ZyXEL

Firmware Release Note

ZyWALL 100

Release 3.50(WB.8)c0

Date: **Apr. 9, 2003**
Author: **Neil Cheng**

ZyXEL ZyWALL 100 Standard Version 3.50(WB.8)c0 Release Note

Date: Apr. 9, 2003

Supported Platforms:

ZyXEL ZyWALL 100

Versions:

ZyNOS F/W Version : V3.50(WB.8) | 04/09/2003 17:35:02
BootBase : V1.04 | 09/11/2001 15:20:23

Notes:

1. Hard-coded packet filter for NetBIOS has enhancement, but eWC configuration is not ready yet. Please refer Appendix 4 to configure this feature.
2. The setting of ignore triangle route is on in default ROM FILE. If you only update the firmware from older than 3.50(WB.5)b5, please type “sys firewall ignore triangle all on” in SMT24.8 to bypass firewall check of triangle route traffic. Triangle route network topology has potential security crisis. If you are not clear about it, please refer to Appendix 5 for the triangle route issue.
3. MAC address needs colons to separate each byte.
4. 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.
5. 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.
6. When firewall turns from "off" to "on", the firewall initialization procedure will disconnect all connections running through the ZyWALL.
7. SUA/NAT address loopback feature was enable on ZyWALL 100 by default, however, if users do not need it, a C/I command "ip nat loopback off" could turn it off.
8. Although there are 120 IPSec SAs can be configured, only 100 of them can be activated concurrently.
9. To achieve higher throughput on routing/encrypting/decrypting/NATing/…, a trade-off may sometimes suffer administrator from slower response user interface.
10. It is a trade-off that if users (from LAN/DMZ) want to access servers (in LAN/DMZ) via global IP addresses (in NAT/SUA case), throughput would suffer from an user-friendly yet redundant translation of IP address.
11. BootBase was extended to 128KB.
12. ROMFILE was extended to 256KB, and it takes more time (about 5 seconds) to save configurations

13. Pre-Shared Key support hexadecimal format now, but even numbers is required in hexadecimal format. If you just provide odd numbers, the first character will automatically add 0 so that PSK will be even numbers.
14. If the BootBase version was older than V1.02 and ZyNOS version was older than V3.50(WB.0)b2, a special upgrade procedure must be followed:
    14.1 In DOS prompt mode,
        copy /b WB104.BM+350WB0b7.ROM+350WB0b7.BIN allin1.bin
    14.2 reboot ZW100, and enter debug mode
    14.3 use "ATUX0,30" to start XMODEM upload
    14.4 upload "allin1.bin"
    14.5 use "ATSR" to reboot ZW100

Known Issues:

1. VPN function “Keep Alive” is not ready yet, so configuration of VPN eWC page is useless.
2. eWC of NetBIOS filter configuration is not ready yet.
3. Dial-backup fails to work currently with Wireless LAN.
4. PPTP/L2TP VPN is not ready yet.
5. Content Filter does not block cookies.

Features:

Modifications in V 3.50(WB.8)c0 | 04/09/2003

Modifications in V 3.50(WB.8)b1 | 03/20/2003

1. [ENHANCEMENT] Add “Telia Login” for Telia ISP.
2. [ENHANCEMENT] Support hexadecimal format of pre-shared key. Now pre-shared key starting with "0x" or "0X" will be treated as hexadecimal format.
   NOTE: If old configuration with leading "0x" or "0X" will also be treated as hexadecimal input when save it again.
3. [BUG FIX] Fix two vulnerabilities in eWC.

Modifications in V 3.50(WB.7) | 03/14/2003

Modifications in V 3.50(WB.6) | 09/20/2002

1. [FEATURE CHANGED] The mechanism for IPSec idle time out has been changed. If and only if there is outgoing traffic but NO incoming traffic for 5 minutes (by default), ZyWALL will drop the tunnel. Users can still change the timer by this CI command, “ipsec timer chk_conn <minutes>”
2. [BUG FIXED]
   Symptom: Change SMT 15.1 NAT rule set from Many-to-One to One-to-One, then this rule can not work.
   Condition: If anyone edits an existing NAT rule directly, the configuration is saved into flash but ZyWALL do not refresh runtime data. As a result, this rule cannot work unless system reboot.

3. [BUG FIXED]
   Symptom: Configuration of daylight saving is not consistent between SMT and WEB.
   Condition: Enable daylight saving via SMT menu, you will see daylight saving still disable in Web configuration.
3 [BUG FIXED]
   Symptom: eWC does not show correct string in SUA/NAT page.
   Condition: In eWC SUA/NAT-> Address Mapping still shows “Many to Many no overload”. It should be “Many one to one”.
4 [BUG FIXED]
   Symptom: eWC does not show correct setting in dial backp page.
   Condition: eWC, WAN setup-> Route page, Dial backup Metric show 2, it should be 15.
5 [BUG FIXED]
   Symptom: VPN configuration cannot be saved correctly in eWC.
   Condition: Use eWC configure VPN policy, users must use SMT menu to save again, then zw100 can establish VPN tunnel.
6 [BUG FIXED]
   Symptom: LAN to DMZ NetBIOS filter does not work.
   Condition: Even LAN to DMZ NetBIOS filter is set to “block”, LAN PC still can use NetBIOS to access PC on DMZ.
7 [BUG FIXED]
   Symptom: eWC accepts over-ranged IP pool size setting.
   Condition: Use eWC to set LAN -> IP pool size over range, zw100 still accepts it.
8 [BUG FIXED]
   Symptom: SUA/NAT delete functions are not consistent between SMT and eWC.
   Condition: Use eWC to set SUA/NAT port forwarding then use SMT to delete it, back to eWC, the name field still exists. It should be empty
9 [BUG FIXED]
   Symptom: DMZ host cannot ping ZyWALL DMZ port when Port Forwarding in web page is configured.
   Condition: Ping from DMZ host to ZyWALL 100 DMZ port is ok when no Port Forwarding setting is configured through web. But when there is a SUA port/IP entry is set through web configurator, ZyWALL 100 fails to response ping from DMZ host.
10 [BUG FIXED]
   Symptom: PPP link establishment may be considered as successful even the PAP/CHAP authentication was failed. Hence there is a zombie WAN interface, which has no IP address assigned, and can not route any packet to/from Internet.
   Condition: ISP has ill PAP/CHAP procedure.
11 [BUG FIXED]
   Symptom: An active link may be dropped before a lower cost link is established.
   Condition: PPPoE/PPTP vs. dial-backup may dial alternately.
12 [BUG FIXED] VPN dynamic rule is not stable. When a runtime rule conflicts with the other during IKE phase 2 negotiation, sometimes ZyWALL will crash.
13 [BUG FIXED] SNMP regression. DHCP packets can not send and receive.To fix SNMP problem in b2, some regression has happened. In b2, UDP packets toward

ZyWALL were dropped directly. As a result, DHCP and IKE features did not work.

14 [BUG FIXED] A large number of SNMP packets sending to the ZyWALL will cause it reboot.

15 [BUG FIXED] When ZyWALL receives the TCP packets which are set both SYN and ACK bits, corresponding remote management service is not available any more. (Vulnerability of SecurityFocus™ reported).

16 [BUG FIXED] Changing SNMP setting from eWC cause ZyWALL crash.

17 [BUG FIXED] Using Mozilla, 0.0.0.0 only shows dots in eWC of SUA/NAT address mapping.

18 [BUG FIXED] Setting Dial Timeout, Drop Timeout,and Call Back Delay in SMT 2.1 cause crash.

19 [BUG FIXED] Changing the Web access setting in SMT 24.11, the HTTPD data crash error log isn't correct.

20 [BUG FIXED] Download CyberNOT list crash on passive mode.

21 [BUG FIXED] Port setting in VPN rule cannot work.

22 [FEATURE CHANGED] Wording changed for IPSec address configuration in SMT27.1, SMT27.1.1 and WEB→IPSec.

23 [FEATURE CHANGED] Triangle route network topology is allowed. We changed the CI command to switch on/off firewall checking for triangle route, and this setting is saved in flash rom. It's "sys firewall ignore triangle all [on|off]". The default value is to ignore triangle route check.

24 [FEATURE CHANGED] 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.

25 [BUG FIXED] No matter WAN IP and gateway in the same subnet or not, eWC always shows "Gateway must be on same subnet as this host".

Modifications in V 3.50(WB.5) | 06/18/2002

1. [BUG FIXED] Aggressive mode failed to work.
2. [BUG FIXED] Firewall blocks triangle-route reply packets which going through IP alias.
3. [BUG FIXED] IP checksum error causes that IGMP cannot work.
4. [BUG FIXED] Unexpected termination of the telnet session.
5. [FEATURE ENHANCED] Enhanced DoS ICMP handling.
6. [FEATURE ENHANCED] Added CI command "sys firewall ignore triangle <lan|dmz> [on|off]" to ignore triangle route problem. For example, user can bypass firewall checking on LAN by using "sys firewall ignore triangle lan on". Please note that the traffic DO NOT bypass DoS checking when you only use this command.
7. [FEATURE CHANGED] Accept peer's SA lifetime set to both SEC and KB.
8. [BUG FIXED] Use PPPoE / PPTP connection: after disconnection and then dial up again (Nail-up connection), if ZyWALL get new WAN IP, NAT mapping still used old IP address.
9. [BUG FIXED] Dynamic session does not found when NAT loopback.
10. [BUG FIXED] In virtue of port forwarding and NAT loopback, a server connects to itself through WAN IP. ZyWALL treats as "Land Attack".
11. [BUG FIXED] Use Netscape or Mozilla, eWC in Advance WAN page have square

symbol.
12. [BUG FIXED] PFS writing error: “Perfect” instead of “Prefect”.
13. [BUG FIXED] Use Mozilla, eWC in Wireless LAN page have square symbol.
14. [BUG FIXED] In WAN page, error message “Gateway must be on the same subnet” instead of “Fail to update due to internal error (-10)!”
15. [BUG FIXED] NetBIOS packets always trigger dial no matter “trigger dial” enabled or not.
16. [BUG FIXED] Hard coded netbios filters for IPSec didn’t work. Even it is set to “Non-blocking”, LAN-to-WAN filter will block netbios packets trying to pass IPSec tunnel.
17. [BUG FIXED] Runtime SPD should not be deleted when its SA lifetime remained.
18. [FEATURE CHANGED] When the DHCP server doesn’t response in busy state, ZyWALL will do much more retransmit.

Modifications in V 3.50(WB.4) | 05/14/2002

1. [BUG FIXED] Dial-backup can not hang up ISDN-TA.
2. [BUG FIXED] race condition makes system crash
3. [BUG FIXED] Saving configuration in IPSec Web pages results crash
4. [BUG FIXED] Add then remove custom port results crash
5. [BUG FIXED] Saving configuration in Menu 11.1 results crash
6. [BUG FIXED] Using the Web configurator to inactivate the default route, fail to activate it again
7. [BUG FIXED] Custom Ports only works as a separate rule
8. [BUG FIXED] Static IP Web page only save the last 2 digits of the MAC address
9. [BUG FIXED] Sometimes firewall blocks ICMP packets without reason messages.
10. [FEATURE CHANGED] Idle timeout mechanism of IPSec is changed. Now if there is no outbound traffic and no inbound traffic, the tunnel will be "idle" and won't be deleted. Only when there is outbound traffic but no inbound traffic after the period set by idle timer period, the tunnel will be deleted.
11. [BUG FIXED] Trigger port Web pages fail to save configuration
12. [BUG FIXED] Content filter fail to "Log and Block"
13. [BUG FIXED] Unresolvable domain name result a "0.0.0.0" IP address
14. [BUG FIXED] RemoteManagement-FTP Web page provide invalid default value
15. [BUG FIXED] Menu 4 may show wrong message "Duplicate Static Route"
16. [FEATURE ENHANCED] When ZyWALL detected that its IP address is used by other host, it will alert an error message
17. [FEATURE ENHANCED] SMT menus now check IP address collision
18. [FEATURE ENHANCED] Add new Web pages WAN-ROUTE in WAN setup page
19. [FEATURE ENHANCED] Renew all of WAN help Web pages
20. [FEATURE ENHANCED] Add MISC tags at Remote Management Web pages
21. [FEATURE ENHANCED] Add netmask configuration for PPTP
22. [FEATURE CHANGED] Move Dial backup, Traffic Redirect pages into WAN Web pages
23. [FEATURE CHANGED] Move Trigger Port Web page into SUA/NAT Web pages
24. [BUG FIXED] Enable syslog client and firewall log may cause system hang on an infinite loop

25. [BUG FIXED] Wrong sub-ids in SNMP packets
26. [BUG FIXED] NAT many-one-to-one failed
27. [BUG FIXED] Dial backup Web pages may clear all settings without save them
28. [BUG FIXED] Incorrect label string "DMZ TCP/IP DMZ TCP/IP"
29. [FEATURE ENHANCED] Content Filter Web pages now has "Block Only" option.
30. [BUG FIXED] DHCP server does not provide DNS server.
31. [BUG FIXED] Content Filter doesn't work.
32. [BUG FIXED] Incorrect error log may crash system.
33. [BUG FIXED] Unexpected operations in Web GUI may leave zombie.
34. [BUG FIXED] Custom Port Web pages is still buggy.
35. [BUG FIXED] Firewall Web pages save wrong settings.
36. [NEW FEATURE] 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"
37. [NEW FEATURE] Add a new C/I command "sys filter blockbc [on|off]". For example, user can block broadcast packets by using "sys filter blockbc on". Broadcast packets will be applied here are DHCP packets and RIP packets.
38. [FEATURE ENHANCED] C/I command set for NetBIOS over TCP/IP (NBT) is enhanced. Please refer to Appendix 4.
39. [FEATURE ENHANCED] C/I command, "ipsec display <rule index>" to display IPSec rules.
40. [FEATURE ENHANCED] C/I command, "ip nat incike <on|off>", to increase IKE source port. This is used in NAT pass-through.
41. [FEATURE ENHANCED] Remote Management Control mechanism now log "Access denied" messages into system log.
42. [FEATURE ENHANCED] Remote Management Control Web pages is ready.
43. [FEATURE ENHANCED] Static DHCP table Web pages is ready.
44. [FEATURE ENHANCED] Trigger Port Web pages is ready.
45. [FEATURE ENHANCED] Trafic Redirect Web pages is ready.
46. [FEATURE ENHANCED] Brand new Firewall Web pages is ready. There are 9 directional ACL sets; For packets originating from LAN to LAN(ZyWALL included)/WAN/DMZ, from WAN to LAN/WAN(ZyWALL included)/DMZ and from DMZ to LAN/WAN/DMZ(ZyWALL included).
47. [FEATURE CHANGED] Default ACL rules - "BOOTP client" and "IKE" pass through are moved from ACL set #2(WAN to LAN) to ACL set #8(WAN to WAN).
48. [FEATURE CHANGED] Dynamic rules will not conflict with static rules. Static rules have higher priority, and will be chose during runtime IKE procedure.
49. [FEATURE CHANGED] The repeated entries showed in VPN LOG are reduced.
50. [FEATURE CHANGED] Content filter and VPN Web pages are modified.
51. [FEATURE CHANGED] Wording consistency in Web GUI and SMT.
52. [BUG FIXED] Out-of-range error in Firewall Web pages.
53. [BUG FIXED] Custom Port Web pages is buggy.
54. [BUG FIXED] System crash after changing password.
55. [BUG FIXED] Fragmentation problems have been fixed, including teardrop, full feature NAT and ACL block.
56. [BUG FIXED] When ZyWALL as RESPONDER, it will accept all PFS setting from

INITIATOR and does not check its own configuration.

57. [BUG FIXED] Notify message <No proposal chosen> has incorrect format.
58. [BUG FIXED] PFS mechanism has race condition. When two peers start to re-key simultaneously, sometimes one side will reject the connection.
59. [BUG FIXED] Packets to LAN should not match a rule whose remote IP range is "all".
60. [BUG FIXED] When rules configured as SUBNET, checking NAT full feature mapping with VPN failed.
61. [BUG FIXED] Web has wrong characters in ADVANCE page under Netscape 6.x.
62. [BUG FIXED] Enlarge memory parameters to assure there are enough memory for system operation after VPN tunnels are built.
63. [BUG FIXED] After enable SUA, remote management to LAN IP via VPN tunnel failed.
64. [BUG FIXED] Connectivity Monitor may trigger PPTP dial by accident.
65. [FEATURE CHANGED] Missing Attack Atert and DoS Thresholds Web pages.
66. [BUG FIXED] Web GUI fail to setup Dial Backup, and make crash cycle.
67. [BUG FIXED] Incomplete function in Firewall Custom Port Web pages.
68. [BUG FIXED] Unfriendly operations in menu 15.3.
69. [BUG FIXED] Unfriendly operations in SUA/NAT Address Mapping Web pages.
70. [BUG FIXED] Log displaying mechanism may require additional keypress.
71. [FEATURE ENHANCED] Add new predefined service port AUTH, SYSLOG, and NEW-ICQ into Firewall Web pages.
72. [BUG FIXED] Dial-backup route may lost data, which makes FTP or HTTP fail sometimes.
73. [FEATURE ENHANCED] Add "Hide ESSID" in menu 3.5.
74. [BUG FIXED] Missing default setting (IKE UDP packets pass firewall)
75. [FEATURE ENHANCED] Send IPSec VPN logs to syslog server.
76. [FEATURE ENHANCED] More friendly error messages when SMTP client failed to send e-mail.
77. [FEATURE ENHANCED] Add C/I command "ipsec dial <#rule>", which can be used to trigger IPSec tunnel establishment.
78. [BUG FIXED] menu 11 cannot delete Dial-backup remote node, a nonactive zombie still there.
79. [BUG FIXED] menu 27.1.1 may persist claiming address conflict even mis-configuration has been corrected.
80. [FEATURE CHANGED] Because NetBIOS over TCP/IP (NBT) packet filter is hard-coded now, the factory default filters in menu 21.1 are all removed.
81. [BUG FIXED] Using CLI or Web configurator to configure ACL rules may result inconsistency.
82. [BUG FIXED] Old ROMFILE may result crash.
83. [BUG FIXED] Fail to edit LAN⇔WAN ACL rules via Web configurator.
84. [BUG FIXED] Fail to probe ill-behavior analog modem or ISDN TA.
85. [FEATURE CHANGED] Wireless LAN is back online.
86. [BUG FIXED] menu 15.3 trigger port forward is ready.
87. [BUG FIXED] menu 12 support 12 static routes.
88. [FEATURE CHANGED] default metric value of traffic redirect and dial-backup is

changed to 15.

89. [FEATURE CHANGED] When ZyWALL plays as RESPONDER, it will delay 10 packets to start initiating the re-key procedure, if the INITIATOR does not re-key during the period.
90. [BUG FIXED] Transmitting phase-2 DEL packets during the IKE procedure should wait until the IKE finished.
91. [BUG FIXED] Race condition in NAT module may result crash.
92. [BUG FIXED] Fail to route tunneled packets.
93. [BUG FIXED] Compatibility issue. Fail to drop analog modem/ISDN TA.
94. [BUG FIXED] Fail to detect PPTP connectivity failure.
95. [NEW FEATURE] NetBIOS over TCP/IP (NBT) packet filter is hard-coded now. A set of C/I command is available:
    95.1 To enable/disable triggering dial by NBT packets:
    95.2 sys filter trigdial [on/off] , default is off
    95.3 To block/forward NBT packets
    95.4 sys filter blocknb [on/off] , default is on
    95.5 To make changes permanent, please edit autoexec.net
96. [ENHANCEMENT] Support 12 static routes.
97. [ENHANCEMENT] Add 3rd DNS and WINS server for DHCP server option. We add two C/I commands, "ip dhcp <iface name> server <dns server>" and "ip dhcp <iface name> server <wins server>" to add server IP.
98. [ENHANCEMENT] Add a switch to control NAT IRC service turned on/off. We provide a new C/I command "ip nat service irc <on|off>" to control the service.
99. [ENHANCEMENT] VPN LOG will show detail notify message type.
100. [FEATURE CHANGED] IPSec-related C/I commands are visible.
101. [FEATURE CHANGED] When peer's ID is single for dynamic rule, SA monitor will show a single address.
102. [BUG FIXED] After long time test, IPSec process will cause system lack of memory.
103. [BUG FIXED] Phase 1 time out in dynamic rule will delete runtime SPD and then tunnel fails.
104. [BUG FIXED] Only local ID being the same with remote ID can dynamic rule work.
105. [BUG FIXED] Dynamic SPD will be deleted during re-key procedure and cause tunnel down.
106. [BUG FIXED] Re-key-procedure will use wrong SA lifetime value.
107. [BUG FIXED] Under PPPoE connection, tunnel is built but no traffic can pass through it.
108. [BUG FIXED] Web a SUA/NAT behavior is wrong.
109. [BUG FIXED] "ip nat reset enif1" don't work.
110. [BUG FIXED] Firewall will check back-record for the TRACEROUTE reply to port unreachable of ICMP at the end host.
111. [BUG FIXED] Static routed packets from LAN to LAN will be blocked by firewall.
112. [BUG FIXED] Solve the SNMPv1 vulnerability problem.
113. [BUG FIXED] After using SMT to change password, WEB login procedure will fail.
114. [FEATURE CHANGED] Phase 1 SA will time out. And its lifetime is independent from phase 2 SA lifetime.
115. [BUG FIXED] Remote management from web cannot use port other than 80.

116. [BUG FIXED] Sometimes packets cannot pass through tunnel built from dynamic rule.
117. [BUG FIXED] SUA/NAT configuration in WEB is incorrect.
118. [BUG FIXED] Routing cache calculation will overflow.
119. [ENHANCEMENT] After a packet is processed IPSec and going to be transmitted, it can be applied IPSec again. We provide C/I commands to control which destination side can be applied IPSec. They are "ipsec route wan / lan".
120. [ENHANCEMENT] Add IPSec parser in C/I command, "sys trcpacket parse".
121. [ENHANCEMENT] Add SNMP link UP / DOWN trap for channels.
122. [FEATURE CHANGE] IPSec related SMT and WEB wording changed.
123. [FEATURE CHANGED] IPSec MyIP and secure gateway address can be set to 0.0.0.0 at the same time.
124. [FEATURE CHANGED] IPSec support LAN IP as MyIP.
125. [FEATURE CHANGED] DHCP packets will not run into IPSec process.
126. [BUG FIXED] Manual key cannot swap from one rule to another, if these two rules have the same secure gateway.
127. [BUG FIXED] 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.
128. [BUG FIXED] When building the tunnel, sometimes system will crash.
129. [BUG FIXED] Provide online help for IPSec ADVANCE page in WEB.
130. [ENHANCEMENT] Support phase 2 ID: SINGLE / RANGE / SUBNET.
131. [ENHANCEMENT] Support using domain name as secure gateway address. We will periodically update peer IP according to the domain name. We provide two new C/I commands: "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.
132. [ENHANCEMENT] Different rules can connect to the same secure gateway. However, there are some criteria for these rules, please refer to Appendix 2.
133. [ENHANCEMENT] Multiple dynamic rules are supported. There is no ordering issue for these dynamic rules.
134. [ENHANCEMENT] Web configurator can modify phase 1 algorithms through ADVANCE page.
135. [ENHANCEMENT] Add two C/I 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.
136. [ENHANCEMENT] Add remote management for support SNMP and DNS.
137. [FEATURE CHANGE] C/I commands for ipsec such as "ipsec sa" and "ipsec sa_sdb_status" are removed. To show SA status, we provide C/I command "ipsec show_runtime sa".
138. [NEW FEATURE] Add SNMP and DNS access control. For more information, please refer to Appendix 1
139. [NEW FEATURE] Add Trigger Port support. For more information, please refer Appendix 2.
140. [NEW FEATURE] Add a new C/I command:
141. ip aliasdis [on/off], , enable/disable routing between alias.
142. [ENHANCEMENT] Add Custom, Static DDNS domain name support.
143. [BUG FIXED] PPPOE cannot re-connect if previous disconnection time took too

long

144. [NEW FEATURE] Add Internet Connectivity Monitor, Traffic Redirect and Dial-backup feature. For more information, please refer to Appendix 3.
145. [BUG FIXED] eWc spoof the fake LAN MAC address fail.
146. [ENHANCEMENT] Add SNMP linkup and linkdown trap of enet0, enet1, poe0, pns0 channel.
147. [BUG FIXED] Menu 22 SNMP trap configurations need to reboot system to become effective.
148. [ENHANCEMENT] Change eWC help pages format.
149. [ENHANCEMENT] Add C/I command to support the remote node option setting feature:
    - 149.1 sys rn load <entry no.> , load instruction
    - 149.2 sys rn disp <entry no.> , display instruction (0:working buffer)
    - 149.3 sys rn nat <none|sua|full_feature> , NAT setting instruction.
    - 149.4 sys rn nailup <no|yes> , Enable/Disable NAIL-UP feature.
    - 149.5 sys rn save <entry no.> , save instruction.
150. [BUG FIXED] Bug fix for multi-IPSEC Pass through problem
151. [BUG FIXED] Fix DHCP duplicated entries bug.
152. [BUG FIXED] Fix DNS server IP address runtime value will be cleaned.

Modifications in V 3.50(WB.3) | 01/22/2002

1. [BUG FIXED] PCI bus broken master at A0-AA/AB/AC board.
2. [ENHANCEMENT] RTL8139C(+) driver throughput.
3. [ENHANCEMENT] RTL8139C(+) driver stability.
4. [BUG FIXED] memory leak in IPSec VPN connections.
5. [ENHANCEMENT] RTL8139C(+) test OK in HTP.
6. [ENHANCEMENT] RTL8139C(+) Driver.

Modifications in V 3.50(WB.2) | 12/10/2001

1. [ENHANCEMENT] RTL8139C Driver reliability.

Modifications in V 3.50(WB.1) | 11/27/2001

1. [ENHANCEMENT] A connection from DMZ to the system's itself WAN address should be checked by firewall access control rule.
2. [FEATURE CHANGED] IPSec-VPN phase 1 SA algorithm was default to DES-MD5 via web configurator, user should change it via SMT if needed.

Modifications in V 3.50(WB.0) | 11/26/2001

1. [ENHANCEMENT] A connection from WAN to the system's itself DMZ address should be checked by firewall access control rule.
2. [BUG FIXED] SMT 24.11 fail to control connections from WAN using LAN/DMZ IP (or alias) addresses.
3. [BUG FIXED] System crash if time calibration fails.
4. [BUG FIXED] In web configurator DMZ pages, some default values mess-up.
5. [BUG FIXED] SMT 24.11 fail to control connections from WAN using LAN alias IP addresses.

6. [BUG FIXED] ICMP echo/reply message from WAN can pass through NAT/SUA if the destination address is an ILA.
7. [BUG FIXED] Firewall ACL will not apply to IPALIAS address.
8. [FEATURE CHANGED] Do not provide DHCP server on DMZ .
9. [BUG FIXED] C/I command "sys ddns disp" sometimes make crash.
10. [BUG FIXED] Setup DMZ via web configurator, then switch to SMT 5.2, an error message will claim missing required field.
11. [ENHANCEMENT] Support IP multicast on DMZ
12. [BUG FIXED] Alternative stress test by Smartbit 2000 make MAC chip block
13. [BUG FIXED] With PPPoE/PPTP, connections from DMZ can not reach WAN.
14. [BUG FIXED] When an (via telnet/web) administrator doing something for a long time or waiting for interactive operation, an (via console) administrator would fail to kick out the former one gracefully but a system reset will be triggered. The following cases match the criterion:
    14.1 Waiting on SMT 24.10
    14.2 Waiting on log displaying
    14.3 Waiting on interaction operation, e.g. waiting for "Y" or "N"
15. [BUG FIXED] Fail to change default route in web configurator.
16. [BUG FIXED] Applying missing filter (set #3).
17. [BUG FIXED] SMT 24.11 fail to control connections from DMZ
18. [BUG FIXED] Fail to access FTP server from LAN to DMZ.
19. [BUG FIXED] Web configurator (VPN / Content filter) cannot be accessed by Netscape 4.78
20. [BUG FIXED] With PPPoE / PPTP configured, but no dial-up, system would crash after typing "ip ro st" in C/I command mode.
21. [BUG FIXED] DNS proxy can't get the address when the original DNS server failed.
22. [BUG FIXED] After PPTP connection built, system would crash.
23. [BUG FIXED] When SNMP query through the system, it would crash.
24. [BUG FIXED] In SMT 24.6, interrupt the upload procedure would cause system crashed.
25. [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.
26. [FEATURE CHANGED] When system crashes, it will not stop in the screen. Instead after showing memory dump, system will reboot automatically.
27. [ENHANCEMENT] In firewall setup, IKE (UDP:500) is placed in standard protocol instead of custom port. Default romfile changed.
28. [ENHANCEMENT] VPN logs and debug messages were modified to be much readable.
29. [ENHANCEMENT] When dynamic WAN-IP changes, system will disconnect all VPN connections which MyIP is "0.0.0.0".
30. [ENHANCEMENT] When VPN connection has no traffic through it for a period, it will disconnect automatically.
31. [ENHANCEMENT] Add two new C/I commands in "ipsec timer" to configure VPN timers.
32. [BUG FIXED] When firewall turns off and SUA only, PC in the WAN side can ping

PCs in the LAN side.

33. [BUG FIXED] with PPPoE connection, WAN-to-LAN ACL will not be applied. Even a packet is allowed to be transferred from WAN to LAN, firewall will block it.
34. [BUG FIXED] When the WAN side is using PPPoE connection and NAT turns off, firewall does not protect the LAN side.
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. [FEATURE CHANGED] Web status after saving configuration has changed to "Configuration updated successfully".
37. [FEATURE CHANGED] Only the last rule can apply security gateway to "0.0.0.0".
38. [FEATURE CHANGED] Web (SUA/NAT) default DMZ server changes to default server.
39. [BUG FIXED] When remote IP is too long, SA monitor will show incorrect layout.
40. [BUG FIXED] When phase 2 SA life time out, sometimes there exists a phase 1 SA and no tunnel can be built.
41. [BUG FIXED] Using Web to upgrade firmware, system will reply "internal error".
42. [BUG FIXED] VPN timeout re-connection function is not robust.
43. When "SA Life time" is time out, sometimes the VPN tunnel cannot be re-established again.
44. [BUG FIXED] VPN tunnel cannot be established if WAN IP is static without default gateway configured.
45. 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.
46. [BUG FIXED] VPN tunnel cannot work with multi-NAT.
47. [BUG FIXED] Web (VPN) pages are not consistent with SMT. SMT27.xx have been modified, but not Web pages.
48. [BUG FIXED] Use Web setup VPN for manual mode, it can not work until save in SMT again
49. [BUG FIXED] Web (Firewall) will show error messages when try to access help pages, which are not available now.
50. [ENHANCEMENT] Manual key SA will runtime creates when traffic matches SPD.
51. [ENHANCEMENT] SA monitor will show manual key SA, and command to delete it is available.
52. [ENHANCEMENT] Idle timer also applies on manual key SA. When no traffic transmits through the SA, system will delete it.
53. [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.
54. [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.
55. [ENHANCEMENT] Simultaneous SA check: All VPN rules can be set to "ACTIVE", but only 10 runtime SA can be established at the same time.
56. [FEATURE CHANGED] Default idle timer value is set to 1 minute.
57. [BUG FIXED] Web (Content filtera EXEMPT ZONE) Apply button didn't work.

58. [BUG FIXED] VPN connection cannot be re-built after dynamic WAN IP being changed.
59. 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.

    59.1 ZyWALL #1 (security gateway IP 0.0.0.0) ← ZyWALL #2 (my IP 0.0.0.0)

    59.2 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.
60. Fix:
61. 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.
62. 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 3 minutes, system will disconnect the tunnel.
63. There are two new C/I commands to configure 1) and 2). They are "ipsec timer chk_my_ip" and "ipsec timer chk_conn"
64. 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.
65. [BUG FIXED] Can not download Content filter list
66. [BUG FIXED] IPSec-VPN settings in SMT menu was not saved to ROM
67. [ENHANCEMENT] Re-program 93C46 AGAIN to enhance RTL8139C's reliability.
68. [ENHANCEMENT] Users from LAN/WAN/DMZ can not use the same IP address (the global IP address which was usually resolved from FQDN) to access servers in LAN/DMZ when NAT/SUA was enabled.
69. [ENHANCEMENT] Re-program 93C46 to enhance RTL8139C's reliability.
70. [ENHANCEMENT] FLASH programming procedure was improved that it runs triple speed on Intel J3A series.
71. [BUG FIXED] All known crash issues.
72. [INTERNAL] Throughput (routing only) is about 20Mbps.
73. [BUG FIXED] System crashed by unusual IKE message
74. [BUG FIXED] IPSec configuration bugs
75. [ENHANCEMENT] Re-program 93C46
76. [ENHANCEMENT] Speed up IPSec DES engine
77. [ENHANCEMENT] Speed up FLASH writing process.
78. [ENHANCEMENT] System stability enhanced
79. [ENHANCEMENT] Throughput enhanced
80. [BUG FIXED] IPSec rule name disappear
81. [BUG FIXED] Console login didn't kick out web configurator
82. [BUG FIXED] Debug messages removed
83. [ENHANCEMENT] System stability enhanced
84. [NEW FEATURE] SA monitor was added in Web Configurator
85. [BUG FIXED] SMT menu 27.x.x.x mess-up
86. [BUG FIXED] Setup IPSec (rule 9) to Manual mode, ZW100 crash

87. [BUG FIXED] Configure IPSec in Manual mode, when starting establish an SA, ZW100 crash
88. [BUG FIXED] Use Web Reset to default rom file, although ZW100 has reboot, but configuration still not change
89. [BUG FIXED] Can not use web restore backup configuration file
90. [BUG FIXED] Firewall block LAN to DMZ traffic
91. [BUG FIXED] In web configurator, restoring default ROMFILE make ZW100 crash
92. [BUG FIXED] After remote node was deleted from menu 11, accessing menu 5 make ZW100 crash
93. [INTERNAL] BootBase was extended to 128KB
94. [INTERNAL] ROMFILE was extended to 256KB
95. [BUG FIXED] Use FTP upgrade Firmware, ZW100 will crash
96. [BUG FIXED] Can not use Web configurator upgrade firmware
97. [BUG FIXED] Annoy debug messages
98. [BUG FIXED] Make an VPN connection with ZyWALL10, ZyWALL10 will crash
99. [BUG FIXED] PPTP can not dial up
100. [BUG FIXED] Access Internet(WWW), ZyWALL100 crash
101. [BUG FIXED] Change menu 4 to PPTP,ZW100 crash
102. [BUG FIXED] Can ping LAN PC from the PC behind DMZ port
103. [BUG FIXED] Menu 24.5/24.6 fail
104. [BUG FIXED] HTP test AUX port, LINK/ACT LEDs don’t work
105. [BUG FIXED] Web configurator failed on VPN page
106. [NEW FEATURE] IP police routes can be applied to LAN port in menu 3.2
107. [BUG FIXED] HTP test failed on LAN/WAN/DMZ items
108. [ENHANCEMENT] Wireless LAN bridge was enhanced.
109. [NEW FEATURE] IPSec VPN support 120 SAs

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

New function

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

Modification

(1) We **removed** the default TEL_FTP_WEB filter in Menu 11.5.
(2) The default value for Server access rule is **LAN only**.
(3) Under the default setting: You can setup the Menu 15 to forwarding the server to LAN IP address. Thus you can configure the router through the WAN and you don't need to modify the server management or filter.

```
          Menu 24.11 - Remote Management Control

TELNET Server:    Port = 23       Access = LAN only
                  Secured Client IP = 0.0.0.0

FTP Server:       Port = 21       Access = LAN only
                  Secured Client IP = 0.0.0.0

Web Server:       Port = 80       Access = LAN only
                  Secured Client IP = 0.0.0.0

SNMP server:      Port = 161      Access = LAN only
                  Secured Client IP = 0.0.0.0

DNS server:       Port = 53       Access = LAN only
                  Secured Client IP = 0.0.0.0


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

Appendix 2 Trigger Port

Introduction

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

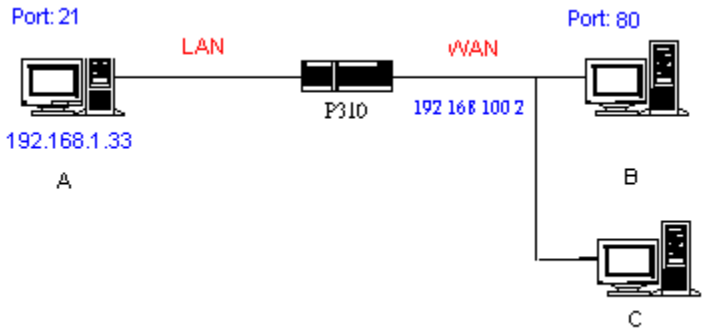
These triggered events can be timed so that they erase the port mapping as soon as they are done with the data transfer, so that the port mapping can be triggered by another Client computer. This gives the ***illusion*** that multiple computers can use the same port mapping at the same time, but the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

How to use it

Following table is a configuration table.

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

How it works



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

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

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

"Incoming Port". If it matches, Prestige will forward the packet to the recorded IP address in the internal table for this port. (This behavior is the same as we did for port forwarding.)

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

Notes

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

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

Appendix 3 Internet Connectivity Monitor, Traffic Redirect and Dial-Backup

Introduction

These features are used to keep Internet connectivity of the ZyWALL. The Connectivity Monitor is running at interval to detect if the ZyWALL can reach a desired host/address or the adjacent upstream gateway. Once the ZyWALL has detected the connectivity is broken, it tries to forward the traffic to another gateway that user has specified.

Menu 11.6 - Traffic Redirect Setup

```
              Menu 11.1 - Remote Node Profile

Rem Node Name= Normal_route   Route= IP
Active= Yes

Encapsulation= Ethernet       Edit IP= No
Service Type= Standard        Session Options:
Service Name= N/A             Edit Filter Sets= No
Outgoing:
  My Login= N/A               Edit Traffic Redirect= YES
  My Password= N/A
  Server IP= N/A

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

```
            Menu 11.6 - Traffic Redirect Setup

          Active= No
          Configuration:
            Backup Gateway IP Address= 0.0.0.0
            Metric= 2
            Check WAN IP Address= 0.0.0.0
              Fail Tolerance= 0
              Period(sec)= 0
              Timeout(sec)= 0

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

(1) Configure "Active" to "YES" if you want this feature work.
(2) "Backup Gateway". When the primary ISP or the check point is unreachable, traffic will be handed over to this backup gateway. [In IP address format]
(3) "Metric". Please reference section "**Metric**"
(4) "Check WAN IP Address". The Connectivity Monitor will probe the connectivity to a check-point. In general case, this check-point is the adjacent upstream gateway, which is typically assigned by ISP. However, if user desires to check a more significant point on the Internet, it can be specified here. A special case should be noticed that, even the ISP is online, this check-point maybe not reachable. The hand-over mechanism will function when the check-point failed. Leave it to 0.0.0.0, and the ZyWALL will take the upstream gateway as the default check-point.
(5) "Fail Tolerance" is the check failure upper limit. For example, if this value is 2. When ZyWALL failed to reach the check-point at the 3rd try, Connectivity Monitor will

invalidate the corresponding route and promote candidate to be the default route.

(6) "Period". The Connectivity Monitor will examine physical link signal and then probe the check-point at a interval of "period" seconds.

(7) "Timeout". The check-point is expected to response ZyWALL's probe within a reasonable time. After that, ZyWALL will log a failure. When the fail tolerance is exceeded, traffic will be handed over to the candidate route.

(8) The probing mechanism employs ICMP echo request/reply. Some hosts or routers on Internet may discard such packets.

Menu 2 - Dial-Backup Setup

```
                    Menu 2 - WAN Setup

               MAC Address:
                 Assigned By= Factory default
                 IP Address= N/A

               Dial-Backup:
                 Active= YES
                 Phone Number=
                 Port Speed= 115200
                 AT Command String:
                   Init= at&fs0=0
                 Edit Advanced Setup= No

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

This menu setup the dial device, which is typically an analog modem or ISDN TA. To activate the dial device, please toggle "Avtive" to "YES".

Menu 11.1 - Backup ISP Setup

```
       Menu 11.1 - Remote Node Profile (Backup ISP)

Rem Node Name= Backup route  Edit PPP Options= No
Active= Yes                   Rem IP Addr= 0.0.0.0
                              Edit IP= YES
Outgoing:                     Edit Script Options= No
  My Login=
  My Password= ********       Telco Option:
  Authen= CHAP/PAP              Allocated Budget(min)= 0
  Pri Phone #= ?                Period(hr)= 0
  Sec Phone #=                   Nailed-Up Connection= No

                              Session Options:
                                Edit Filter Sets= No
                                Idle Timeout(sec)= 100

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

A valid pair of login username and password is required. And the phone number of ISP is required. Leave "Rem IP Addr" to 0.0.0.0 makes ZyWALL try to get its IP

address from ISP.

```
        Menu 11.3 - Remote Node Network Layer Options

          Rem IP Addr= 0.0.0.0
          Rem Subnet Mask= 0.0.0.0
          My WAN Addr= 0.0.0.0

          Network Address Translation= SUA Only
          Metric= 2
          Private= No
          RIP Direction= Both
          Version= RIP-2B
          Multicast= None

            Enter here to CONFIRM or ESC to CANCEL:
```

Typically, "Network Address Translation" should be "SUA Only".

Metric

Once the traffic redirect and dial-backup mechanism were activated, ZyWALL will have 3 default routes to Internet. The first one is the normal route that designated by ISP or the static route mechanism; the second one is the traffic-redirect route (i.e. the backup gateway); the third one is the dial-backup route.

Customable metrics are provided in the menu 11.6 (Traffic Redirect) and menu 11.3 (Dial-backup) to determine the priority of the 3 default routes. For example, if the normal route has a metric "1" and traffic-redirect route has a metric "2" and dial-backup route has a metric "3", then the normal route is the first priority candidate to be the primary default route. If the normal route failed to get on Internet, the traffic-redirect route will be the successor. By the same theorem, dial-backup route is the successor after traffic-redirect route failed. For any two of the default routes match the same metric, a pre-defined priority is taken:

Normal route > Traffic-redirect route > Dial-backup route

For another example, if user want ZyWALL to use dial-backup route prior than traffic-redirect route or even the normal route, all need to do is to make metric of dial-backup route to be "1" and the others to be equal to "2" (or greater).

C/I commands

A set of C/I commands are provided.

(1) "ip tredir active [on/off]" to enable/disable traffic redirect.
(2) "ip tredir partner" IP address of the backup gateway.
(3) "ip tredir target" IP address of the check target.
(4) "ip tredir failcount" to setup fail tolerance.
(5) "ip tredir checktime" to setup checking period.
(6) "ip tredir timeout" to setup check timeout.
(7) "ip tredir disp" to show system value and run time value.
(8) "ip tredir save" will save the configuration.

Note

(1) Turn off "RIP" in SMT3.2 is recommended.
(2) When traffic redirect is turned on, and encapsulation type is PPPOE or PPTP, "Nail-UP" function in SMT11.1 will be enabled
(3) A useful WINDOWS commands "tracert" can be used to verify the packet routing.
(4) Connectivity Monitor can not be disabled. However, traffic redirect and dial-backup mechanism can be enabled/disabled independently.
(5) Because the primary ISP and the backup ISP may assign different WAN IP address to ZyWALL. When traffic have handed over from one ISP to the other, all exist connections may be forced to reconnect.

Appendix 4 Hard-coded packet filter for "NetBIOS over TCP/IP" (NBT)

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

There are two CI commands:
(1) "sys filter netbios disp": It will display the current filter mode.

Example ouput:

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

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

Type	Description	Default mode
0	LAN to WAN	Forward
1	WAN to LAN	Forward
2	LAN to DMZ	Forward
3	WAN to DMZ	Forward
4	DMZ to LAN	Forward
5	DMZ to WAN	Forward
6	IPSec pass through	Forward
7	Trigger dial	Disabled

Example commands:

```
sys filter netbios config 0 on  => block LAN to WAN NBT packets
sys filter netbios config 1 on  => block WAN to LAN NBT packets
sys filter netbios config 2 off => pass LAN to DMZ NBT packets
sys filter netbios config 6 on  => block IPSec NBT packets
sys filter netbios config 7 off => disable trigger dail
```

Appendix 5 Traffic Redirect/Static Route/Policy Route Application Note

Why traffic redirect/static/policy route be blocked by ZyWALL

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

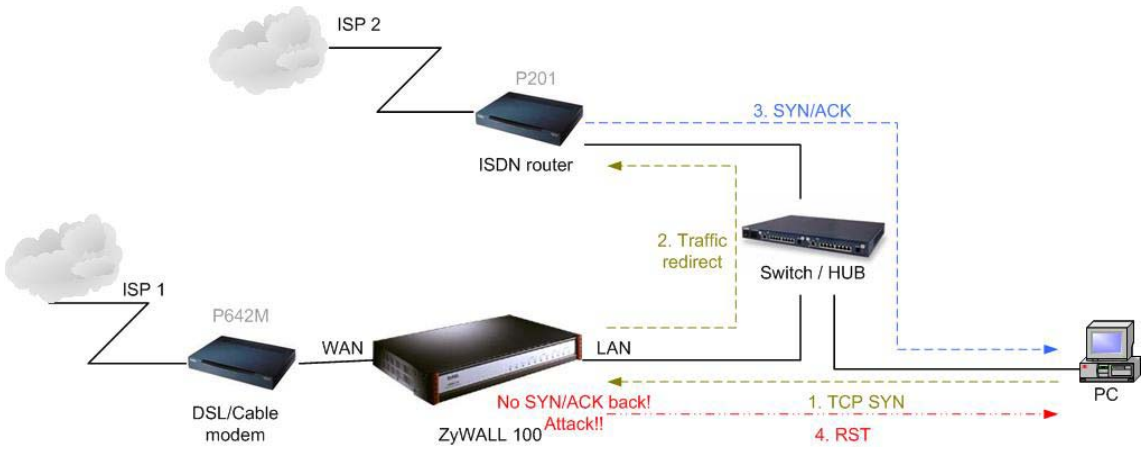


Figure 5-1 Triangle Route

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**.

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

That causes all of outgoing TCP traffics being reset!

How traffic redirect/static/policy 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.

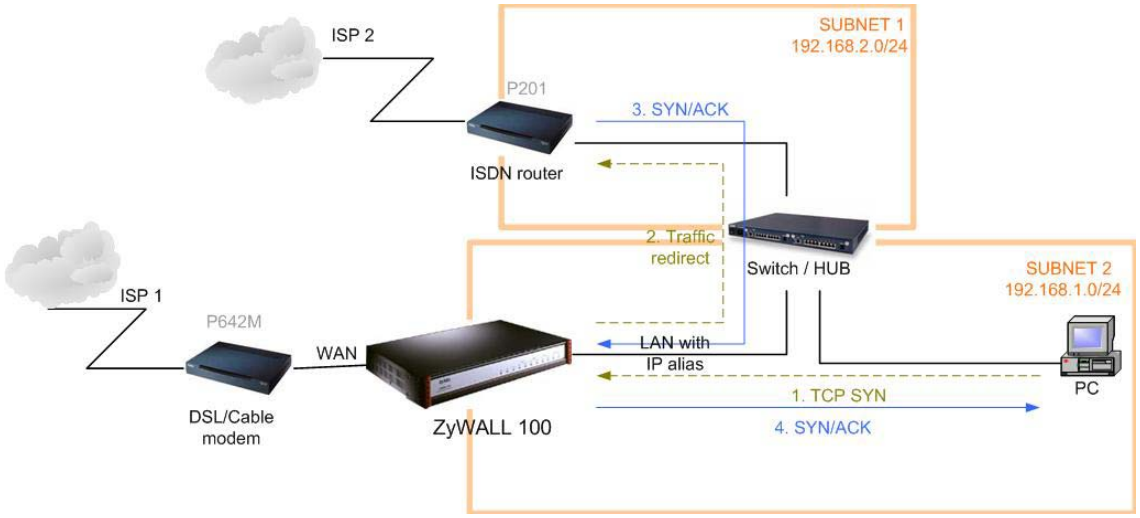


Figure 5-2 Gateway on alias IP network

(2) Gateway on WAN side

A working topology is suggested as below.

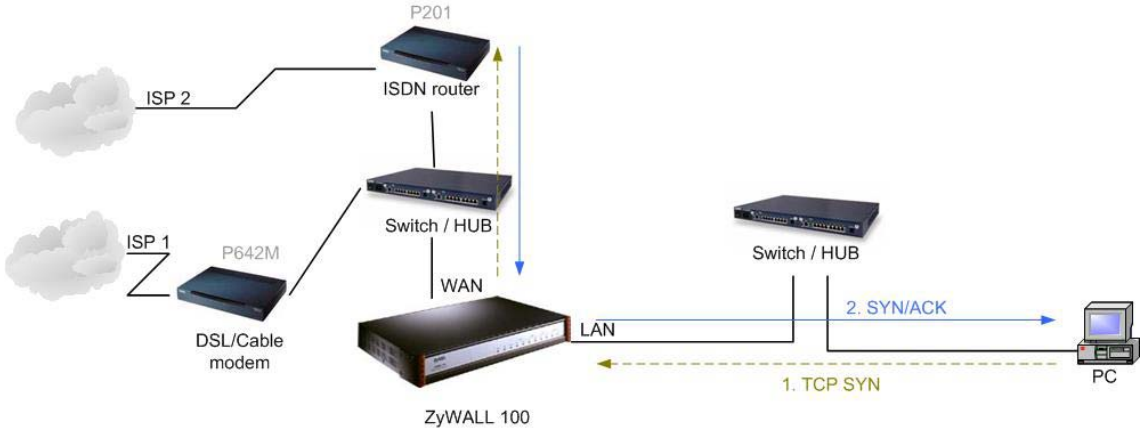


Figure 5-3 Gateway on WAN side