ZyXEL Prestige P312 Release Note/Manual Supplement

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:

1. The default romfile is 320S00.rom
2. Firmware name 320S00.bin
3. 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.