ZyXEL ZyWALL 50 Standard Version 3.50(WC.0)C0 Release Note

Date: December 4, 2001

Supported Platforms:

ZyWALL 50

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. For a VPN peer which uses IP subnet range, we have a workaround for that. Please fill the IP Addr End as the subnet mask.
2. 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.

Known Bugs:

1. MAC spoofing cannot work with IPALIAS.
2. Content Filter does not block cookies.
3. Turning off firewall by console or WEB and turning it on by TELNET, the TELNET session will disconnect.

Features:

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.

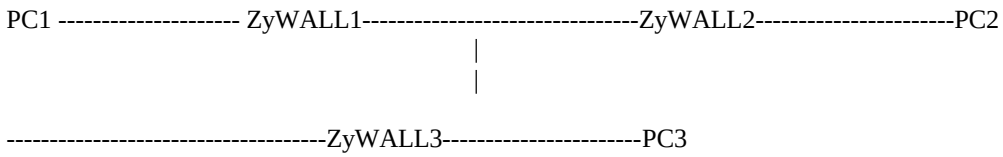
    →Fix:
    1) For the role of ZyWALL2, it periodically checks WAN IP, as long as IP changes, system will auto-disconnect tunnel. This will be logs in VPN Logs.
    2) For the role of ZyWALL1, it periodically checks if any runtime SA has no traffic for a long time. If a SA has no traffic through it in 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:  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.