ZyXEL Prestige 312 (Firewall)

ZyNOS v3.00(S.00) | 05/30/2000

Release Notes & Manual Supplement

Date: May 30, 2000

Supported Platforms:

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

Version:

ZyNOS F/W Version: V3.00(S.00) | 5/30/2000 16:38:41
BootBase: v1.13 for P312

Note:

1. The default configuration (rom-0) filename is: **p312.rom**
2. The binary ZyNOS firmware (ras) filename is: **p312.bin**

New Features:

1. NAT

   Prestige has a full feature NAT function supporting 1-1, Many-1, Many-Many Overload, Many-Many Non-Overload and Server mapping. To those thinking SUA is enough, they can switch to "SUA only" in SMT menu 11.3 or SMT menu 4. Menu 15 has two sub menus. Menu 15.1 is for NAT rules. Set 1 applies to the traffic when a user selects the NAT FULL FEATURE. Set 255 is only for SUA usage, which is not configurable. Menu 15.2 is the same as the SUA Setup option in the P310.

2. Firewall:

   When a user turns on firewall through PNC or SMT menu 21.2, the firewall will protect LAN networks and the Prestige from Denial of Service attacks. For further requirements, a user can configure policy rules to meet them. The default setting for the firewall is "Active" (i.e., on) in the P312. To configure the firewall, a user can use menu 21.2 to switch it on/off. Menu 21.3 displays the firewall log. If a user want to configure his own firewall policy and alerts, please use the PNC. **For those requiring high security, please turn off FTP and configure ONE (only) IP for TELNET access using menu 24.11.**

3. Real Time Setup:

   Through SMT menu 24.10, the user can type in the real time or configure an appropriate protocol to get real time from the Internet. There are three protocols to choose from: NTP, Daytime, and Time.

4. Remote Management Setup:

   Through SMT menu 24.11, the user can shut down Prestige TELNET and FTP service. If a user enables TELNET service, he/she can select one IP address in his/her LAN network to be the only secure administrator.

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. NetMeeting and other H.323 related applications might not work under the firewall. We are currently investigating how to support them appropriately.