ZyXEL

Firmware Release Note

ZyWALL 10

Release 3.50(WA.6)

Date: **Nov 19, 2002**
Author: **Raymond Chen**

ZyXEL ZyWALL 10 Standard Version 3.50(WA.6) Release Note

Date: Nov 19, 2002

Supported Platforms:

ZyXEL ZyWALL 10

Versions:

ZyNOS Version: V3.50(WA.6) | 11/08/2002 11:05:24
Bootbase Version: V2.10 | 03/22/2002 14:38:58

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 ADVANCE page to configure them.
4. When firewall turns from "off" to "on", the firewall initialization procedure will disconnect all connections running through the ZyWALL.
5. Please refer to Appendix 5 for the triangle route issue.

Known Bugs:

1. Content Filter does not block cookies.
2. To fix the bug of "When the user setups the schedule to the block time of date, ZyWALL always blocks traffic matching domain name", data structure of content filter was changed. However, the auto-convert function had some bugs. If you are using content filter feature, please do following steps to convert data structure from old to new: WEB→ADVANCE→CONTENT FILTER→Categories→ Apply. Or the content filter function may not work properly. We will complete the auto-convert function in the future.
3. After configuring DDNS through eWC, ZyWALL will not update DDNS server when IP changes. Please use SMT to configure DDNS.

Features:

Modification in V3.50(WA.6) | 11/08/2002

1. [BUG FIX] Symptom: When editing firewall ACL in some condition, ZyWALL10 crashes.
   Condition: The procedure to duplicate the problem is
   1) Add one firewall rule in Wan to Lan. in source field, one is subnet, two are single. Save it.
   2) goto WAN to LAN policy, change subnet to single address. First you'll see that after applying, only two ip adresses are shown in the list (three ips were before). then immediately klick on apply to confirm the WAN to LAN policies -> crash!
   3) the zywall should rebooting now the hole time and give a debug output at the hyperterminal. only by uploading the factory default romfile, the zywall is working again
2. [BUG FIX] Fix a security issue related with IP stack.
3. [BUG FIX] Symptom: Default setting was not correct.
   Condition: When using WEB to reset ZyWALL to factory default, the firewall default setting is not correct. And the device filter of PPPoE / PPTP should be removed.

Modification in V3.50(WA.5) | 08/13/2002

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. [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.
6. [FEATURE CHANGE] 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>"
7. [BUG FIX] When the user setups the schedule to the block time of date, ZyWALL always block traffic matching "domain name".
8. [BUG FIX] CI command to configure trigger dial in netbios packet filter cannot work.
9. [BUG FIX] Port setting in VPN rule cannot work.
10. [BUG FIX] Download CyberNOT list crash on passive mode.
11. [BUG FIX] Clearing default server in WEB→SUA/NAT by entering non-ip string will leave that field containing incorrect numbers.
12. [BUG FIX] Clear multi-page VPN LOG, the log index will not reset.
13. [BUG FIX] Static route from LAN to LAN (IP alias segment) will be blocked by firewall.
14. [BUG FIX] Fix a security issue about TCP stack.

Modification in V3.50(WA.4) | 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(WA.3) | 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(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 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
    LAN to DMZ:          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	IPSec pass through	Forward
4	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 3 on      => block IPSec NB/IP packets
sys filter netbios config 4 off     => disable trigger dial
```

3) NOTE: Since one of “WAN to LAN” or “LAN to WAN” switch will affect packets transmitted through ZyWALL, if you need to access PCs on LAN side, please turn these two switch to “forward”. We will combine this two switches to a single one in the future.

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.

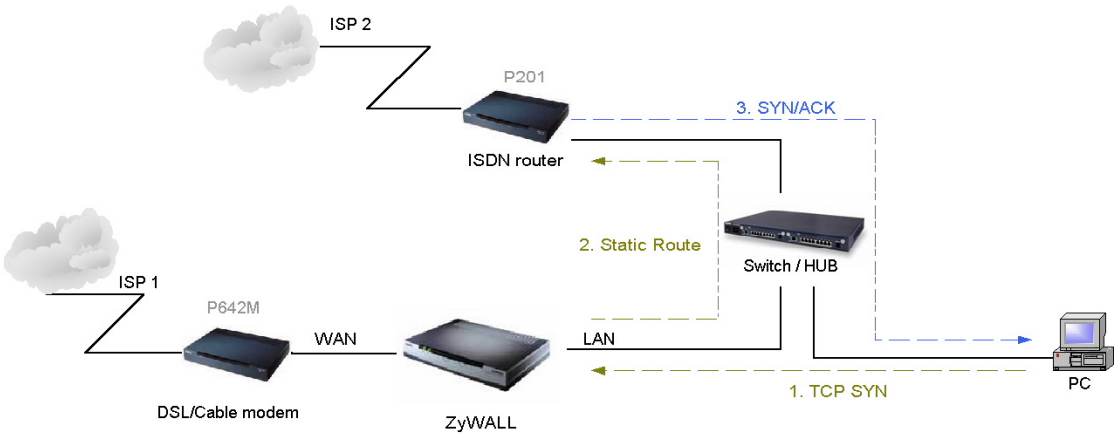

Figure 5-1 Triangle Route

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.

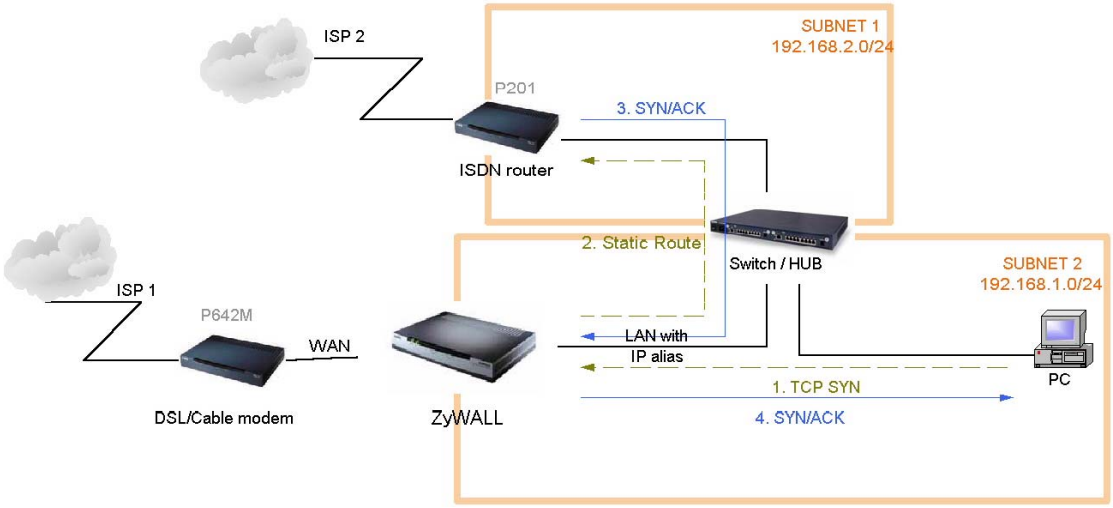

Figure 5-2 Gateway on alias IP network

(2) Gateway on WAN side

A working topology is suggested as below.

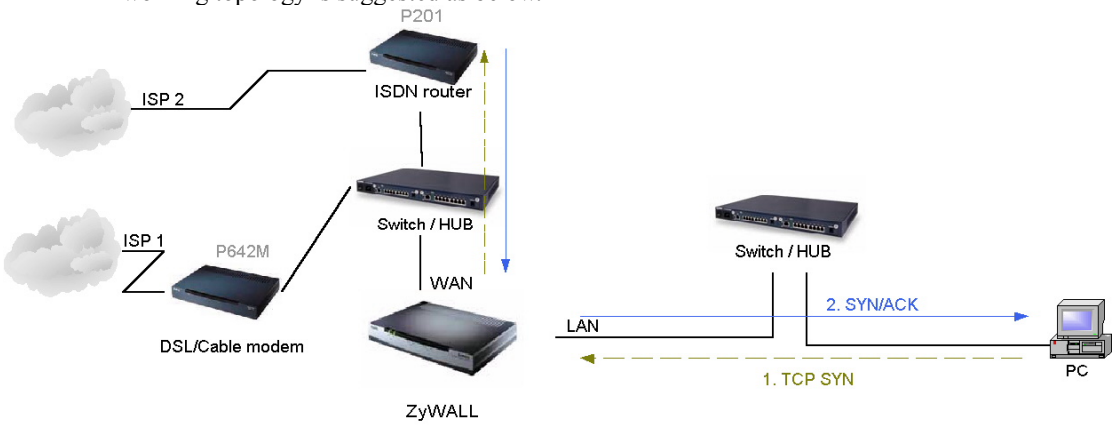

Figure 5-3 Place other gateways on WAN side