ZyXEL Prestige P312 Release Note/Manual Supplement

Date: October 15, 2001

ZyNOS V3.50(S.00) | 10/11/2001

Support Platforms:

ZyXEL Prestige firmware V3.50(S.00) Firewall supports the P312 two-LAN router hardware.

Version:

ZyNOS F/W Version: V3.50(S.00)

Note: FTP firmware uploading is not supported if you try to update the firmware from V3.2x to V3.5x. It is because the memory allocation for FTP firmware uploading in 3.2x is smaller than 3.5x, thus it is not big enough to store the bigger firmware size of 3.5x release. It is around 1.2M.

In this case, TFTP or Console is suggested for firmware update.

It will not be a problem for uploading from 3.5x to 3.5x since the memory allocation is the same. Only 3.2x to 3.5x is a gap.

Note:

1. The default romfile is 350S00C0.rom
2. Firmware name 350S00C0.bin

Known Bug:

1. 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.
2. VPN timeout re-connection function is not robust.
   →When “SA Life time” is time out, sometimes the VPN tunnel cannot be re-established again. To avoid this, a longer life time setting or manual disconnect is suggested.
3. VPN tunnel cannot work with multi-NAT.
4. 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.

New Feature:

1. NAT

  - -multi-session IKE support
  - -NAT multi-session IPSec-ESP-Tunnel support
  - -NAT range port forwarding support

2. IPSec
   - -Supports IKE for automatic security negotiation and key management
   - -Currently using pre-shared authentication keys for establishing trust between hosts.
   - -Provides DES (56-bit key strength) and 3DES (168-bit key strength) encryption algorithms
   - -SHA-1 and MD5 integrity algorithms for ESP.
   - -SHA-1 and MD5 integrity algorithms for AH.
   - -Provide ESP Tunnel mode, Transport Mode
   - -Provide AH Tunnel mode, Transport Mode

Bug Fix:

1. Fix multi-language support
2. Fix web configuration delete firewall rule error
3. Fix firewall crash problem under heavy ftp traffic
4. Fix Download content filter cannot success
5. Fix ip traceroute cannot work
6. Fix web configuration cannot reset to factory default
7. Fix web configuration cannot add more than one rule in firewall
8. Fix static routing cannot work when firewall on
9. Fix Firewall web configuration make buffer overflow
10. Fix cannot upload firmware by web
11. content filter register error
12. content filter list download error
13. ESP teardrop attack parser error
14. DNS lookup fail when menu 3.2 "DHCP server == None"
15. Fix SNMPv2 packet make router reboot
16. Fix Router crash when doing reconfiguration

Date: December 11, 2000

ZyNOS V3.20(S.01) | 12/11/2000

Support Platforms:

ZyXEL Prestige firmware V3.20(S.01) Firewall supports the P312 two-LAN router hardware.

Version:

ZyNOS F/W Version: V3.20(S.01)

Note:

1. The default romfile is 320S01.rom
2. Firmware name 320S01.bin

Bug Fix:

Fix menu 11.3 make system crash when choosing pptp

Date: November 23, 2000

ZyNOS V3.20(S.00) | 11/23/2000

Support Platforms:

ZyXEL Prestige firmware V3.20(S.00) Firewall supports the P312 two-LAN router hardware.

Version:

ZyNOS F/W Version: V3.20(S.00)

Note:

3. The default romfile is 320S00.rom
4. Firmware name 320S00.bin
5. IE (4.X and 5.X) will keep user' s login name and password. This makes Web Authentication not work.

New Feature:

Add Content Filter
Add new web configuration for Content Filter
Add new web configuration for NAT
Add new web configuration for LAN
Add new web configuration for WAN
Add SMTP "AUTH" support
add Nail-Up in menu 11.2
performance enhancement
Add CI command to turn on/off RST (default value: off , except port 113)
WEB URL Filter
Cookei Filter
Java Applet Filter
Proxy Filter
ActiveX Filter
Multimedia application support for Firewall. (Netmeeting, RealPlayer7, Quicktime ..).
PPTP, IGMP, IPSEC(ESP) support for Firewall
IPSEC SEC (Tunnel mode) support for NAT
Embedded Web Server for Firewall configuration.
PPTP Clinet
Dynamic DNS
Telnet client
Traceroute
Command line history
Sending firewall log by syslog
SNMP management
IP alias
IP Multicast
Call Scheduling

WEB Configuration:

Login name: admin
Password: 1234

Currently, web configuration only support firewall. Advance menu

Telnet Clinet / Traceroute Client / Command Line History:

Teracetoute:
1. enter menu 24.8
2. use CI command “ip traceroute <host> [ttl] [wait] [queries]”

Telnet
1. enter menu 24.8
3. use CI command “ip telnet <hostname>

Command Line History
1. Set terminal type to “VT100”

Applications Firewall Supports:

1. To support a certain application when the firewall is on, an appropriate policy rule is needed.
2. MIRC, ICQ and RealPlayer work under the default firewall configuration.
3. The following are additional configurations for some applications to work properly.
   a. Cu-SeeMe:

   For outgoing connections (from LAN to WAN), using the default firewall configuration is OK.

   For incoming connections (from WAN to LAN) do the following:

      LAN to WAN set: default configuration is OK.

      WAN to LAN set: add a rule to allow UDP packets with destination ports 7648 and 24032.

   If the configuration is correct, but the connection is still not up, then extend the UDP idle-timeout, e.g., from a number in the 20s to a number in the 60s.

   b. Quick Time:

   It is necessary to add a rule in the WAN to LAN set to allow UDP packets with source ports 2000 and 2001. It is OK for LAN-to-WAN direction to use the default firewall configuration.

   c. Eudora:

   For outgoing connections (from LAN to WAN), using the default firewall configuration is acceptable.

   For incoming connections (from WAN to LAN):

      LAN to WAN: using the default configuration is OK;

      WAN to LAN: add a rule to allow TCP packets with destination ports 25 and 110.

4. VDO Live

ACL allows packet with destination port 7000 pass. This rule will allow for a VDO LIVE to be run behind firewall on port 7000.

5. IRC

ACL allows packet with destination port 6667 pass. This rule will allow for a IRC to be run behind firewall on port 6667.

6. Quake3

ACL allows packet with destination port 27960 pass. This rule will allow for a Quake3 to be run behind firewall on port 27960.