ZyXEL ZyWALL 50 Standard Version 3.50(WC.3)C0 Release Note

Date: June 17, 2002

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.
2. Using Web to configure VPN, the phase 1 algorithms have been fixed to DES + MD5. If other algorithms are preferred, please use ADVANCE page to configure them.
3. When firewall turns from "off" to "on", initialization procedure will disconnect all connections running through the ZyWALL.
4. Please refer to Appendix 5 for the triangle route issue.

Known Bugs:

1. Content Filter does not block cookies.
2. "sys filter netbios config 3 on" doesn't work.

Features:

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

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

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

1. [ENHANCEMENT] Support phase 2 ID: SINGLE / RANGE / SUBNET.
2. [ENHANCEMENT] Support using domain name as secure gateway address. We will periodically update peer IP according to the domain name. Two new CI commands are provided: "ipsec timer update_peer" and "ipsec updatePeerIp". The former is to set the interval for updating, and the latter is to force system update right away.
3. [ENHANCEMENT] Different rules can connect to the same secure gateway. However, there are some criteria for these rules, please refer to Appendix 2.
4. [ENHANCEMENT] Multiple dynamic rules are supported. There is no ordering issue for these dynamic rules.
5. [ENHANCEMENT] Web configurator can modify phase 1 algorithms through ADVANCE page.

6. [ENHANCEMENT] Add two CI commands : "ppp lcp echo time" and "ppp lcp echo retry" to control echo timer and retry counts. Set one of them to 0 will disable echo request.
7. [ENHANCEMENT] Add remote management for support SNMP and DNS.
8. [ENHANCEMENT] Some workarounds for “VPN route” are supported: After a packet is processed IPSec and going to be transmitted, it can be applied IPSec again. We provide CI commands to control which destination side can be applied IPSec. They are “ipsec route wan / lan”.
9. [ENHANCEMENT] Add IPSec parser in CI command, "sys trcpacket parse".
10. [ENHANCEMENT] Add SNMP link UP / DOWN trap for channels.
11. [ENHANCEMENT] VPN LOG will show detail notify message type.
12. [ENHANCEMENT] Add 3rd DNS and WINS server for DHCP server option. We add two CI commands, <ip dhcp "iface name" server dnsserver> and <ip dhcp "iface name" server winsserver> to add server IP.
13. [ENHANCEMENT] Add a switch to control NAT IRC service turned on/off. We provide a new CI command “ip nat service irc <on|off>” to control the service.
14. [ENHANCEMENT] Send UNIX syslog for VPN LOG.
15. [ENHANCEMENT] Add new CI commands to filter netbios and broadcast packets. For netbios packets, they are “sys filter netbios”. Please refer to Appendix 4 for detailed description. And for broadcast packets, they are “sys filter blockbc <on|off>”. Broadcast packets will be applied here are DHCP packets and RIP packets.
16. [ENHANCEMENT] Add new CI commands to adjust MTU. For LAN side, it’s “ether edit mtu” and for WAN side, it’s “sys rn mtu”. For more detailed description, please refer to Appendix 3.
17. [ENHANCEMENT] Add a new CI command, “ipsec display <rule index>” to display IPSec rules.
18. [ENHANCEMENT] Add a new CI command, "ipsec dial <rule index>" to trigger the IKE procedure.
19. [ENHANCEMENT] Add a new CI command, "ip nat incike <on|off>", to increase IKE source port. This is used in NAT pass-through.
20. [ENHANCEMENT] Add a new C/I command "sys firewall dos ignore <lan|wan|dmz> [on|off]". For example, user can bypass DoS attack checking on LAN by using "sys firewall dos ignore lan on"
21. [ENHANCEMENT] Hard coded netbios filters work with port 445, which used by Windows 2000/XP.
22. [FEATURE CHANGE] IPSec related SMT and WEB wording changed.
23. [FEATURE CHANGE] MyIP and secure gateway address can be set to 0.0.0.0 at the same time.
24. [FEATURE CHANGE] Support LAN IP as MyIP.
25. [FEATURE CHANGE] CI commands for ipsec such as “ipsec sa” and “ipsec sa_sdb_status” are removed. To show SA status, we provide CI command “ipsec show_runtime sa”.
26. [FEATURE CHANGE] Phase 1 SA will time out. And its lifetime is independent from phase 2 SA lifetime.
27. [FEATURE CHANGE] Ipsec-related CI commands are visible.
28. [FETURE CHANGE] Dynamic rules will not conflict with static rules. Static rules have higher priority, and will be chose during runtime IKE procedure.
29. [FEATURE CHANGE] The repeated entries showed in VPN LOG are reduced.
30. [FEATURE CHANGE] Content filter and VPN pages in WEB are modified.
31. [FEATURE CHANGE] Accept peer’s SA lifetime set to both SEC and KB.
32. [BUG FIX] Use PPPoE / PPTP connection: after disconnection and then dial up again, if ZyWALL get new WAN IP, NAT mapping still used old IP address.
33. [BUG FIX] During IKE process, if SMT tried to save or delete that rule, sometimes system crashed.
34. [BUG FIX] Using VPN tunnel to transfer large file, sometimes after a period there cannot be any traffic pass through the tunnel.
35. [BUG FIX] Fragmentation problems have been fixed, including teardrop, full feature NAT and ACL block.
36. [BUG FIX] When ZyWALL as RESPONDER, it will accept all PFS setting from INITIATOR and does not check its own configuration.
37. [BUG FIX] Notify message <No proposal chosen> has incorrect format.
38. [BUG FIX] PFS has race condition. When two peers start to re-key simultaneously, sometimes one side will reject the connection.
39. [BUG FIX] Packets to LAN should not match a rule whose remote IP range is "all".
40. [BUG FIX] Broadcast DHCP reply packets are blocked.

41. [BUG FIX] Enlarge memory parameters to assure there exists enough memory for system operation after VPN tunnels are built.
42. [BUG FIX] After enable SUA, remote management to LAN IP via VPN tunnel failed.
43. [BUG FIX] After long time test, IPSec process will cause system lack of memory.
44. [BUG FIX] Under PPPoE connection, tunnel is built but no traffic can pass through it.
45. [BUG FIX] "ip nat reset enif1" don't work.
46. [BUG FIX] Firewall will check back-record for the TRACEROUTE reply to port unreachable of ICMP at the end host.
47. [BUG FIX] Static routed packets from LAN to LAN will be blocked by firewall.
48. [BUG FIX] Solve the SNMPv1 vulnerability problem.
49. [BUG FIX] Sometimes packets cannot pass through tunnel built from dynamic rule.
50. [BUG FIX] Routing cache calculation will overflow.
51. [BUG FIX] Manual key cannot swap from one rule to another, if these two rules have the same secure gateway.
52. [BUG FIX] When two peers initiate connections at the same time in some special cases, the two peers will reject each other and on tunnel can be established.
53. [BUG FIX] When building the tunnel, sometimes system will crash.

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

1. [ENHANCEMENT] When phase 2 id check fails, VPN LOG will show both peer ID information and system setting.
2. [FEATURE CHANGE] Add CLI support.
3. [FEATURE CHANGE] SMT24.7 wording changed.
4. [FEATURE CHANGE] In SMT27.1, "EDIT" will jump to the selected rule automatically
5. [BUG FIX] When using PPPoE encapsulation and turning on firewall, system is very unstable and it may crash.
6. [BUG FIX] When there are two active IPSEC rules with the same secure gateway, packets which should match the latter rule will still use the former rule for IKE process. In some cases, this will cause system to establish many invalid tunnels for one rule. At last, system does not have enough memory.
7. [BUG FIX] When encapsulation switches from Ethernet to PPPoE, IP Alias 2 will become “not available”.
8. [BUG FIX] Opera 6.0 cannot login eWC.
9. [BUG FIX] IP Alias cannot fake MAC address in SMT2 and WEB.
10. [BUG FIX] When firewall turned on, received a invalid AH packet (protocol 51) from LAN will cause ZyWALL crashed
11. [BUG FIX] Remove incorrect tag in WEB→WAN→PPPoE / PPTP
12. [BUG FIX] Smartbit test with 1 VPN tunnel cause ZyWALL crashed.
13. [BUG FIX] Typing “atgo” in debug mode, the restore default romfile ping didn’t work.
14. [BUG FIX] WEB: When modifying a used custom port, it will not apply to the rule using this custom port. If trying to remove the custom port from that rule, ZyWALL will crash.
15. [BUG FIX] After IKE re-keying procedure, some memory doesn’t be freed. After a long term test, system will have no free memory section.

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

1. [ENHANCEMENT] Add a new CI command “ipsec show_runtime sa” to show runtime phase 1 and phase2 SA information.
2. [ENHANCEMENT] Manual key SA will runtime creates when traffic matches SPD.
3. [ENHANCEMENT] SA monitor will show manual key SA, and command to delete it is available.
4. [ENHANCEMENT] Idle timer also applies on manual key SA. When no traffic transmits through the SA, system will delete it.
5. [ENHANCEMENT] VPN LOG is totally revised. Now it will show all IKE packets information. Besides, It will show error messages to identify the reason why connection cannot be built.

6. [ENHANCEMENT] IKE process in phase 2 will check ID information between system and the peer. If they don't match, i.e. both sites have different local / remote Addr setting, system will reject the connection and log in the VPN LOG.
7. [ENHANCEMENT] Simultaneous SA check: All VPN rules can be set to "ACTIVE", but only 50 runtime SA can be established at the same time.
8. [FEATURE CHANGE] Only the last rule (rule 60)can apply security gateway to "0.0.0.0".
9. [FEATURE CHANGE] Web (SUA/NAT) default DMZ server changes to default server.
10. [FEATURE CHANGE] Web status after saving configuration has changed to "Configuration updated successfully".
11. [FEATURE CHANGE] Put default PPTP settings(my PPTP IP and PPTP server IP) on Wizard.
12. [BUG FIXED] Cannot use IPSec tunnel for remote management.
13. [BUG FIXED] Remove non-configured filter set from remote node.
14. [BUG FIXED] Fix incorrect help page link in WEB.
15. [BUG FIXED] SMT 24.11 fail to control connections from WAN using LAN alias IP addresses.
16. [BUG FIXED] When firewall turns off and SUA only, PC in the WAN side can ping PCs in the LAN side.
17. [BUG FIXED] When the WAN side is using PPPoE connection and NAT turns off, firewall does not protect the LAN side.
18. [BUG FIXED] When the WAN side is using PPPoE connection, LAN-to-WAN ACL rule will not be applied. The Packet will transmit through firewall from LAN to WAN, even existing a firewall rule to block it.
19. [BUG FIXED] Web (Content filter→ EXEMPT ZONE) Apply button didn't work.
20. [BUG FIXED] VPN connection cannot be re-built after dynamic WAN IP being changed.
    →When one ZyWALL has "Secure Gateway IP Addr" to be "0.0.0.0" and the other one has "My IP Addr" to be "0.0.0.0", as below.

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

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

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

21. [BUG FIXED] VPN timeout re-connection function is not robust.
    → When "SA Life time" is time out, sometimes the VPN tunnel cannot be re-established again.
22. [BUG FIXED] VPN tunnel cannot be established if WAN IP is static without default gateway configured.
    →When a ZyWALL is configured as "static IP" but default gateway as "0.0.0.0", and the other ZyWALL is placed in the same subnet, the VPN tunnel cannot be established between them.
23. [BUG FIXED] VPN tunnel cannot work with multi-NAT.
24. [BUG FIXED] Use Web setup VPN for manual mode, it can not work until save in SMT again
25. [BUG FIXED] Web (Firewall) will show error messages when try to access help pages.
26. [BUG FIXED] When phase 2 SA life time out, sometimes there exists a phase 1 SA and no tunnel can be built.
27. [BUG FIXED] IPSEC pass through cannot support multiple sessions.
28. [BUG FIXED] NAT loopback server problem is solved. When a server in the LAN site and there exists a NAT server set directed to it, WAN site traffic can access the WAN IP, then be redirected to the server.

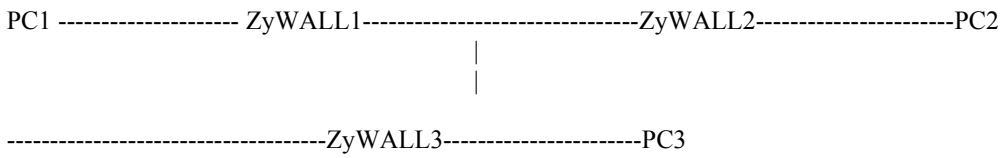
But the LAN site cannot use the WAN IP to access the server. It only can access the server through LAN IP. A new CI command "`ip nat loopback`" is added to turn on the feature, "NAT server loopback". When it turns on, PC on LAN site can access the LAN site server through WAN IP. NOTE: Turn on the feature will cause throughput decreased.

29. [BUG FIXED] POP3(TCP:110) didn't show on firewall pre-configured port.
30. [BUG FIXED] When VPN LOG recorded more than 64 entries, it will show incorrect format.
31. [BUG FIXED] Responder cannot find phase1 SA by address pair. This will cause sometimes phase 1 SA will remain after SA reconnection
32. [BUG FIXED] Web VPN LOG format corrected.
33. [BUG FIXED] When receive deleting phase 1 packet, system will only delete phase 1 SA and let an useless phase2 SA alive. This will cause a long delay to reconnection.
34. [BUG FIXED] Wrong wording in content filter log.
35. [BUG FIXED] Time initialized won't show in the content filter and firewall logs.
36. [BUG FIXED] In firewall log mail, the header contained wrong date display.
37. [BUG FIXED] IPALIAS didn't apply firewall LAN-to-WAN ACL rules.
38. [BUG FIXED] Web configurator (VPN / Content filter) cannot be accessed by Netscape 4.78
39. [BUG FIXED] In b6, Web configurator (WAN→PPPoE / PPTP) will cause system crashed
40. [BUG FIXED] With PPPoE / PPTP configured, but no dial-up, system would crash after typing "ip ro st" in CI command mode.
41. [BUG FIXED] DNS proxy can't get the address when the original DNS server failed.
42. [BUG FIXED] In debug mode, command "atgo" will cause RAS to restore default romfile.
43. [BUG FIXED] After PPTP connection built, system would crash.
44. [BUG FIXED] When SNMP query through the system, it would crash.
45. [BUG FIXED] IPAlias couldn't work.
46. [BUG FIXED] In SMT 24.6, interrupt the upload procedure would cause system crashed.
47. [BUG FIXED] Web (WAN→MAC): if MAC spoofing is active, change configuration back to "factory default" will not apply at the same time. System must be reboot to make change done.
48. [BUG FIXED] After applying MAC spoofing, both WAN and LAN MAC will be changed to be the same as PC.
49. [BUG FIXED] Content filter cannot get the list.
50. [BUG FIXED] Content filter configuration behavior modified. Configuration changes will not be saved unless press the "apply" button. "Reset" button will clear all configuration changes and reload the page.
51. [BUG FIXED] System hanged during smart-bit testing (100M ←→100M).
52. [FEATURE CHANGE] When system crashes, it will not stop in the screen. Instead after showing memory dump, system will reboot automatically.
53. [ENHANCEMENT] In firewall setup, IKE (UDP:500) is placed in standard protocol instead of custom port. Default romfile changed.
54. [ENHANCEMENT] VPN logs and debug messages were modified to be much readable.
55. [ENHANCEMENT] When dynamic WAN-IP changes, system will disconnect all VPN connections which MyIP is "0.0.0.0".
56. [ENHANCEMENT] When VPN connection has no traffic through it for a period, it will disconnect automatically.
57. [ENHANCEMENT] Add two new CI commands in "ipsec timer" to configure VPN timers.
58. [BUG FIXED] SMT 27.1.1.1 pre-shared key check error.
59. [ENHANCEMENT] Enhanced Ethernet driver.
60. [ENHANCEMENT] Enhanced firewall stability.
61. [BUG FIXED] Restore default romfile can not work in V3.50(WC.0)b4.
62. [BUG FIXED] When DHCP server and DHCP relay exist in the same network providing ZyWALL50 IP address, saving configuration will not be correct.
63. [BUG FIXED] Content filter keyword blocking didn't work.
64. [ENHANCEMENT] System stability enhanced.
65. [BUG FIXED] System crashed by unusual IKE message.
66. [BUG FIXED] Fix IPSec configuration bugs.
67. [BUG FIXED] Debug messages removed.
68. [ENHANCEMENT] Speed up flesh writing process.
69. [BUG FIXED] IPSec rule name disappear.

70. [BUG FIXED] Console login didn’t kick out web configurator.
71. [BUG FIXED] Debug messages removed.
72. [BUG FIXED] When use web to configure IPSEC, system crashed.
73. [BUG FIXED] When use web to move firewall rules, system crashed.
74. [BUG FIXED] When use web to configure Content Filter, system crashed.
75. [BUG FIXED] VPN failed when transmitting large packets.
76. [BUG FIXED] SA monitor was incorrect.
77. [ENHANCEMENT] System stability enhanced.
78. [ENHANCEMENT] Add support for reset button (restore default romfile).

Appendix:

1. Example for configuring security gateway to be 0.0.0.0.



SMT27.1.1 of ZyWALL1:

```
                    Menu 27.1.1 - IPSec Setup

Index #= 10         Name= ZyWALL1
Active= Yes

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

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

SMT27.1 of ZyWALL1 will show:

```
                          Menu 27.1 - IPSec Summary

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

003

004

005


             Select Command=  None          Select Rule=  N/A

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

SMT27.1.1. of ZyWALL2:

```
                          Menu 27.1.1 - IPSec Setup

          Index #= 1         Name= ZyWALL2
          Active= Yes

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

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

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

```
                                        Menu 27.2 - SA Monitor

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

                  Select Command= Refresh
                  Select Connection= N/A

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

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

NOTE:

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

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

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

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

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

3. Procedure to set MTU for LAN and WAN.

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

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

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

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

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

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

Example output:

```
================ NetBIOS Filter Status ================
 LAN to WAN:            Non-blocking
 LAN to DMZ:            Non-blocking
 IPSec Packets:         Non-blocking
 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	Non-blocking
1	LAN to DMZ	Non-blocking
2	IPSec pass through	Non-blocking
3	Trigger dial	Disabled

Example commands:

```
sys filter netbios config 0 on      => block LAN to WAN NB/IP packets
sys filter netbios config 1 off     => pass LAN to DMZ NB/IP packets
sys filter netbios config 2 on      => block IPSec NB/IP packets
sys filter netbios config 3 off     => disable trigger dial
```

5. Static Route Application Note

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

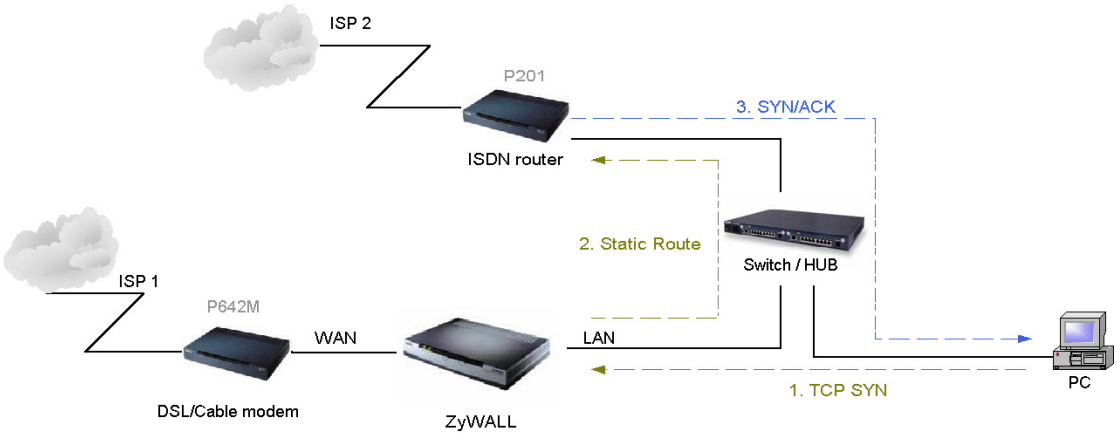


Figure 5-1 Triangle Route

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

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

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

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

How static route works under protection - Solutions

(1) Gateway on alias IP network

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

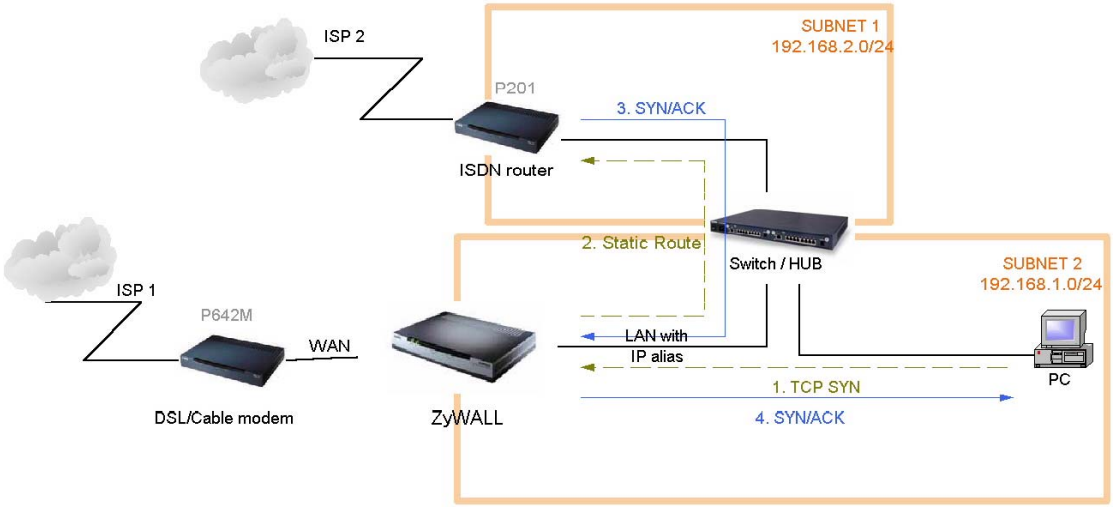


Figure 5-2 Gateway on alias IP network

(2) Gateway on WAN side

A working topology is suggested as below.

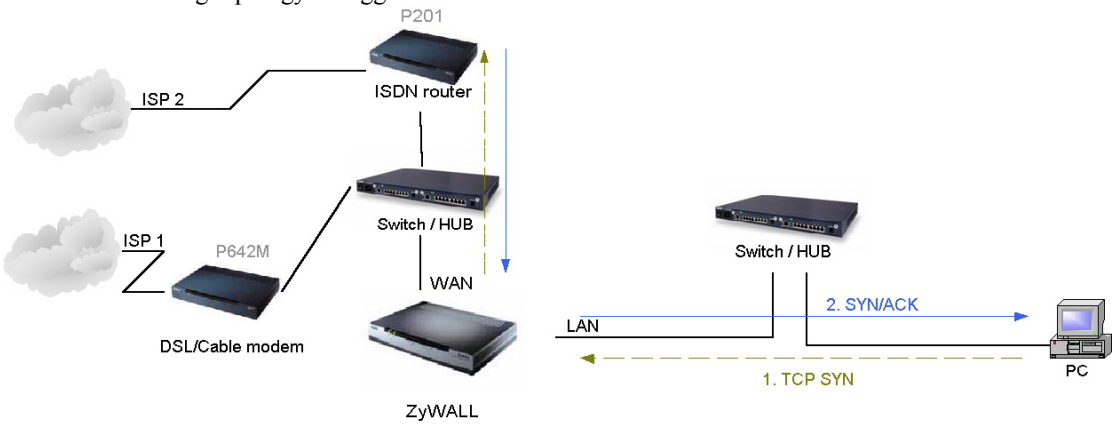


Figure 5-3 Place other gateways on WAN side