ZyXEL ZyWALL 10 Standard Version 3.50(WA.2) Release Note

Date: December 27, 2001

Supported Platforms:

ZyXEL ZyWALL 10

Note:

1. Using FTP to upload firmware from V3.2x to V3.5x is not supported. It is because the V3.5x firmware size is bigger than memory allocation for firmware uploading in V3.2x. Instead firmware upload through TFTP or Console is suggested.
2. Using FTP or Web to upload firmware from V3.50(WA.1) to V3.50(WA.2) is not supported, either. It is also because the latter's firmware size is bigger. To avoid this problem happens again, from V3.50(WA.2), we have modified the firmware upload procedure. When uploading firmware, we will not use "pre-defined memory allocation" any more. On the contrary, we will use whole available memory to do firmware upload. In this case, as long as there is enough free memory, user can upload firmware by FTP.
3. Using Web to configure VPN, the phase 1 algorithms have been fixed to DES + MD5. If other algorithms are preferred, please use SMT to configure them.
4. When firewall turns from "off" to "on", the firewall initialization procedure will disconnect all connections running through the ZyWALL.

Known Bugs:

1. Content Filter does not block cookies.

Features:

Modification in V3.50(WA.2) | 12/27/2001

1. [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.
2. [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.
3. [ENHANCEMENT] Manual key SA will runtime creates when traffic matches SPD.
4. [ENHANCEMENT] SA monitor will show manual key SA, and command to delete it is available.
5. [ENHANCEMENT] Idle timer also applies on manual key SA. When no traffic transmits through the SA, system will delete it.

6. [FEATURE CHANGE] Multi-NAT "Many-to-many non overload" will use static mapping between IGA and ILA. In other words, it becomes "Many one-to-one".
7. [FEATURE CHANGE] SMT24.7 wording changed.
8. [FEATURE CHANGE] In SMT27.1, "EDIT" will jump to the selected rule automatically
9. [FEATURE CHANGE] Web status after saving configuration has changed to "Configuration updated successfully".
10. [FEATURE CHANGE] Web (SUA/NAT) default DMZ server changes to default server.
11. [FEATURE CHANGE] Simultaneous SA check: All VPN rules can be set to "ACTIVE", but only 10 runtime SA can be established at the same time.
12. [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.
13. [BUG FIXED] POP3(TCP:110) didn't show on firewall pre-configured port.
14. [BUG FIXED] Wrong wording in content filter log.
15. [BUG FIXED] "Time initialized" won't show in the content filter and firewall logs.
16. [BUG FIXED] In firewall log mail, the header contained wrong date display.
17. [BUG FIXED] IP Alias didn't apply firewall LAN-to-WAN ACL rules.
18. [BUG FIXED] When VPN LOG recorded more than 64 entries, it will show incorrect format.
19. [BUG FIXED] Responder cannot find phase1 SA by address pair. This will cause sometimes phase 1 SA will remain after SA reconnection
20. [BUG FIXED] Web VPN LOG format corrected.
21. [BUG FIXED] When receiving deleting phase 1 packet, system will only delete phase 1 SA and let a useless phase2 SA alive. This will cause a long delay to reconnection.
22. [BUG FIXED] Firewall alert mail didn't have correct format.
23. [BUG FIXED] 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.
24. [BUG FIXED] When encapsulation switches from Ethernet to PPPoE, IP Alias 2 will become "not available".
25. [BUG FIXED] IPSEC pass through didn't support multiple sessions.
26. [BUG FIXED] When primary DNS is not accessible, ZyWALL would switch to secondary DNS. However, When the secondary DNS failed, ZyWALL didn't check the primary DNS again.
27. [BUG FIXED] If there exist multiple custom ports and above 4 rules use these ports, the display format in rule summary was incorrect.
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] 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.
30. [BUG FIXED] IP Alias address cannot fake MAC address in SMT2 and WEB.
31. [BUG FIXED] When firewall turned on, received a invalid AH packet (protocol 51) from LAN will cause ZyWALL crashed
32. [BUG FIXED] Opera 6 cannot login WEB.
33. [BUG FIXED] In content filter, if the WEB site in trusted domain use "POST" instead of "GET", ZyWALL will still treat it as un-trusted site.
34. [BUG FIXED] When there exist a telnet session on "VIEW LOG" page, such as error log, firewall log or VPN log, login from console will cause system rebooted.
35. [BUG FIXED] When SA time out and reconnect, sometimes system will not free corresponding memory correctly. After a long connection, system will be exhausted.
36. [BUG FIXED] When phase 2 SA life time out, sometimes there exists a phase 1 SA and no tunnel can be built.
37. [BUG FIXED] Using Web to upgrade firmware, system will reply "internal error".
38. [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.

39. [BUG FIXED] VPN tunnel cannot be established if WAN IP is static without default gateway configured.
    →When a ZyWALL 10 / P312 is configured as "static IP" but default gateway as "0.0.0.0", and the other ZyWALL 10 / P312 is placed in the same subnet, the VPN tunnel cannot be established between them.
40. [BUG FIXED] VPN tunnel cannot work with multi-NAT.
41. [BUG FIXED] Use Web setup VPN for manual mode, it can not work until save in SMT again
42. [BUG FIXED] Web (Content filter→ EXEMPT ZONE) Apply button didn't work.
43. [BUG FIXED] VPN connection cannot be re-built after dynamic WAN IP being changed.
    →When one ZyWALL / P312 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.

Modification in V3.50(WA.1) | 11/06/2001
1. [BUG FIXED] When firewall turns off and SUA only, PC in the WAN side can ping PCs in the LAN side.
2. [BUG FIXED] When the WAN side is using PPPoE connection and NAT turns off, firewall does not protect the LAN side.
3. [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.

Modification in V3.50(WA.0) | 10/15/2001
1. [BUG FIXED] content filter register error
2. [BUG FIXED] content filter list download error
3. [BUG FIXED] ESP teardrop attack parser error
4. [BUG FIXED] DNS lookup fail when menu 3.2 "DHCP server == None"
5. [BUG FIXED] Fix SNMPv2 packet make router reboot
6. [BUG FIXED] Fix Router crash when doing reconfiguration
7. [BUG FIXED] Fix cannot upload firmware by web
8. [BUG FIXED] Fix Firewall web configuration make buffer overflow
9. [BUG FIXED] Fix ip traceroute cannot work
10. [BUG FIXED] Fix web configuration cannot reset to factory default
11. [BUG FIXED] Fix web configuration cannot add more than one rule in firewall
12. [BUG FIXED] Fix static routing cannot work when firewall on
13. [BUG FIXED] Fix multi-language support
14. [BUG FIXED] Fix web configuration delete firewall rule error

15. [BUG FIXED] fix firewall crash problem under heavy ftp traffic
16. [BUG FIXED] merge SNMP bug fix from p310
17. [BUG FIXED] Fix PPPoE firewall bugs
18. [BUG FIXED] Fix Content filter access fail caused system crash
19. [NEW FEATURE] NAT multi-session IKE support
20. [NEW FEATURE] NAT multi-session IPSec-ESP-Tunnel support
21. [NEW FEATURE] NAT range port forwarding support
22. [NEW FEATURE] Supports IKE for automatic security negotiation and key management
23. [NEW FEATURE] Currently using pre-shared authentication keys for establishing trust between hosts.
24. [NEW FEATURE] Provides DES (56-bit key strength) and 3DES (168-bit key strength) encryption algorithms
25. [NEW FEATURE] SHA-1 and MD5 integrity algorithms for ESP.
26. [NEW FEATURE] SHA-1 and MD5 integrity algorithms for AH.
27. [NEW FEATURE] Provide ESP Tunnel mode, Transport Mode
28. [NEW FEATURE] Provide AH Tunnel mode, Transport Mode

Modification in V3.24(WA.2) | 07/08/2001

1. [BUG FIXED] content filter register error
2. [BUG FIXED] content filter list download error
3. [BUG FIXED] ESP teardrop attack parser error
4. [BUG FIXED] DNS lookup fail when menu 3.2 "DHCP server == None"

Modification in V3.24(WA.1) | 07/06/2001

1. [BUG FIXED] Fix HTP does not initial EPROM

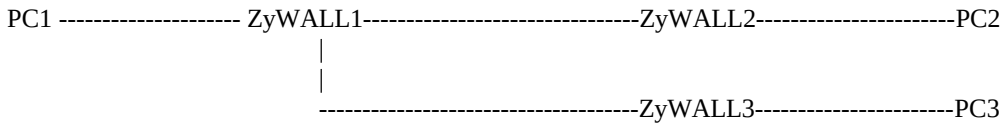
Modification in V3.24(WA.0) | 05/21/2001

1. [BUG FIXED] Change the content filter register server address and domain main.
2. [BUG FIXED] Fix content filter "URL Keyword configuration error"
3. [BUG FIXED] Firmware wrong version number
4. [BUG FIXED] Add SMTP parser support "BDAT" command
5. [BUG FIXED] Fix bug system crash when trying to add more than 1 subnet on the firewall rules. [BUG FIXED] This includes "Local Network" and "Internet" rules on both source and destination IP.
6. [BUG FIXED] Fix content filter "Enable URL keyword blocking" cannot save
7. [BUG FIXED] Fix SMTP parser for Exchange server support
8. [BUG FIXED] Bug fix on Firewall SMTP protocol parser
9. [BUG FIXED] Bug fix on telnet client not sending terminal type
10. [BUG FIXED] Bug fix con Content filter web configuration error
11. [BUG FIXED] Content Filter List cannot save to Flash
12. [BUG FIXED] Content Filter makes all HTTP connection Fail
13. [BUG FIXED] Content Filter: If we didn't registry and going to download Filter List, "Status" must show error message, not show "Write to Prestige router successfully".
14. [BUG FIXED] In "URL KEYWORD" page, when we "Add Keyword" it write to ROM, so Apply is useless.
15. [BUG FIXED] Can't use web set CATEGORIES, if we enable some categories and push Apply button, status will show "Write to Prestige router successfully", we refresh this page, the check box was clear.
16. [BUG FIXED] Block all categories then clear all categories, but we refresh web, "Intolerance" still enable.
17. [BUG FIXED] Content Filter Category cannot be configured problem
18. [BUG FIXED] Content Filter Packet block by Fireall

19. [BUG FIXED] Send Content Filter log by e-mail failure
20. [BUG FIXED] Firewall syslog empty string fix
21. [BUG FIXED] eWeb timeout problem fixed
22. [BUG FIXED] pptp firewall pass through problem fixed
23. [BUG FIXED] Firewall SMTP parser bug fix
24. [BUG FIXED] NAT checksum bug fix
25. [BUG FIXED] eWeb make system hang fix
26. [NEW FEATURE] Add ci command to change different Content filter List server.
27. [NEW FEATURE] Add ci command "sys firewall dos stmp on" to turn on SMTP defender
28. [NEW FEATURE] Add ci command "sys firewall dos stmp off" to turn on SMTP defender
29. [NEW FEATURE] Add ci command "sys firewall dos display" to display the smtp defender status.
30. [NEW FEATURE] Add Netbios over TCP NAT support
31. [NEW FEATURE] DHCP relay
32. [NEW FEATURE] Add NAT Net2Phone support
33. [NEW FEATURE] Content Filter log send to syslog
34. [NEW FEATURE] MSN Firewall support
35. [NEW FEATURE] Parent control support
36. [NEW FEATURE] MSN NAT support
37. [NEW FEATURE] Login Password security support

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:  IP Addr Start= 1.1.1.1           End= 1.1.1.50
                    Port Start= 0                  End= N/A
          Remote: IP Addr Start= N/A               End= N/A
                    Port Start= N/A                End= N/A
          Enable Replay Detection= No
          Key Management= IKE
          Edit IKE Setup= No
          Edit Manual 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
                   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           dynamic           dynamic                     dynamic
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:  IP Addr Start= 3.3.3.1           End= 3.3.3.100
                  Port Start= 0                  End= N/A
        Remote: 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 IKE Setup= No
        Edit Manual 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 security 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 initiate a connection. It only can receive others’ IKE request to built the tunnel.
5) Only the last rule can apply security gateway 0.0.0.0.