masses of ICMP packet logs.
29. [BUG FIX] Fix a security issue related with smurf attack.
30. [BUG FIX] Symptom: The system will allow the packet with DF=1 and the packet length > MTU to pass through the router without any error message returned to the sender.
    Condition: When the packet with its length larger than MTU but DF bit set, it is still allowed to pass through the router.
31. [BUG FIX] Symptom: Firewall->Edit: The "Active" checkbox value will not be saved.
    Condition: If user clicks "SrcAdd" or "SrcEdit" button in Firewall Edit page to configure "Source Address" in one rule, then the value of "Active" checkbox will not be saved.
32. [BUG FIX] Symptom: Remote management to LAN IP over IPSec failed.
    Condition: While NAT was enabled, remote device could not access router's LAN IP through IPSec tunnel. In other words, remote management to the LAN IP over IPSec tunnel failed.
33. [BUG FIX] Fix a security issue related with port scan.
34. [BUG FIX] Symptom: VPN web page configuration is not correct.
    Conditions:
    1. If Edit VPN configuration choose "manual key", then it cannot be save. The error message "Manual My ID only can be IP" will be displayed.
    2. If Edit VPN configuration choose "manual key", and ESP encryption algorithm choose "NULL", then press Apply. Edit the rule again, the authentication key cannot input anymore.
35. [BUG FIX] Symptom: When a PC traces route from LAN to WAN, ZyWALL is not visible in the tracing path with firewall on.
    Condition: Firewall blocks the time exceed ICMP packet and log message is "Unsupported/out-of-order ICMP".
36. [BUG FIX] Symptom: The content of web forward log message is junk.
    Condition: If user blocks the keyword "kimo" and access the web site that does not contain the keyword "kimo", the system will generate web forward log message.
37. [BUG FIX] Symptom: Some IKE INFO logs are treated as ALERT.
    Condition: IKE logs "RECV: [payload]" messages are marked as alert, but it should be INFO.
38. [BUG FIX] Symptom: Conflict check between multi-NAT configuration and VPN is not correct.
    Condition: When VPN local IP address is SUBNET, the conflict check with multi-NAT will reply

incorrect result.

39. [BUG FIX] Symptom: The isolated DNS proxy server behinds firewall can not work.
    Condition: When the second or proxy DNS server behinds firewall and try to connect with public DNS server, the TCP 3-ways handshake fails.
40. [BUG FIX] Symptom: The content of the 128th email log is junk.
    Condition: The content of email log will be incorrect if each log is large.
41. [BUG FIX] Symptom: The system crashes when establishing IPSec connection.
    Condition: When local and peer machine use different phase 1 authentication algorithms in IKE, both systems crash.
42. [BUG FIX] Symptom: PC can ping router's LAN IP.
    Condition: When "SUA only" and "firewall off", outside PC can ping router's LAN IP.
43. [BUG FIX] Symptom: ZyWALL50 can not block JAVA & Active-X components.
    Condition: When connecting to web site that has JAVA & Active-X components, the router can not block them by content filter.
44. [BUG FIX] Symptom: XBox Live can't work through router.
    Condition: Xbox Live can not work through ZyWALL 50.
45. [BUG FIX] Symptom: Telnet session issue when firmware uploaded.
    Condition: After firmware uploaded, system will reboot. However ZyWALL will not disconnect the telnet session connecting to it. As a result, users have to disconnect the telnet session manually.
46. [BUG FIX] Symptom: Email log can not be sent.
    Condition: When alert address is not set in the "Log->Log settings->Send alerts to:" field in the GUI, press the "Email Log Now" button in the Log->View Log page will not email the logs.

Modification in V3.52(WC.0)b2 | 10/30/2002

1. [ENHANCEMENT] Add traffic redirect with remote node setup.
2. [ENHANCEMENT] Extended firewall ACL rule numbers to 100.
3. [ENHANCEMENT] Extended static route rule numbers to 30.
4. [ENHANCEMENT] Enlarge NAT concurrent session to 2048.
5. [ENHANCEMENT] Add a protection mechanism for password check. When users enter wrong password three times, the system will block users trying to log in for the minutes that user defined. The blocking time will be set by CI command. NOTE: Use CI command "sys pwderrtm [minutes]" to set this timeout value. System will not perform this check when timeout calur is empty.
6. [ENHANCEMENT] Add more ID supported in IKE phase 1 authentication. Now ZyWALL50 supports ID-IP, ID-FQDN, ID-USER-FQDN.
7. [ENHANCEMENT] Add remote management as menu 24.11 in eWC. User can set "SNMP" and "Ping on internet WAN port" in web configuration.
8. [ENHANCEMENT] Add IP Alias under LAN configuration. User can configure it in eWC.
9. [ENHANCEMENT] Modified "ip dhcp enif0 server dnsorder" CI command. Through this command, users can assign DNS order.
10. [ENHANCEMENT] Add Nailed-Up connection settings for PPPOE & PPTP of eWC.
11. [ENHANCEMENT] Add "stroute" in ip command set. Through this command, users can set / modify static routes.
12. [ENANCEMENT] DDNS enhancement. In previous firmware, ZyWALL will provide its WAN IP to DDNS server, even if it's a private IP. Now a user can specify the public IP by himself, or let the DDNS detect a proper global IP for ZyWALL.
13. [ENHANCEMENT] When NAT session table is full, there will be a log in Centralized log. Its category is "System Maintenance".
14. [ENHANCEMENT] When a host exhausts NAT session table, there will be a log in Centralized log. Its category is "System Errors".
15. [ENHANCEMENT] In "ip nat iface" CI command, system will parse ESP packets in NAT table list.
16. [ENHANCEMENT] When system updates its time or assign an IP to a host, there will be a log in Centralized log. The category is "System Maintenance".
17. [ENHANCEMENT] When the user login to the router (SMT, FTP, TELNET, or WEB), there will be a log in Centralized log. The category is "System Maintenance".

18. [ENHANCEMENT] Add a protection mechanism for password check. When users enter wrong password three times, the system will block users trying to log in for three minutes. The blocking time will be set by CI command. NOTE: Use CI command : "sys pwderrtm [minutes]" to set this value.
19. [ENHANCEMENT] In CI command "sys logs display", add a category filter to display only the specified category. For example, "sys logs display access" to display the access category only.
20. [FEATURE CHANGE] The value of "sys stdio" will be kept after users log off. But after power on/off, the value will be restored to default.
21. [FEATURE CHANGE] In firewall log, use "CHECK NEXT RULE" instead of blank left when a rule log setting is "not match".
22. [FEATURE CHANGE] Modify the firmware upload successful page.
23. [FEATURE CHANGE] If eWC:LAN→Pool Size sets to 0, it must show warning message on status.
24. [FEATURE CHANGE] Hard-coded Netbios filters are modified. Now WAN-to-LAN and LAN-to-WAN are independent. Add corresponding pages in eWC: WAN / LAN / VPN.
25. [FEATURE CHANGE] The default value of resolving IPSec peer's DNS is changed from 30 min to 15 min.
26. [FEATURE CHANGE] Default values of hard-coded Netbios filters are changed. They are LAN to WAN: block; WAN to LAN: block; IPSec: Forward; Trigger dial: Disable.
27. [FEATURE CHANGE] Log settings of default policy are changed. For those default policies are "forward", there will be no logs. On the other hand, for those default policies are "block", there will be logs.
28. [FEATURE CHANGE] Log schedule in Centralized log is default to "NONE".
29. [FEATURE CHANGE] Default value of remote management is changed to "ALL".
30. [FEATURE CHANGE] IPSec idle timeout value is changed back to 2 min.
31. [BUG FIX] Content Filter does not block cookies.
32. [BUG FIX] Netbios packet crash the router when firewall is enabled.
33. [BUG FIX] Fix a security issue related with IP stack.
34. [BUG FIX] Symptom: User may not enter SMT menu when the stdio timeout value is 0.
    Condition: Using CI command "sys stdio 0" to set no stdio timeout and enter SMT menu then log out.
35. [BUG FIX] Symptom: Using CI command "ip pong" sometimes caused system reboot.
    Condition: When "pong" a host with large packet in a short time, ex "ip pong somehost 3000 200", system may crash.
36. [BUG FIX] Symptom: Ftp remote management can't work over IPSec tunnel, even if access=ALL.
    Condition: Control channel can be opened over tunnel, but data channel is failed.
37. [BUG FIX] Symptom: Send an email log with more than 34 logs will cause system crash.
    Condition: In logs->view log in the WEB menu, when the number of logs is more than 34, press "Email Log Now" will cause system crash.
38. [BUG FIX] Symptom: Router learns illegal ARP packet.
    Condition: Router learns IP MAC addresses from wrong interface. For example, router may learn LAN IP Mac address from WAN. It causes some host can not connect to the router.
39. [BUG FIX] Symptom: Packet with it's length > MTU and don't fragment(DF) bit is set will pass through and without any error message returned to sender.
40. [BUG FIX] Symptom: Under VPN channel, when sending out large file, the system will crash.
    Condition: When continuously sending large packet and the data packet size is over certain size (say 1450), then the system will eventually crash.
41. [BUG FIX] Symptom: Deniel Access Message is too small.
    Condition: The "Denied Access Message" of content filter Full path should extend to all web page, not only the frames..
42. [BUG FIX] Symptom: "Deleting" function for a NAT set is not complete.
    Condition: Create a rule in menu 15.1.1 in NAT full feature mode then delete the set that contains the rule. Using ci command "ip nat lookup #setnum" will see the deleted set with no rules in it.
43. [BUG FIX] Symptom: Delete an NAT set or that contains an active rule or modify the rule and ping outside host will cause system crashed.
    Condition: Create a rule in menu 15.1.1 in NAT full feature mode and ping outside host, then delete the set that contains the rule and ping it again.
44. [BUG FIX] Symptom: In centralized log, the format of IKE packets is incorrect.

Condition: During IKE process, ZyWALL will record all payload types of both sent and received packets. However in centralized log, all these payload information is lost.

45. [BUG FIX] Symptom: CI command "ip dns server" is hidden.
    Condition: Entering the following ci command "ip dns", the server command which should be opened is hidden.
46. [BUG FIX] Symptom: Default DNS server can't work.
    Condition: When a user set a static IP on wan and set DHCP = none on LAN setup, the default DNS server can't work and there is no way to set the default DNS server IP.
    Note: A new CI command "ip dns default <ip>" is used to change the default DNS server IP.
47. [BUG FIX] Symptom: mIRC "DCC SEND file" function can't work.
    Condition: Behind NAT router, when user tries to send a file by using mIRC DCC SEND function, the file transfer will not only succeed, but also will cause disconnection from mIRC server.
48. [BUG FIX] Symptom:
    1) Using ci command to set content filter registration will cause system crash
    2) Using ci command to set content filter block time of day will set wrong time value in ROM
    Condition:
    1) Enter the following four content filter registration ci commands "ip urlfilter reginfo name/eMail/country/clearall" will cause system crashed.
    2) Enter ci command "ip urlfilter category timeOfDay" will set wrong value of begin time and end time into ROM.
49. [BUG FIX] Symptom: content filtering doesn't apply after VPN
    Condition: ZyWALL supports a special application:
    ZW(branch)=====VPN=====ZW(HQ)------>Internet
    Internet access from branch office must go out through the VPN tunnel. Thus HQ can control the traffic from / to the branch office. However, content filter setting in HQ cannot control the traffic from branch through the VPN tunnel.
50. [BUG FIX] Symptom: IKE process does not check encapsulation.
    Condition: During IKE negotiation, responder only accepts initiator's encapsulation setting and do not compare the value with its own setting.
51. [BUG FIX] Symptom: CI command "ipsec switch on/off" did not work.
    Condition: CI command "ipsec switch on/off" cannot change the switch state.
52. [BUG FIX] Symptom: When “sys firewall dos ignore lan on”, traceroute failed.
    Condition: When “sys firewall dos ignore lan on”, there will no hop information showed.
53. [BUG FIX] Symptom: SMT menu 24.2.1 will not show correct system name.
    Condition: Once the user configures the system and domain name in SMT menu 1, SMT menu 24.1 will show the string which joins system name and domain, but SMT menu 24.2.1 just display the system name.

Modification in V3.52(WC.0)b1 | 09/03/2002

1. [ENHANCEMENT] Add keep-alive feature for IPSec. When the switch turns on, even no packets passed through the tunnel, ZyWALL will re-key automatically after SA lifetime times out.
2. [ENHANCEMENT] Add CNM support. CI command “cnm active 1” could be used to active this feature. The default is inactive. CI command “cnm managerIp xxx.xxx.xxx.xxx” is used to specify the IP address of the ZyXEL’s CNM management station. For details for CNM, please reference to the User Guide for CNM.
3. [ENHANCEMENT] Add Centralized LOG support. We added a new page “LOGS” in eWC to combine all LOGs from firewall, content filter, IPSec and error log into the same format.
4. [ENHANCEMENT] In content filter, users can modify the “Denied Access Message”. When it block one URL, ZyWALL will show this messages to the client.
5. [ENHANCEMENT] URL checking in content filter is enhanced. Now it can parse full URL path for blocking, and the URL checking can be case insensitive. We have added two CI commands to allow users to turn on these two features. They are “ip urlfilter customize actionFlags act5 enable / disable” and “ip urlfilter customize actionFlags act6 enable”. NOTE: Turns on these two features will enlarge search

load during content filter process and throughput will be impacted. The default values of them are both "disable".

6. [FEATURE CHANGE] Firewall page in eWC is totally changed. There are 4 directional ACL sets; For packets originating from LAN to LAN (ZyWALL included)/WAN, and from WAN to LAN/WAN (ZyWALL included).
7. [FEATURE CHANGE] Triangle route network topology is allowed. We added a CI command to switch on / off firewall checking for triangle route. It's "sys firewall ignore triangle all [on|off]". The default value is to ignore triangle route check.
8. [FEATURE CHANGE] Wording changed for IPSec address configuration in SMT27.1, SMT27.1.1 and WEB→IPSec.
9. [FEATURE CHANGE] In Many-One-to-One case, NAT sessions can be established by packets from WAN or LAN. In the past only those packets from LAN could establish NAT seesions.
10. [FEATURE CHANGE] CI command for netbios filter is revised. Now WAN-to-LAN traffic is controlled by LAN-to-WAN switch.
11. [BUG FIX] When ZyWALL receives TCP packets with both SYN and ACK bits are set, corresponding remote management service is no more available.
12. [BUG FIX] When the user setups the schedule to the block time of date, ZyWALL always block traffic matching "domain name.
13. [BUG FIX] Port setting in VPN rule cannot work.
14. [BUG FIX] Download CyberNOT list crash on passive mode.
15. [BUG FIX] Static route from LAN to LAN (IP alias segment) will be blocked by firewall.
16. [BUG FIX] Symptom: Dynamic VPN rule is not stable. ZyWALL may crashes. Condition: This symptom is observed when ZyWALL is configured one dynamic rule for serving multiple dynamic VPN SAs. This symptom occurs if ZyWALL receives a dynamic VPN request which local and remote host IP(phase 2 parameters) are checked to be the same with the current running VPN policy, ZyWALL may crash. The router should reject the connection without crash.
17. [BUG FIX] Symptom: Some special applications may not work behind ZyWALL's NAT function. Condition: This symptom is observed when NAT is enabled on ZyWALL. Some special applications have unusual TCP connect procedure. After TCP connection is established, a RESET followed re-connect steps right away will make the NAT session be deleted very quickly.
18. [BUG FIX] Symptom: PC on ZyWALL LAN cannot use any outbound packet via ZyWALL. Condition: Set ZyWALL block LAN to WAN NetBIOS and enable SMT 24.3.2 UNIX syslog to LinkLogger, run LinkLogger host lookup program, then PC ping ZyWALL will request time out.

Modification in V3.50(WC.4)b2 | 06/28/2002

1. [BUG FIX] When ZyWALL receives TCP packets with both SYN and ACK bits are set, corresponding remote management service is no more available.

Modification in V3.50(WC.4)b1 | 06/25/2002

1. [FEATURE CHANGE] WAN to LAN traffic is allowed in hard-coded netbios packet filter. We add one more CI command for users to control it. Please refer to appendix 4 for more information.
2. [FEATURE CHANGE] Web→WAN error messages changed when the gateway IP address was out of the range of subnet.
3. [FEATURE CHANGE] Triangle route network topology is allowed. We added a CI command to switch on / off firewall checking for triangle route. It's "sys firewall ignore triangle all [on|off]". The default value is to ignore triangle route check.
4. [FEATURE CHANGE] Wording changed for IPSec address configuration in SMT27.1, SMT27.1.1 and WEB→IPSec.
5. [BUG FIX] When the user setups the schedule to the block time of date, ZyWALL always block traffic matching "domain name".
6. [BUG FIX] Using telnet to connect to ZyWALL and stay in LOG display page, system rebooted if disconnected the telnet session.

7. [BUG FIX] CI command to configure trigger dial in netbios packet filter cannot work.
8. [BUG FIX] Port setting in VPN rule cannot work.
9. [BUG FIX] Download CyberNOT list crash on passive mode.
10. [BUG FIX] Clearing default server in WEB→SUA/NAT by entering non-ip string will leave that field containing incorrect numbers.
11. [BUG FIX] Clear multi-page VPN LOG, the log index will not reset.
12. [BUG FIX] Static route from LAN to LAN (IP alias segment) will be blocked by firewall.

Modification in V3.50(WC.3) | 06/17/2002

1. [FEATURE CHANGE] When the DHCP server doesn't response in busy state, ZyWALL will do much more retransmit.
2. [BUG FIX] Aggressive mode failed to work.

Modification in V3.50(WC.2) | 05/27/2002

1. [ENHANCEMENT] Support phase 2 ID: SINGLE / RANGE / SUBNET.
2. [ENHANCEMENT] Support using domain name as secure gateway address. We will periodically update peer IP according to the domain name. Two new CI commands are provided: "ipsec timer update_peer" and "ipsec updatePeerIp". The former is to set the interval for updating, and the latter is to force system update right away.
3. [ENHANCEMENT] Different rules can connect to the same secure gateway. However, there are some criteria for these rules, please refer to Appendix 2.
4. [ENHANCEMENT] Multiple dynamic rules are supported. There is no ordering issue for these dynamic rules.
5. [ENHANCEMENT] Web configurator can modify phase 1 algorithms through ADVANCE page.
6. [ENHANCEMENT] Add two CI commands : "ppp lcp echo time" and "ppp lcp echo retry" to control echo timer and retry counts. Set one of them to 0 will disable echo request.
7. [ENHANCEMENT] Add remote management for support SNMP and DNS.
8. [ENHANCEMENT] Some workarounds for "VPN route" are supported: After a packet is processed IPSec and going to be transmitted, it can be applied IPSec again. We provide CI commands to control which destination side can be applied IPSec. They are "ipsec route wan / lan".
9. [ENHANCEMENT] Add IPSec parser in CI command, "sys trcpacket parse".
10. [ENHANCEMENT] Add SNMP link UP / DOWN trap for channels.
11. [ENHANCEMENT] VPN LOG will show detail notify message type.
12. [ENHANCEMENT] Add 3rd DNS and WINS server for DHCP server option. We add two CI commands, <ip dhcp "iface name" server dnsserver> and <ip dhcp "iface name" server winsserver> to add server IP.
13. [ENHANCEMENT] Add a switch to control NAT IRC service turned on/off. We provide a new CI command "ip nat service irc <on|off>" to control the service.
14. [ENHANCEMENT] Send UNIX syslog for VPN LOG.
15. [ENHANCEMENT] Add new CI commands to filter netbios and broadcast packets. For netbios packets, they are "sys filter netbios". Please refer to Appendix 4 for detailed description. And for broadcast packets, they are "sys filter blockbc <on|off>". Broadcast packets will be applied here are DHCP packets and RIP packets.
16. [ENHANCEMENT] Add new CI commands to adjust MTU. For LAN side, it's "ether edit mtu" and for WAN side, it's "sys rn mtu". For more detailed description, please refer to Appendix 3.
17. [ENHANCEMENT] Add a new CI command, "ipsec display <rule index>" to display IPSec rules.
18. [ENHANCEMENT] Add a new CI command, "ipsec dial <rule index>" to trigger the IKE procedure.
19. [ENHANCEMENT] Add a new CI command, "ip nat incike <on|off>", to increase IKE source port. This is used in NAT pass-through.
20. [ENHANCEMENT] Add a new C/I command "sys firewall dos ignore <lan|wan|dmz> [on|off]". For example, user can bypass DoS attack checking on LAN by using "sys firewall dos ignore lan on"
21. [ENHANCEMENT] Hard coded netbios filters work with port 445, which used by Windows 2000/XP.

22. [FEATURE CHANGE] IPSec related SMT and WEB wording changed.
23. [FEATURE CHANGE] MyIP and secure gateway address can be set to 0.0.0.0 at the same time.
24. [FEATURE CHANGE] Support LAN IP as MyIP.
25. [FEATURE CHANGE] CI commands for ipsec such as “ipsec sa” and “ipsec sa_sdb_status” are removed. To show SA status, we provide CI command “ipsec show_runtime sa”.
26. [FEATURE CHANGE] Phase 1 SA will time out. And its lifetime is independent from phase 2 SA lifetime.
27. [FEATURE CHANGE] Ipsec-related CI commands are visible.
28. [FETURE CHANGE] Dynamic rules will not conflict with static rules. Static rules have higher priority, and will be chose during runtime IKE procedure.
29. [FEATURE CHANGE] The repeated entries showed in VPN LOG are reduced.
30. [FEATURE CHANGE] Content filter and VPN pages in WEB are modified.
31. [FEATURE CHANGE] Accept peer’s SA lifetime set to both SEC and KB.
32. [BUG FIX] Use PPPoE / PPTP connection: after disconnection and then dial up again, if ZyWALL get new WAN IP, NAT mapping still used old IP address.
33. [BUG FIX] During IKE process, if SMT tried to save or delete that rule, sometimes system crashed.
34. [BUG FIX] Using VPN tunnel to transfer large file, sometimes after a period there cannot be any traffic pass through the tunnel.
35. [BUG FIX] Fragmentation problems have been fixed, including teardrop, full feature NAT and ACL block.
36. [BUG FIX] When ZyWALL as RESPONDER, it will accept all PFS setting from INITIATOR and does not check its own configuration.
37. [BUG FIX] Notify message <No proposal chosen> has incorrect format.
38. [BUG FIX] PFS has race condition. When two peers start to re-key simultaneously, sometimes one side will reject the connection.
39. [BUG FIX] Packets to LAN should not match a rule whose remote IP range is "all".
40. [BUG FIX] Broadcast DHCP reply packets are blocked.
41. [BUG FIX] Enlarge memory parameters to assure there exists enough memory for system operation after VPN tunnels are built.
42. [BUG FIX] After enable SUA, remote management to LAN IP via VPN tunnel failed.
43. [BUG FIX] After long time test, IPSec process will cause system lack of memory.
44. [BUG FIX] Under PPPoE connection, tunnel is built but no traffic can pass through it.
45. [BUG FIX] "ip nat reset enif1" don't work.
46. [BUG FIX] Firewall will check back-record for the TRACEROUTE reply to port unreachable of ICMP at the end host.
47. [BUG FIX] Static routed packets from LAN to LAN will be blocked by firewall.
48. [BUG FIX] Solve the SNMPv1 vulnerability problem.
49. [BUG FIX] Sometimes packets cannot pass through tunnel built from dynamic rule.
50. [BUG FIX] Routing cache calculation will overflow.
51. [BUG FIX] Manual key cannot swap from one rule to another, if these two rules have the same secure gateway.
52. [BUG FIX] When two peers initiate connections at the same time in some special cases, the two peers will reject each other and on tunnel can be established.
53. [BUG FIX] When building the tunnel, sometimes system will crash.

Modification in V3.50(WC.1) | 12/18/2001

1. [ENHANCEMENT] When phase 2 id check fails, VPN LOG will show both peer ID information and system setting.
2. [FEATURE CHANGE] Add CLI support.
3. [FEATURE CHANGE] SMT24.7 wording changed.
4. [FEATURE CHANGE] In SMT27.1, "EDIT" will jump to the selected rule automatically
5. [BUG FIX] When using PPPoE encapsulation and turning on firewall, system is very unstable and it may crash.

6. [BUG FIX] When there are two active IPSEC rules with the same secure gateway, packets which should match the latter rule will still use the former rule for IKE process. In some cases, this will cause system to establish many invalid tunnels for one rule. At last, system does not have enough memory.
7. [BUG FIX] When encapsulation switches from Ethernet to PPPoE, IP Alias 2 will become “not available”.
8. [BUG FIX] Opera 6.0 cannot login eWC.
9. [BUG FIX] IP Alias cannot fake MAC address in SMT2 and WEB.
10. [BUG FIX] When firewall turned on, received a invalid AH packet (protocol 51) from LAN will cause ZyWALL crashed
11. [BUG FIX] Remove incorrect tag in WEB→WAN→PPPoE / PPTP
12. [BUG FIX] Smartbit test with 1 VPN tunnel cause ZyWALL crashed.
13. [BUG FIX] Typing “atgo” in debug mode, the restore default romfile ping didn’t work.
14. [BUG FIX] WEB: When modifying a used custom port, it will not apply to the rule using this custom port. If trying to remove the custom port from that rule, ZyWALL will crash.
15. [BUG FIX] After IKE re-keying procedure, some memory doesn’t be freed. After a long term test, system will have no free memory section.

Modification in V3.50(WC.0) | 12/04/2001

1. [ENHANCEMENT] Add a new CI command “ipsec show_runtime sa” to show runtime phase 1 and phase2 SA information.
2. [ENHANCEMENT] Manual key SA will runtime creates when traffic matches SPD.
3. [ENHANCEMENT] SA monitor will show manual key SA, and command to delete it is available.
4. [ENHANCEMENT] Idle timer also applies on manual key SA. When no traffic transmits through the SA, system will delete it.
5. [ENHANCEMENT] VPN LOG is totally revised. Now it will show all IKE packets information. Besides, It will show error messages to identify the reason why connection cannot be built.
6. [ENHANCEMENT] IKE process in phase 2 will check ID information between system and the peer. If they don’t match, i.e. both sites have different local / remote Addr setting, system will reject the connection and log in the VPN LOG.
7. [ENHANCEMENT] Simultaneous SA check: All VPN rules can be set to “ACTIVE”, but only 50 runtime SA can be established at the same time.
8. [FEATURE CHANGE] Only the last rule (rule 60)can apply security gateway to “0.0.0.0”.
9. [FEATURE CHANGE] Web (SUA/NAT) default DMZ server changes to default server.
10. [FEATURE CHANGE] Web status after saving configuration has changed to “Configuration updated successfully”.
11. [FEATURE CHANGE] Put default PPTP settings(my PPTP IP and PPTP server IP) on Wizard.
12. [BUG FIXED] Cannot use IPSec tunnel for remote management.
13. [BUG FIXED] Remove non-configured filter set from remote node.
14. [BUG FIXED] Fix incorrect help page link in WEB.
15. [BUG FIXED] SMT 24.11 fail to control connections from WAN using LAN alias IP addresses.
16. [BUG FIXED] When firewall turns off and SUA only, PC in the WAN side can ping PCs in the LAN side.
17. [BUG FIXED] When the WAN side is using PPPoE connection and NAT turns off, firewall does not protect the LAN side.
18. [BUG FIXED] When the WAN side is using PPPoE connection, LAN-to-WAN ACL rule will not be applied. The Packet will transmit through firewall from LAN to WAN, even existing a firewall rule to block it.
19. [BUG FIXED] Web (Content filter→ EXEMPT ZONE) Apply button didn’t work.
20. [BUG FIXED] VPN connection cannot be re-built after dynamic WAN IP being changed.
    →When one ZyWALL has “Secure Gateway IP Addr” to be "0.0.0.0" and the other one has “My IP Addr” to be "0.0.0.0", as below.

ZyWALL 1 (security gateway IP 0.0.0.0) <--------- ZyWALL 2 (my IP 0.0.0.0)

If ZyWALL 2 has been configured as "dynamic WAN IP", the VPN tunnel between ZyWALL 1 and ZyWALL 2 can be established at the first time. However, if ZyWALL 2 has its WAN ip changed, the VPN tunnel cannot be re-built again.

→Fix:

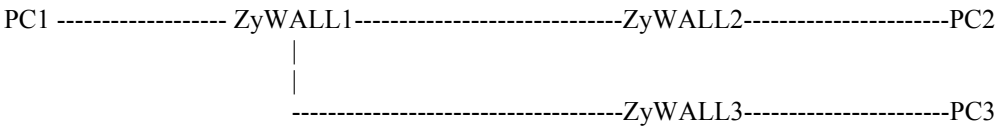
1) For the role of ZyWALL2, it periodically checks WAN IP, as long as IP changes, system will auto-disconnect tunnel. This will be logs in VPN Logs.
2) For the role of ZyWALL1, it periodically checks if any runtime SA has no traffic for a long time. If a SA has no traffic through it in 2 minutes, system will disconnect the tunnel.
3) There are two new CI commands to configure 1) and 2). They are "ipsec timer chk_my_ip" and "ipsec timer chk_conn"
4) For the role of ZyWALL1, security gateway IP setting to be 0.0.0.0 can receive multiple requests at the same time. Appendix 1 is a simple configuration example.

21. [BUG FIXED] VPN timeout re-connection function is not robust.
    → When "SA Life time" is time out, sometimes the VPN tunnel cannot be re-established again.
22. [BUG FIXED] VPN tunnel cannot be established if WAN IP is static without default gateway configured.
    →When a ZyWALL is configured as "static IP" but default gateway as "0.0.0.0", and the other ZyWALL is placed in the same subnet, the VPN tunnel cannot be established between them.
23. [BUG FIXED] VPN tunnel cannot work with multi-NAT.
24. [BUG FIXED] Use Web setup VPN for manual mode, it can not work until save in SMT again
25. [BUG FIXED] Web (Firewall) will show error messages when try to access help pages.
26. [BUG FIXED] When phase 2 SA life time out, sometimes there exists a phase 1 SA and no tunnel can be built.
27. [BUG FIXED] IPSEC pass through cannot support multiple sessions.
28. [BUG FIXED] NAT loopback server problem is solved. When a server in the LAN site and there exists a NAT server set directed to it, WAN site traffic can access the WAN IP, then be redirected to the server. But the LAN site cannot use the WAN IP to access the server. It only can access the server through LAN IP. A new CI command "`ip nat loopback`" is added to turn on the feature, "NAT server loopback". When it turns on, PC on LAN site can access the LAN site server through WAN IP. NOTE: Turn on the feature will cause throughput decreased.
29. [BUG FIXED] POP3(TCP:110) didn't show on firewall pre-configured port.
30. [BUG FIXED] When VPN LOG recorded more than 64 entries, it will show incorrect format.
31. [BUG FIXED] Responder cannot find phase1 SA by address pair. This will cause sometimes phase 1 SA will remain after SA reconnection
32. [BUG FIXED] Web VPN LOG format corrected.
33. [BUG FIXED] When receive deleting phase 1 packet, system will only delete phase 1 SA and let an useless phase2 SA alive. This will cause a long delay to reconnection.
34. [BUG FIXED] Wrong wording in content filter log.
35. [BUG FIXED] Time initialized won't show in the content filter and firewall logs.
36. [BUG FIXED] In firewall log mail, the header contained wrong date display.
37. [BUG FIXED] IPALIAS didn't apply firewall LAN-to-WAN ACL rules.
38. [BUG FIXED] Web configurator (VPN / Content filter) cannot be accessed by Netscape 4.78
39. [BUG FIXED] In b6, Web configurator (WAN→PPPoE / PPTP) will cause system crashed
40. [BUG FIXED] With PPPoE / PPTP configured, but no dial-up, system would crash after typing "ip ro st" in CI command mode.
41. [BUG FIXED] DNS proxy can't get the address when the original DNS server failed.
42. [BUG FIXED] In debug mode, command "atgo" will cause RAS to restore default romfile.
43. [BUG FIXED] After PPTP connection built, system would crash.
44. [BUG FIXED] When SNMP query through the system, it would crash.
45. [BUG FIXED] IPAlias couldn't work.
46. [BUG FIXED] In SMT 24.6, interrupt the upload procedure would cause system crashed.
47. [BUG FIXED] Web (WAN→MAC): if MAC spoofing is active, change configuration back to "factory default" will not apply at the same time. System must be reboot to make change done.

48. [BUG FIXED] After applying MAC spoofing, both WAN and LAN MAC will be changed to be the same as PC.
49. [BUG FIXED] Content filter cannot get the list.
50. [BUG FIXED] Content filter configuration behavior modified. Configuration changes will not be saved unless press the “apply” button. “Reset” button will clear all configuration changes and reload the page.
51. [BUG FIXED] System hanged during smart-bit testing (100M ←→100M).
52. [FEATURE CHANGE] When system crashes, it will not stop in the screen. Instead after showing memory dump, system will reboot automatically.
53. [ENHANCEMENT] In firewall setup, IKE (UDP:500) is placed in standard protocol instead of custom port. Default romfile changed.
54. [ENHANCEMENT] VPN logs and debug messages were modified to be much readable.
55. [ENHANCEMENT] When dynamic WAN-IP changes, system will disconnect all VPN connections which MyIP is “0.0.0.0”.
56. [ENHANCEMENT] When VPN connection has no traffic through it for a period, it will disconnect automatically.
57. [ENHANCEMENT] Add two new CI commands in “ipsec timer” to configure VPN timers.
58. [BUG FIXED] SMT 27.1.1.1 pre-shared key check error.
59. [ENHANCEMENT] Enhanced Ethernet driver.
60. [ENHANCEMENT] Enhanced firewall stability.
61. [BUG FIXED] Restore default romfile can not work in V3.50(WC.0)b4.
62. [BUG FIXED] When DHCP server and DHCP relay exist in the same network providing ZyWALL50 IP address, saving configuration will not be correct.
63. [BUG FIXED] Content filter keyword blocking didn’t work.
64. [ENHANCEMENT] System stability enhanced.
65. [BUG FIXED] System crashed by unusual IKE message.
66. [BUG FIXED] Fix IPSec configuration bugs.
67. [BUG FIXED] Debug messages removed.
68. [ENHANCEMENT] Speed up flesh writing process.
69. [BUG FIXED] IPSec rule name disappear.
70. [BUG FIXED] Console login didn’t kick out web configurator.
71. [BUG FIXED] Debug messages removed.
72. [BUG FIXED] When use web to configure IPSEC, system crashed.
73. [BUG FIXED] When use web to move firewall rules, system crashed.
74. [BUG FIXED] When use web to configure Content Filter, system crashed.
75. [BUG FIXED] VPN failed when transmitting large packets.
76. [BUG FIXED] SA monitor was incorrect.
77. [ENHANCEMENT] System stability enhanced.
78. [ENHANCEMENT] Add support for reset button (restore default romfile).

Appendix:

1. Example for configuring security gateway to be 0.0.0.0.



SMT27.1.1 of ZyWALL1:

```
                    Menu 27.1.1 - IPSec Setup

Index #= 10         Name= ZyWALL1
Active= Yes

My IP Addr= 4.4.4.254
Secure Gateway IP Addr= 0.0.0.0
Protocol= 0
Local:       Addr Type= RANGE
           IP Addr Start= 1.1.1.1             End= 1.1.1.50
              Port Start= 0                   End= N/A
Remote:      Addr Type= N/A
           IP Addr Start= N/A                 End= N/A
              Port Start= N/A                  End= N/A
Enable Replay Detection= No
Key Management= IKE
Edit Key Management Setup= N/A

            Press ENTER to Confirm or ESC to Cancel:
```

SMT27.1 of ZyWALL1 will show:

```
                          Menu 27.1 - IPSec Summary

#      Name    A   Local Addr Start  - Local Addr End   Encap.  IPSec Algorithm
     Key Mgt        Remote Addr Start - Remote Addr End           Secure Gw Addr
--- ---------- - ----------------   ----------------- ------ ----------------
001 ZyWALL1     Y    1.1.1.1             1.1.1.50      Tunnel   ESP DES-SHA1
      IKE              N/A                 N/A                    0.0.0.0
002

003

004

005


             Select Command=  None          Select Rule=  N/A

                   Press ENTER to Confirm or ESC to Cancel:
```

SMT27.1.1. of ZyWALL2:

```
                        Menu 27.1.1 - IPSec Setup

         Index #= 1        Name= ZyWALL2
         Active= Yes

         My IP Addr= 4.4.4.1
         Secure Gateway IP Addr= 4.4.4.254
         Protocol= 0
         Local:          Addr Type= RANGE
                      IP Addr Start= 3.3.3.1            End= 3.3.3.100
                     Port Start= 0                     End= N/A
         Remote:         Addr Type= RANGE
                      IP Addr Start= 1.1.1.1            End= 1.1.1.50
                     Port Start= 0                     End= N/A
         Enable Replay Detection= No
         Key Management= IKE
         Edit Key Management Setup= N/A

                    Press ENTER to Confirm or ESC to Cancel:
```

After connection built successfully, the SA Monitor in ZyWALL1 will show:

```
                        Menu 27.2 - SA Monitor

#             Name                                  Encap.    IPSec ALgorithm
--- ------------------------------------------- -------- ---------------
1   ZyWALL1    : 3.3.3.1 - 3.3.3.100              Tunnel      ESP DES-SHA1
2
3
4
5
6
7
8
9
10

                  Select Command= Refresh
                  Select Connection= N/A

                  Press ENTER to Confirm or ESC to Cancel:
```

What follows the Name is the runtime "Remote IP Addr" linking with the dial-in user. Since there will be a lot of users match the rule named "ZyWALL1", we use "Remote IP Addr" to distinguish them and selecting one of them to delete will not affect others. However, for the rule whose security gateway is not 0.0.0.0, we can use names to distinguish them, so their Remote IP Addr will not be showed.

NOTE:

1) Only IKE supports secure gateway to be 0.0.0.0. Manual key does not.
2) For ZyWALL 2 and ZyWALL3, their "Local IP Addr" will become the "Remote IP Addr" in ZyWALL1's runtime SPD, so they should not overlap, or ZyWALL1 will be confused which route is correct. If this IP conflict happens, IKE procedure will fail and will log in the VPN Logs.
3) Also for ZyWALL2 and ZyWALL3, their "Remote IP Addr" should match the "Local IP Addr", or the runtime SPD check will fail.
4) For the rule whose security gateway is 0.0.0.0, it only can be "responder". In other words, it can NOT initiate a connection. It only can receive others' IKE request to build the tunnel.

2. Criteria of multiple rules connect to the same secure gateway.

For initiator, there is no problem. We can get the right rule by SPD. However, for responder, we have little information during IKE procedure to identify these different rules. We will use the first rule to receive the IKE packet, and use its SA payload and ID payload to swap from one rule to another.

For responder, there will be some criteria for IKE swap from one rule to another:

1) These rules MUST have the same secure gateway and the same negotiation mode.
2) If finding different phase 1 algorithms, IKE procedure can swap from one rule to another
3) Only with the same phase 1 algorithms, the same pre-shared key, but different phase 2 algorithms, IKE procedure can swap from one to another.
4) Only with the same phase 1 algorithms, the same pre-shared key, the same phase 2 algorithms, but not the same phase 2 ID, IKE procedure can swap from one to the other.

3. Procedure to set MTU for LAN and WAN.

The procedure to set MUT is load parameter first, set MTU, and then save them back.

1) For LAN:
   ether edit load 1
   ether edit mtu <value>
   ether edit save

2) For WAN:
   sys rn load 1
   sys rn mtu <value>
   sys rn save

4. Hard-coded packet filter for "NetBIOS over TCP/IP"

The new set C/I commands are under "sys filter netbios" sub-command.
There are two CI commands:

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

Example output:

```
================ NetBIOS Filter Status ================
  LAN to WAN:       Block
  WAN to LAN:       Block
  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	Block
1	WAN to LAN	Block
6	IPSec pass through	Forward
7	Trigger dial	Disabled

Example commands:

```
sys filter netbios config 0 on      => block LAN to WAN NB/IP packets
sys filter netbios config 1 off     => forward WAN to LAN NB/IP packets
sys filter netbios config 6 on      => block IPSec NB/IP packets
sys filter netbios config 7 off     => disable trigger dial
```

5. Static Route Application Note

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 static route.

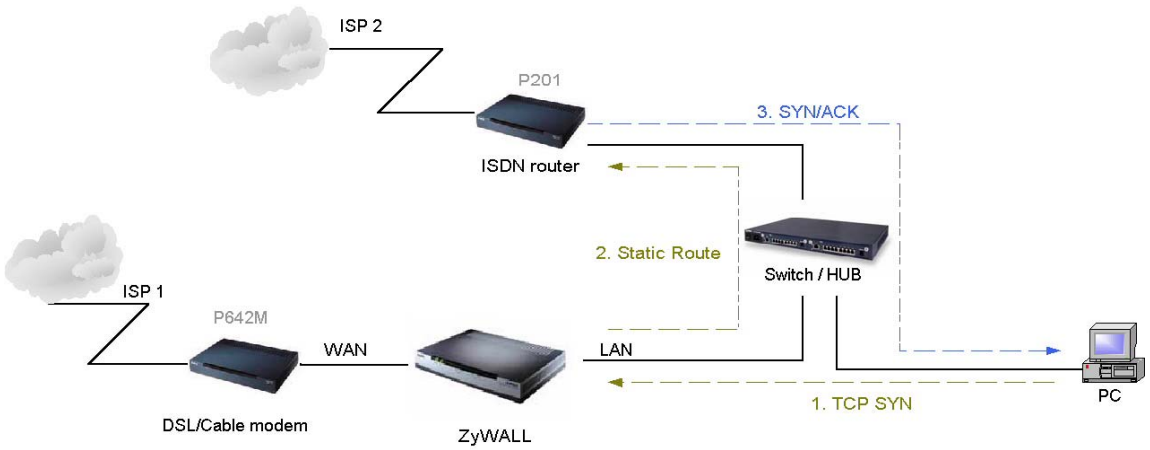


Figure 5-1 Triangle Route

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

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

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

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

How static route works under protection - Solutions

(1) Gateway on alias IP network

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

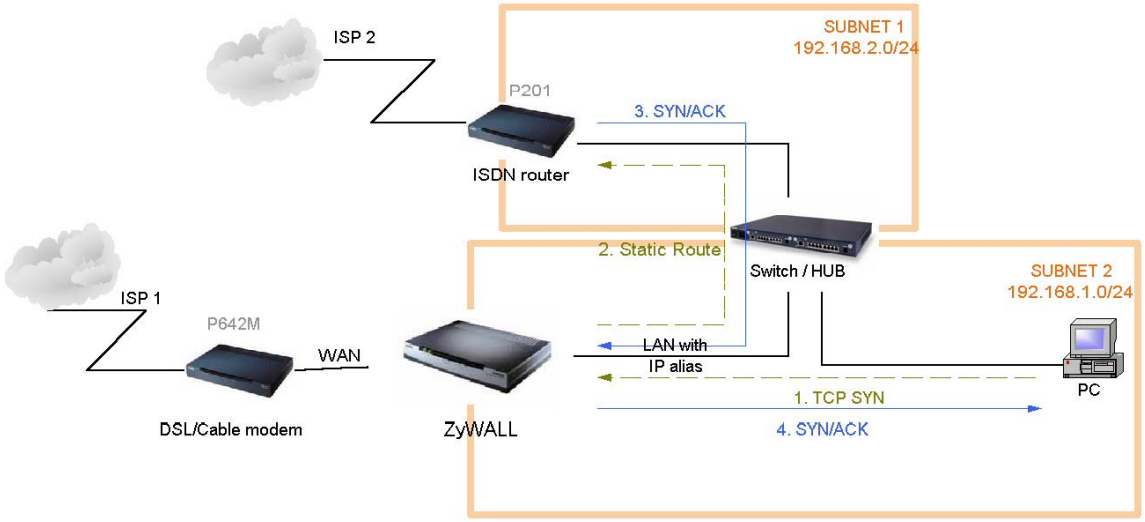


Figure 5-2 Gateway on alias IP network

(2) Gateway on WAN side

A working topology is suggested as below.

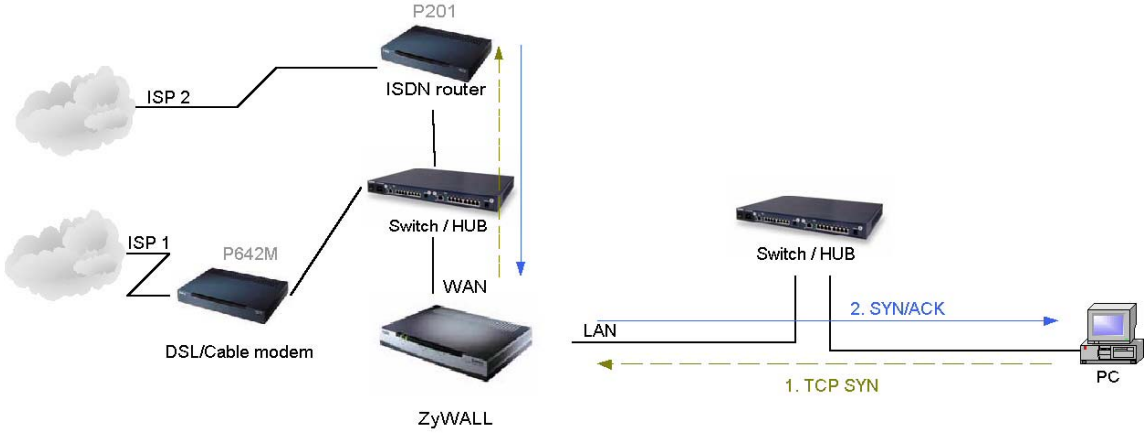


Figure 5-3 Place other gateways on WAN side

6. Appendix 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 or 0.0.0.0	My WAN IP	My WAN IP
0.0.0.0	a.b.c.d (NOT 0.0.0.0)	My WAN IP	a.b.c.d
a.b.c.d (not 0.0.0.0)	*blank or 0.0.0.0	a.b.c.d	a.b.c.d
a.b.c.d (not 0.0.0.0)	e.f.g.h (NOT 0.0.0.0)	a.b.c.d	e.f.g.h

*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 or 0.0.0.0	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 (NOT 0.0.0.0)	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 or 0.0.0.0, 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 or 0.0.0.0, 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 or 0.0.0.0, 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 such a kind of rule in top of rule list, it may be matched first. To avoid this problem, we will enhance it in the future.

Command Class List Table		
System Related Command	Exit Command	Ethernet Related Command
IP Related Command	IPSec Related Command	Firewall Related Command

System Related Command Home

Command				Description
sys				
	adjtime			retrive date and time from Internet
	callhist			
		display		display call history
		remove	<index>	remove entry from call history
	countrycode		[countrycode]	set country code
	date		[year month date]	set/display date
	domainname			display domain name
	edit		<filename>	edit a text file
	extraphnum			maintain extra phone numbers for outcalls
		add	<set 1-3> <1st phone num> [2nd phone num]	add extra phone numbers
		display		display extra phone numbers
		node	<num>	set all extend phone number to remote node <num>
		remove	<set 1-3>	remove extra phone numbers
		reset		reset flag and mask
	feature			display feature bit
	hostname		[hostname]	display system hostname
	logs			
		category		
			access [0:none/1:log]	record the access control logs
			attack [0:none/1:log/2:alert/3:both]	record and alert the firewall attack logs
			display	display the category setting
			error [0:none/1:log/2:alert/3:both]	record and alert the system error logs
			ipsec [0:none/1:log]	record the access control logs
			javablocked [0:none/1:log]	record the java etc. blocked logs
			mten [0:none/1:log]	record the system maintenance logs
			upnp [0:none/1:log]	record upnp logs
			urlblocked [0:none/1:log/2:alert/3:both]	record and alert the web blocked logs
			urlforward [0:none/1:log]	record web forward logs
		clear		clear log
		display		display all logs
		errlog		
			clear	display log error

			disp	clear log error
			online	turn on/off error log online display
		load		load the log setting buffer
		mail		
			alertAddr [mail address]	send alerts to this mail address
			display	display mail setting
			logAddr [mail address]	send logs to this mail address
			schedule display	display mail schedule
			schedule hour [0-23]	hour time to send the logs
			schedule minute [0-59]	minute time to send the logs
			schedule policy [0:full/1:hourly/2:daily/3:weekly/4:none]	mail schedule policy
			schedule week [0:sun/1:mon/2:tue/3:wed/4:thu/5:fri/6:sat]	weekly time to send the logs
			server [domainName/IP]	mail server to send the logs
			subject [mail subject]	mail subject
		save		save the log setting buffer
		syslog		
			active [0:no/1:yes]	active to enable unix syslog
			display	display syslog setting
			facility [Local ID(1-7)]	log the messages to different files
			server [domainName/IP]	syslog server to send the logs
	rn			
		load	<entry no.>	load remote node information
		disp	<entry no.>(0:working buffer)	display remote node information
		nat	<none|sua|full_feature>	config remote node nat
		nailup	<no|yes>	config remote node nailup
		mtu	<value>	set remote node mtu
		save	[entry no.]	save remote node information
	stdio		[second]	change terminal timeout value
	time		[hour [min [sec]]]	display/set system time
	trcdisp	parse, brief, disp		monitor packets
	trclog			
	trcpacket			
	version			display RAS code and driver version
	view		<filename>	view a text file
	wdog			
		switch	[on|off]	set on/off wdog
		cnt	[value]	display watchdog counts value: 0-34463
	romreset			restore default romfile
	pwderrtm			set error password timeout value
	socket			display system socket information
	filter			
		netbios		

	roadrunner			
		debug	<level>	enable/disable roadrunner service 0: diable <default> 1: enable
		display	<iface name>	display roadrunner information iface-name: enif0, wanif0
		restart	<iface name>	restart roadrunner
	ddns			
		debug	<level>	enable/disable ddns service
		display	<iface name>	display ddns information
		restart	<iface name>	restart ddns
		logout	<iface name>	logout ddns
	cpu			
		display		display CPU utilization

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
			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
	edit			
		load	<ether no.>	load ether data from spt
		mtu	<value>	set ether data mtu
		save		save ether data to spt

IP Related Command Home

Command				Description
ip				
	address		[addr]	display host ip address
	alias		<iface>	alias iface
	aliasdis		<0|1>	disable alias
	arp			
		status	<iface>	display ip arp status
	dhcp		<iface>	
		client		
			release	release DHCP client IP

			renew	renew DHCP client IP
		status	[option]	show dhcp status
	dns			
		query		
		server	<primary> [secondary] [third]	set dns server
		stats		
			Clear	clear dns statistics
			Disp	display dns statistics
		default	<ip>	Set default DNS server
	httpd			
	icmp			
		status		display icmp statistic counter
		discovery	<iface> [on|off]	set icmp router discovery flag
	ifconfig		[iface] [ipaddr] [broadcast <addr> |mtu <value>|dynamic]	configure network interface
	ping		<hostid>	ping remote host
	route			
		status	[if]	display routing table
		add	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add route
		addiface	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add an entry to the routing table to iface
		addprivate	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add private route
		drop	<host addr> [/<bits>]	drop a route
	smtp			
	status			display ip statistic counters
	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
	xparent			
		join	<iface1> [<iface2>]	join iface2 to iface1 group

		break	<iface>	break iface to leave ipxparent group
	urlfilter			
		reginfo		
			display	display urlfilter registration information
			name	set urlfilter registration name
			eMail <size>	set urlfilter registration email addr
			country <size>	set urlfilter registration country
			clearAll	clear urlfilter register information
		category		
			display	display urlfilter category
			webFeature [block/nonblock] [activex/java/cookei/webproxy]	block or unblock webfeature
			logAndBlock [log/logAndBlock]	set log only or log and block
			blockCategory [block/nonblock] [all/type(1-14)]	block or unblock type
			timeOfDay [always/hh:mm] [hh:mm]	set block time
			clearAll	clear all category information
		listUpdate		
			display	display listupdate status
			actionFlags [yes/no]	set listupdate or not
			scheduleFlag [pending]	set schedule flag
			dayFlag [pending]	set day flag
			time [pending]	set time
			clearAll	clear all listupdate information
		exemptZo ne		
			display	display exemptzone information
			actionFlags [type(1-3)][enable/disable]	set action flags
			add [ip1] [ip2]	add exempt range
			delete [ip1] [ip2]	delete exempt range
			clearAll	clear exemptzone information
		customize		
			display	display customize action flags
			actionFlags [filterList/disableAllExceptT rusted/unblockRWFToTruste d/keywordBlock/fullPath/cas eInsensitive/fileName][enabl e/disable]	set action flags
			logFlags [type(1-3)][enable/disable]	set log flags
			add [string] [trust/untrust/keyword]	add url string
			delete [string] [trust/untrust/keyword]	delete url string
			clearAll	clear all information
		ftplist		update cyber list data
		listServerI P	<ipaddr>	set list server ip

		listServer Name	<name>	set list server name
	tredir			
		failcount	<count>	set tredir failcount
		partner	<ipaddr>	set tredir partner
		target	<ipaddr>	set tredir target
		timeout	<timeout>	set tredir timeout
		checktime	<period>	set tredir checktime
		active	<on|off>	set tredir active
		save		save tredir information
		disp		display tredir information
		debug	<value>	set tredir debug value
	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

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
		lan	<on|off>	After a packet is IPSec processed and will be sent to LAN side, this switch is to control if this packet can be applied IPSec again.
				Remark: Command available since 3.50(WA.3)
		wan	<on|off>	After a packet is IPSec processed and will be sent to WAN side, this switch is to control if this packet can be applied IPSec again.
				Remark: Command available since 3.50(WA.3)
	show_runtime	sa		display runtime phase 1 and phase 2 SA information
		spd		When a dynamic rule accepts a request and a tunnel is established, a runtime

				SPD is created according to peer local IP address. This command is to show these runtime SPD.
	switch	<on|off>		As long as there exists one active IPSec rule, all packets will run into IPSec process to check SPD. This switch is to control if a packet should do this. If it is turned on, even there exists active IPSec rules, packets will not run IPSec process.
	timer	chk_my_ip	<1~3600>	- Adjust timer to check if WAN IP in menu is changed
				- Interval is in seconds
				- Default is 10 seconds
				- 0 is not a valid value
		chk_conn.	<0~255>	- Adjust auto-timer to check if any IPsec connection has no traffic for certain period. If yes, system will disconnect it.
				- Interval is in minutes
				- Default is 2 minuets
				- 0 means never timeout
		update_peer	<0~255>	- Adjust auto-timer to update IPSec rules which use domain name as the secure gateway IP.
				- Interval is in minutes
				- Default is 30 minutes
				- 0 means never update
				Remark: Command available since 3.50(WA.3)
	updatePeerIp			Force system to update IPSec rules which use domain name as the secure gateway IP right away.
				Remark: Command available since 3.50(WA.3)
	dial	<rule #>		Initiate IPSec rule <#> from ZyWALL box
				Remark: Command available since 3.50(WA.3)
	display	<rule #>		Display IPSec rule #
	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
		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
		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
			preShareKey <string>	Set pre shared key in phase 1 in IKE
			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

Firewall Related Command Home

Command				Description
sys	Firewall			
		acl		
			disp	Display specific ACL set # rule #, or all ACLs.
		active	<yes|no>	Active firewall or deactivate firewall
		cnt		

			disp	Display firewall log type and count.
			clear	Clear firewall log count.
		pktdump		Dump the 64 bytes of dropped packet by firewall
		update		Update firewall
		dynamicrul e		
		tcprst		
			rst	Set TCP reset sending on/off.
			rst113	Set TCP reset sending for port 113 on/off.
			display	Display TCP reset sending setting.
		icmp		
		dos		
			smtp	Set SMTP DoS defender on/off
			display	Display SMTP DoS defender setting.
			ignore	Set if firewall ignore DoS in lan/wan/dmz/wlan
		ignore		
			dos	Set if firewall ignore DoS in lan/wan/dmz/wlan
			triangle	Set if firewall ignore triangle route in lan/wan/dmz/wlan