



Firmware Release Note

Prestige 652R-13

Standard version

Release 3.40(FW.7)C0

Date: June 18, 2003
Author: Brian Chung

ZyXEL Prestige 652R-13 Standard Version release 3.40(FW.7)C0 Release Note

Date: June 18, 2003

Supported Platforms:

ZyXEL Prestige 652R-13

Versions:

ZyNOS F/W Version: V3.40(FW.7) | 6/18/2003 16:37:40

Bootbase Version: V1.06 | 9/3/2002 11:07:17

Notes:

1. The Prestige 652R-I, is an ADSL over ISDN security router with built-in powerful firewall capabilities and secure Virtual Private Network (VPN), which are designed for small and medium-sized businesses (SMBs), and enterprises' branch offices. The high-performance firewall capabilities and VPN secure data transmission over the public Internet and protect Internal network resources from unauthorized access.
2. Alcatel modem code version is 4.9.10

Known Issues:

1. Currently, UPNP not support MSN 5.0
2. Update firmware issue :
 - 1) Update firmware from 3.40(FW.5) to 3.40(FW.7) :
 - a. Update firmware by FTP : have to update to 3.40(FW.6) first, then update to 3.40(FW.7).
 - b. Update firmware by console : just update firmware from 3.40(FW.5) to 3.40(FW.7)
 - 2) Update firmware from 3.40(FW.6) to 3.40(FW.7)
 - a. Update firmware by FTP : just update firmware from 3.40(FW.6) to 3.40(FW.7)
 - b. Update firmware by console : Can't update firmware from 3.40(FW.6) to 3.40(FW.7) by console.

[CI Command List:](#)

Features:

Modification in 3.40(FW.7) | 06/18/2003

1. Change to FCS version.

Modification in 3.40(FW.7)b1 | 05/30/2003

1. [FEATURE CHANGED]
Integrate Errlog, Firewall log, VPN log and Content filter log into Centralized log.
SMT menu : Remove firewall log (menu 21.3), VPN log (menu 27.3); Modify Unix syslog (menu 24.3.2).
WEB page : Remove log of Content filter ,Firewall page and VPN page. Add new page of Centralized log.
CI command : Add “logs” to replace “log”. Please refer to CI command list.
2. [FEATURE ENHANCED]
Symptom: Extend to 5 IPsec sessions.
3. [FEATURE CHANGED]
Symptom: Change modem code version to 4.9.10
4. [FEATURE ENHANCED]
Symptom: Add NetBIOS passthrough for IPsec.
Usage: Using ci-command “sys filter netbios config <6:IPsec pass through><on|off>” or eWC.
5. [FEATURE ENHANCED]
Add FQDN feature for IPsec. See [Appendix 3](#).
6. [FEATURE ENHANCED]
Add KeepAlive feature for IPsec.
7. [NEW FEATURE]
Symptom: Support Goalie CNM (Centralized Network Management) feature.
CI command “cnm active 1” could be used to active this feature. The default is inactive. CI command “cnm managerIp xxx.xxx.xxx.xxx” is used to specify the IP address of the ZyXEL’s CNM management station. For details for CNM, please reference to the User Guide for CNM.
8. [FEATURE CHANGED]
Add firewall rule BOOTP_CLIENT(UDP:68) for default ROM file setting.
Disable multicast option in SMT menu 3.2 for default ROM file setting.
9. [FEATURE ENHANCED]
Add WAN eWC page to config WAN setting.
10. [FEATURE ENHANCED]
Symptom: Enhance traffic redirect and dial backup feature. Add WAN backup eWC.
11. [FEATURE CHANGED]
Symptom: Minimum of IPsec phase 1 and phase 2 SA lifetime enlarge from 60 seconds to 180 seconds.
12. [FEATURE ENHANCED]
Symptom: SPTGEN feature enhancement.
Condition:
 - 1) Add RIP direction and version for SMT menu4.
 - 2) Add active and protocol option for SMT menu15 (NAT).
 - 3) Extend filter set from 1 to 2 set.Support ADSL opencmd function.
13. [FEATURE ENHANCED]
Symptom: When the remote address range and local address range overlap in a IPsec rule, packets from local to local can skip this rule for checking. For example, a rule: local=> start= 192.168.1.0 mask= 255.255.255.0; remote=> start= 192.168.0.0 mask= 255.255.0.0. Then user can define if a packet from 192.168.1.2 to 192.168.1.3 matches this rule.
Note: 1. Please use "ipsec swSkipOverlapIp <on|off>" to control this behavior. When it's "on",

then the packet "192.168.1.2 to 192.168.1.3" will skip this rule.

2. The default setting of swSkipOverlapIp is "off"

14. [FEATURE CHANGED]

Symptom: Add back the inbound idle timer. When a tunnel has no inbound traffic for a certain period, the tunnel will be dropped.

Note: 1. Please use "ipsec timer chk_input <minute> to configure this timer. 2. A value "0" means disable this timer. 3. The default value is "disabled". 4. The inbound idle timer can work with existed "idle timer". The latter monitors if a tunnel with "only outbound traffic but no inbound traffic" for a certain period, and then delete that tunnel.

15. [BUG FIXED]

Symptom: Sometimes IPSec rekey procedure failed.

Condition: Under heavy traffic, sometimes IPSec rekey failed.

16. [BUG FIXED]

Symptom: Two IPSec hosts can establish IPSec connection when one uses main mode and the other chooses aggressive mode.

Condition: When local and peer hosts use different IKE phase1 negotiation mode, they still can establish IPSec connection.

17. [BUG FIXED]

Symptom: In LAN setup page, the IP address can not be xxx.xxx.255.xxx

18. [BUG FIXED]

Symptom: Nailed-up function can't work for Dial backup node.

Condition: Dial backup node can set nailed-up option but this feature can't really work.

19. [BUG FIXED]

Symptom: System reboot when user disconnect established PPTP session.

Condition: 1). Setup PPTP session through P652, 2) do some ping test then disconnect PPTP session will cause device reboot.

20. [BUG FIXED]

Symptom: If the traffic for Polycom camera pass our router, the router would be reboot.

Condition: Polycom camera is implemented by H.323. So our router would do nat for this device.

21. [BUG FIXED]

Symptom: Can't set nailed-up and budget at the same at eWC for wan backup feature.

Condition: For wan backup feature at eWC, can't set nailed-up and budget at the same time.

Modification in 3.40(FW.6)C0 | 03/07/2003

1. Change to FCS version.

Modification in 3.40(FW.6)b2 | 12/27/2002

1. [FEATURE ENHANCED]

Symptom: Add Initial Contact for IPSec.

Condition: Add Initial Contact to differentiate it's first contact or reboot contact.

2. [BUG FIXED]

Symptom: Remote management can't work over IPSec tunnel.

Condition: Remote management can't work over IPSec tunnel. It must set access = ALL in SMT menu 24.11.

3. [BUG FIXED]

Symptom: Unix syslog can't work.

Condition: Unix syslog can't work on LAN side or WAN side.

4. [FEATURE ENHANCED]

Symptom: Support VPN and Firewall log into Unix syslog.

Modification in 3.40(FW.6)b1 | 12/19/2002

1. [FEATURE CHANGED]
Change Rom file setting at SMT menu 3.2 (Multicast = None).
Menu 11.3 for dial backup node (NAT = SUA Only).
2. [FEATURE CHANGED]
Change modem code version to 4.9.8
3. [FEATURE ENHANCED]
Add Traffic Redirection Feature. See [Appendix 2](#).
4. [BUG FIXED]
Sympton: Alcatel DSP code hang problem
Condition: Sometimes Alcatel DSP will hang up and loss communication with Host.
5. [BUG FIXED]
Sympton: The system will allow the packet with DF=1 and packet length > MTU to pass through the router without any error message returned to the sender.
Condition: When the packet with it's length > MTU and don't fragment bit is set, the packet is allowed to pass through the router.
6. [BUG FIXED]
Sympton: Memory leakage occurred when ADSL dropped and plug-in.
Condition: When ADSL line link down/link up, the bridge remoteNode would allocate Local Cache Table. But the memory free had not done.
7. [BUG FIXED]
Sympton: Heavy OAM packets would let our system exception.
8. [BUG FIXED]
Sympton: Nailed-up don't work sometimes.
Condition: Sometimes PPPoA / PPPoE couldn't connect with DSLAM.

Modification in 3.40(FW.5)b6 | 10/1/2002

1. [BUG FIXED]
Sympton: NAT server and Firewall cause 4-byte boundary problem.
Condition: While enable NAT server and Fireall, sometimes access NAT server from wan side will cause router reboot.

Modification in 3.40(FW.5)b5 | 9/26/2002

1. [BUG FIXED]
Sympton: Snmp cause system reboot.
Condition: While testing SNMP with MIB Browser will cause system reboot.
2. [FEATURE EHHANCED] WEB: Modify the Firmware upload successful message page.

Modification in 3.40(FW.5)b4 | 9/24/2002

1. [FEATURE EHHANCED] WEB: Modify the restore factory configuration file page.

Modification in 3.40(FW.5)b3 | 9/20/2002

1. [BUG FIXED]
Sympton: Dial-backup doesn't redirect to SUA-Server.
Condition: While traffic redirect to dial backup port, user can't access SUA-Server at P652's Lan side.
2. [FEATURE EHHANCED] Add subnet mask field in WEB GUI wizard of ENET ENCAP

Modification in 3.40(FW.5)b2 | 9/13/2002

1. [BUG FIXED]

Symptom: NAT server set in WEB can't work if we set the Rule 1.

Condition: In WEB, while we set the NAT Server set at rule 1, it can save but can't work fine.

2. [BUG FIXED]

Symptom: VPN log in WEB is unreadable.

Condition: In web VPN log, the display is unreadable. It should be in order by topic index.

3. [BUG FIXED]

Symptom: Web page display will be out of order.

Condition: In Web configuration, the column will out of order while we set firewall rule set then enable Upnp.

4. [BUG FIXED]

Symptom: UPNP and Dial backup without Web help page

5. [BUG FIXED]

Symptom: Under VPN channel, when sending large ICMP packet size more times, the NAT session table will full.

Condition: While Prestige be a VPN passthrough device. When continuously sending large ICMP packet size, the NAT session table will full, then the Prestige can't forward any packet.

6. [FEATURE ENHANCED] Add ESP protocol display information in CI command "ip nat if wanif0". Originally, the device display the protocol as unknown protocol.

Modification in 3.40(FW.5)b1 | 9/5/2002

1. [FEATURE CHANGED] Change the default value of resolving IPsec peer's DNS. The value is changed from 30 min to 15 min.

2. [FEATURE ENHANCED] Support IEEE 802.1q VLAN-tagging bridging.

3. [NEW FEATURE] Support Dial backup. Add dial backup item in WEB and menu 2 in SMT. The remote node no.8 is reserved for Dial-backup use. See [Appendix 1](#)

4. [NEW FEATURE] Support UPNP. Add UPNP item in WEB.

5. [BUG FIXED]

Symptom: length of PPPoE/PPPoA idle timeout is different between SMT menu and WEB wizard setup.

Condition: Length of idle timeout in SMT menu is 5, but in WEB wizard is only 3.

6. [BUG FIXED]

Symptom: console kick out telnet session cause router reboot.

Condition: While access router by telnet and view firewall log in menu 21.3, disconnect telnet by console cause router reboot.

Modification in 3.40(FW.4)b1 | 8/26/2002

1. [BUG FIXED]

Symptom: Router power on will get the information "Decompressed image checksum Error".

Condition: While reboot router will get the information "Decompressed image checksum Error" and enter debug mode

Modification in 3.40(FW.3)b5 | 8/1/2002

1. [BUG FIXED]

Symptom: console kick out telnet session cause router reboot.

Condition: While access router by telnet and view firewall log in menu 21.3, disconnect telnet by console cause router reboot.

2. [BUG FIXED]

Symptom: Web help dose not update PPP to PPPoA

Condition: Web help dose not update PPP to PPPoA

3. [BUG FIXED]

Symptom: In WizardSetup, user name of PPPoE/PPPoA have problem if user name length more than 70 characters.

Condition: While set User name of PPPoE/PPPoA is more than 70 characters then save, then check again. User name will be 70 characters+password.

4. [BUG FIXED]

Symptom: IPSEC Phase 2 PFS can't work.

Condition: When P652 build up VPN tunnel to ZW-10 or ZW-50, no matter what settings in phase 1 or in phase 2 are used, VPN tunnel does not work when PFS in phase 2 is enabled. But when PFS is disabled, the VPN connection works just fine.

Modification in 3.40(FW.3)b4 | 7/30/2002

1. [EHHANCEMENT] Change "PPP" to "PPPoA" in SMT menu and WEB
2. [EHHANCEMENT] Update bootbase to 1.05 to differentiate model name in SMT Main Menu.
3. [EHHANCEMENT] Extend PPPoE/PPPoA login User Name to 70 characters.

Modification in 3.40(FW.3)b3 | 7/24/2002

1. [BUG FIXED]

Symptom: Set ISP UserID by SPTGen fail

Condition: While UserID > 32 characters, set ISP UserID by SPTGEN will fail.

2. [BUG FIXED]

Symptom: atm RX ISR doesn't judge the RX_BAD_BIT

Condition: While a error packet into router, atm RX ISR doesn't judge the RX_BAD_BIT, so we receive the error packet. Exactly, we should discard the error packet.

3. [BUG FIXED]

Symptom: Write DyingGasp isr message into flash will destroy debug area.

Condition: Write DyingGasp isr message into flash will destroy debug area.

4. [EHHANCEMENT] Enhance SPTGEN to support Nailed-up Connection item.

5. [EHHANCEMENT] Add a CI command ""wan adsl rsploss 0/1" to response signal loss immediately or not.

Bug fixes in 3.40(FW.3)b2 | 7/9/2002

1. [BUG FIXED] Fix the bug that can't save 2nd VPN tunnel while have same local ip address with 1st tunnel.
2. [BUG FIXED] Fix the bug that press return key in SMT menu continuously cause router hang-up.
3. [BUG FIXED] Fix the bug that while firewall is enable, change PPPoE to RFC-1483 (or PPP) then PC on LAN can ping out but FTP and WEB can't work.

Modification in 3.40(FW.3)b1 | 7/5/2002

1. [FEATURE EHHANCED] Add attention note in SMT menu 27.1 and VPN web page.
2. [FEATURE EHHANCED] Modify SPTGEN to support SMT menu 23.
3. [BUG FIXED] Fix the bug of TCP attack packet.
4. [BUG FIXED] Fix the mbuf leakage problem.
5. [BUG FIXED] Fix the plug and unplug problem.
6. [BUG FIXED] Fix the bug that IE 5.0.3315 can't upload F/W.
7. [BUG FIXED] Fix the bug that IPsec rule conflict check error.

Modification in 3.40(FW.1)b2 | 6/11/2002

1. [BUG FIXED] Fix the SPTGEN problem : after put rom-t to router, name of ISP node in SMT11 will change to BACKUP_ISP.
2. [BUG FIXED] Some incorrect operation in SMT will cause router hang-up.

3. [BUG FIXED] Configure NAT server set in port range 1~2000, first ping packet cause router hang-up.

Modification in 3.40(FW.1)b1 | 6/6/2002

1. [FEATURE EHHANCED] Web timer server support domain type.
2. [BUG FIXED] Fix the bug that upgrade to old version firmware have problem.
3. [BUG FIXED] Fix the SPTGEN problem : pppoe can't work.
4. [BUG FIXED] Fix the bug that configure NAT server set will save to wrong index.
5. [BUG FIXED] Fix the checksum error bug in IGMP packet.
6. [BUG FIXED] Fix the pt field error bug in OAM packet.

Bug fixes in 3.40(FW.0)b11 | 5/23/2002

1. [BUG FIXED] Fix the bug that Web atm loopback test can't work if set boot module debug flag=0x00.

Modification in 3.40(FW.0)b10 | 5/22/2002

1. [BUG FIXED] Fix the bug that config NAT in WEB (not save yet) will disconnect all connection.

Modification in 3.40(FW.0)b9 | 5/22/2002

1. [FEATURE CHANGED] Don't log timer server initialized message into FW and CF log.
2. [BUG FIXED] Fix the bug that enter SMT11 submenu cause dialout username = ?.
3. [BUG FIXED] Fix the bug that while set customized service port > 8 will cause firewall rule dest. "ANY" address invisible.
4. [BUG FIXED] Fix the bug that WEB LAN subnetmask setting can't work.
5. [BUG FIXED] Fix the firewall ACL set services as none bug.
6. [BUG FIXED] Fix the bug that WEB timer server can't work well in NTP server mode.
7. [BUG FIXED] Fix the bug that set WEB time zone option will disable server ip field.

Modification in 3.40(FW.0)b8 | 5/17/2002

1. [FEATURE EHHANCED] Support smartbit TERA VPN testing.
2. [BUG FIXED] Fix the bug that VPN phase2 KB can't work.

Modification in 3.40(FW.0)b7 | 5/15/2002

1. [BUG FIXED] Fix the bug that web can't upgrade firmware.
2. [BUG FIXED] Fix the bug that SMT24.10 ENTER key will delete the timer server value.
3. [BUG FIXED] Fix the bug that E-net default gateway is set, when wan is up cause system hang.
4. [BUG FIXED] Fix the bug that SMT delete ISP node, web wizard config at first time can't save VPI/VCI.
5. [BUG FIXED] Fix the bug that firewall log loss some information.
6. [BUG FIXED] Fix the bug that firewall customer service rule no.4 show the wrong value.

Modification in 3.40(FW.0)b6 | 5/10/2002

1. [BUG FIXED] Fix the bug that can't del firewall wan to lan dest. adds.
2. [BUG FIXED] Fix the bug that when PPP is conneting , change to RFC-1483 or E-net cause exception.
3. [BUG FIXED] Fix the bug that SMT delete default remote node, Web wizard config., then SMT11 shows set = 1,1,1,1

Appendix 1 : Dial-Backup

Introduction

The features are used to keep Internet connectivity of the Prestige. The Connectivity Monitor is running at interval to detect the ADSL line status. Once the Prestige has detected the ADSL line is broken, it tries to forward the traffic to dial backup port.

Menu 2 - Dial-Backup Setup

```
Menu 2 - Dial Backup Setup

Dial-Backup:
  Active= No
  Port Speed= 115200

AT Command String:
  Init= at&fs0=0

Edit Advanced Setup= No

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

```
Menu 2.1 - Advanced Dial Backup Setup

AT Command Strings:
  Dial= atd
  Drop= ~~~~~ath
  Answer= ata

Drop DTR When Hang Up= Yes

AT Response Strings:
  CLID= NMBR =
  Called Id=
  Speed= CONNECT

Call Control:
  Dial Timeout(sec)= 60
  Retry Count= 0
  Retry Interval(sec)= N/A
  Drop Timeout(sec)= 20
  Call Back Delay(sec)= 15

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

This menu setup the dial device, which is typically an analog modem or ISDN TA. To activate the dial device, please toggle "Active" to "YES".

Menu 11.1 - Backup ISP Setup

```
Menu 11.1 - Remote Node Profile (Backup ISP)

Rem Node Name= ?
Active= Yes

Outgoing:
My Login=
My Password= *****
Authen= CHAP/PAP
Pri Phone #= ?
Sec Phone #=

Edit PPP Options= No
Rem IP Addr= ?
Edit IP= Yes
Edit Script Options= No

Telco Option:
Allocated Budget(min)= 0
Period(hr)= 0
Nailed-Up Connection= No

Session Options:
Edit Filter Sets= No
Idle Timeout(sec)= 100

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

A valid pair of login username and password is required. And the phone number of ISP is required. Leave "Rem IP Addr" to 0.0.0.0 makes Prestige try to get its IP address from ISP.

```
Menu 11.3 - Remote Node Network Layer Options

IP Options:
IP Address Assignment= Static
Rem IP Addr= 0.0.0.0
Rem Subnet Mask= 0.0.0.0
My WAN Addr= 0.0.0.0

Bridge Options:
Ethernet Addr Timeout(min)= N/A

NAT= SUA Only
Address Mapping Set= N/A
Metric= 2
Private= No
RIP Direction= None
Version= RIP-1
Multicast= None
IP Policies=

Enter here to CONFIRM or ESC to CANCEL:
```

Typically, "NAT" should be "SUA Only".

Appendix 2 : Traffic Redirect

Introduction

The features are used to keep Internet connectivity of the Prestige. The Connectivity Monitor is running at interval to detect the ADSL line status. Once the Prestige has detected the ADSL line is broken, it tries to forward the traffic to another gateway that user has specified.

Menu 11.1 – Traffic Redirect Setup

```
Menu 11.1 - Remote Node Profile

Rem Node Name= ISP                Route= IP
Active= Yes                       Bridge= No

Encapsulation= ENET ENCAP        Edit IP/Bridge= No
Multiplexing= LLC-based          Edit ATM Options= No
Service Name= N/A

Incoming:                          Telco Option:
  Rem Login= N/A                 Allocated Budget(min)= N/A
  Rem Password= N/A             Period(hr)= N/A
Outgoing:                          Schedule Sets= N/A
  My Login= N/A                 Nailed-Up Connection= N/A
  My Password= N/A             Session Options:
  Authen= N/A                  Edit Filter Sets= No
                               Idle Timeout(sec)= N/A
                               Edit Traffic Redirect= Yes

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

```
Menu 11.7 - Traffic Redirect Setup

Active= No
Configuration:
  Backup Gateway IP Address= 0.0.0.0
  Metric= 15

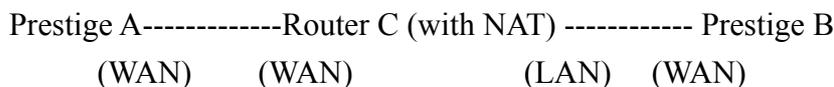
Press ENTER to Confirm or ESC to Cancel:
```

- (1) Configure "Active" to "YES" if you want this feature work.
- (2) "Backup Gateway". When the ADSL line is broken, traffic will be handed over to this backup gateway. [In IP address format]
- (3) "Metric". The default value is 15.

Note :

Currently, Dial backup and Traffic redirect check the ADSL Line status. So user can't enable these two feature at the same time.

Appendix 3 IPsec FQDN support



If Prestige A wants to build a VPN tunnel with Prestige B by passing through Router C with NAT, A can not see B. It has to secure gateway as C. However, Prestige B will send it packet with its own IP and its ID to Prestige A. The IP will be NATed by Router C, but the ID will remain as Prestige B sent.

In FQDN design, all three types, IP, DNS, E-Mail, can set ID content. For ID type is DNS or E-mail, the behavior is simple. Prestige A and Prestige B only checks the ID contents are consistent and they can connect.

Basically the story is the same when ID type is IP. If user configures ID content, then Prestige will use it as a check. So the ID content also has to match each other. For example, ID type and ID content of incoming packets must match “Peer ID Type” and “Peer ID content”. Or Prestige will reject the connection.

However, user can leave “ID content” blank if the ID type is IP. Prestige will put proper value in it during IKE negotiation. This appendix describes all combinations and behaviors of Prestige.

We can put all combinations in to these two tables:

(Local ID Type is IP):

| Configuration | | **Run-time status | |
|-----------------------|-----------------------|-------------------|------------------|
| My IP Addr | Local ID Content | My IP Addr | Local ID Content |
| 0.0.0.0 | *blank or 0.0.0.0 | My WAN IP | My WAN IP |
| 0.0.0.0 | a.b.c.d (NOT 0.0.0.0) | My WAN IP | a.b.c.d |
| a.b.c.d (not 0.0.0.0) | *blank or 0.0.0.0 | a.b.c.d | a.b.c.d |
| a.b.c.d (not 0.0.0.0) | e.f.g.h (NOT 0.0.0.0) | a.b.c.d | e.f.g.h |

*Blank: User can leave this field as empty, doesn't put anything here.

**Runtime status: During IKE negotiation, Prestige will use “My IP Addr” field as source IP of IKE packets, and put “Local ID Content” in the ID payload.

(Peer ID Type is IP):

| Configuration | *Run-time check |
|---------------|-----------------|
| | |

| Secure Gateway Addr | Peer ID Content | |
|---------------------|-----------------------|---|
| 0.0.0.0 | Blank or 0.0.0.0 | Just check ID types of incoming packet and machine's peer ID type. If the peer's ID is IP, then we accept it. |
| 0.0.0.0 | a.b.c.d (NOT 0.0.0.0) | System checks both type and content |
| a.b.c.d | Blank | 1. System will check the ID type and the content. 2. The contents will match only if the ID content of coming packet is a.b.c.d because system will put Secure Gateway Address as Peer ID content. |
| a.b.c.d | e.f.g.h | 1. System will check the ID type and the content. 2. The contents will match only if the ID content of coming packet is e.f.g.h. |

*Runtime Check: During IKE negotiation, we will check ID of incoming packet and see if it matches our setting of "Peer ID Type" and "Peer ID Content".

Summary:

1. When Local ID Content is blank or 0.0.0.0, during IKE negotiation, my ID content will be "My IP Addr" (if it's not 0.0.0.0) or local's WAN IP.
2. When "Peer ID Content" is not blank or 0.0.0.0, ID of incoming packet has to match our setting. Or the connection request will be rejected.
3. When "Secure Gateway IP Addr" is 0.0.0.0 and "Peer ID Content" is blank or 0.0.0.0, system can only check ID type. This is a kind of "dynamic rule" which means it accepts incoming request from any IP, and these requests' ID type is IP. So if user put such a kind of rule in top of rule list, it may be matched first. To avoid this problem, we will enhance it in the future.

CI Command List

| Command Class List Table | | |
|--|--|--|
| System Related Command | Exit Command | Ethernet Related Command |
| AUX Related Command | IP Related Command | IPSec Related Command |
| Bridge Related Command | Firewall Related Command | CNM Related Command |

System Related Command

[home](#)

| Command | | | | Description |
|---------|-------------|----------|---|--|
| sys | | | | |
| | adjtime | | | retrive date and time from Internet |
| | atsh | | | display MRD field |
| | callhist | | | |
| | | display | | display call history |
| | | remove | <index> | remove entry from call history |
| | countrycode | | [countrycode] | set country code |
| | date | | [year month date] | set/display date |
| | domainname | | | display domain name |
| | edit | | <filename> | edit a text file |
| | extraphnum | | | maintain extra phone numbers for outcalls |
| | | add | <set 1-3> <1st phone num> [2nd phone num] | add extra phone numbers |
| | | display | | display extra phone numbers |
| | | node | <num> | set all extend phone number to remote node <num> |
| | | remove | <set 1-3> | remove extra phone numbers |
| | | reset | | reset flag and mask |
| | feature | | | display feature bit |
| | hostname | | [hostname] | display system hostname |
| | logs | | | |
| | | category | | |
| | | | access [0:none/1:log] | record the access control logs |
| | | | attack [0:none/1:log/2:alert/3:both] | record and alert the firewall attack logs |
| | | | display | display the category setting |
| | | | error [0:none/1:log/2:alert/3:both] | record and alert the system error logs |
| | | | ipsec [0:none/1:log] | record the access control logs |
| | | | mten [0:none/1:log] | record the system maintenance logs |

| | | | | |
|--|---------|-----------------------|--|---------------------------------------|
| | | | upnp [0:none/1:log] | record upnp logs |
| | | | urlblocked [0:none/1:log/2:alert/3:both] | record and alert the web blocked logs |
| | | | urlforward [0:none/1:log] | record web forward logs |
| | | clear | | clear log |
| | | display | | display all logs |
| | | errlog | | |
| | | | clear | display log error |
| | | | disp | clear log error |
| | | | online | turn on/off error log online display |
| | | load | | load the log setting buffer |
| | | mail | | |
| | | | alertAddr [mail address] | send alerts to this mail address |
| | | | display | display mail setting |
| | | | logAddr [mail address] | send logs to this mail address |
| | | | schedule display | display mail schedule |
| | | | schedule hour [0-23] | hour time to send the logs |
| | | | schedule minute [0-59] | minute time to send the logs |
| | | | schedule policy [0:full/1:hourly/2:daily/3:weekly/4:none] | mail schedule policy |
| | | | schedule week [0:sun/1:mon/2:tue/3:wed/4:thu/5:fri/6:sat] | weekly time to send the logs |
| | | | server [domainName/IP] | mail server to send the logs |
| | | | subject [mail subject] | mail subject |
| | | save | | save the log setting buffer |
| | | syslog | | |
| | | | active [0:no/1:yes] | active to enable unix syslog |
| | | | display | display syslog setting |
| | | | facility [Local ID(1-7)] | log the messages to different files |
| | | | server [domainName/IP] | syslog server to send the logs |
| | stdio | | [second] | change terminal timeout value |
| | time | | [hour [min [sec]]] | display/set system time |
| | trcdisp | parse, brief, disp | | monitor packets |
| | syslog | | | |
| | | server | [destIP] | set syslog server IP address |
| | | facility | <FacilityNo> | set syslog facility |

| | | | | |
|--|------------|----------------|--------------|--|
| | | type | [type] | set/display syslog type flag |
| | | mode | [on off] | set syslog mode |
| | version | | | display RAS code and driver version |
| | view | | <filename> | view a text file |
| | wdog | | | |
| | | switch | [on off] | set on/off wdog |
| | | cnt | [value] | display watchdog counts value: 0-34463 |
| | romreset | | | restore default romfile |
| | socket | | | display system socket information |
| | ddns | | | |
| | | debug | <level> | enable/disable ddns service |
| | | display | <iface name> | display ddns information |
| | | restart | <iface name> | restart ddns |
| | | logout | <iface name> | logout ddns |
| | cpu | | | |
| | | display | | display CPU utilization |
| | xmodemmode | [crc checksum] | | select xmodem mode |

Exit Command

[home](#)

| Command | | | | Description |
|---------|--|--|--|---------------|
| exit | | | | exit smt menu |

Ethernet Related Command

[home](#)

| Command | | | | Description |
|---------|---------|--------|-------------|---------------------------------------|
| ether | | | | |
| | config | | | display LAN configuration information |
| | driver | | | |
| | | cnt | | |
| | | | disp <name> | display ether driver counters |
| | | status | <ch_name> | see LAN status |
| | version | | | see ethernet device type |

AUX Related Command

[home](#)

| Command | | | | Description |
|---------|--|--|--|-------------|
|---------|--|--|--|-------------|

| | | | | |
|-----|----------|-------|------------------------------------|---------------------------------------|
| aux | | | | |
| | atring | | <device name> (device name = aux0) | Command the AT command to the device. |
| | cnt | | | |
| | | disp | <device name> | display aux counter information |
| | | clear | <device name> | clear aux counter information |
| | drop | | <device name> | disconnect |
| | init | | <device name> | initialize aux channel |
| | mstatus | | <device name> | display modem last call status |
| | mtype | | <device name> | display modem type |
| | netstat | | <device name> | prints upper layer packet information |
| | rate | | <device name> | show tx rx rate |
| | redirect | | <device name> | invalid |
| | signal | | <device name> | show aux signal |

IP Related Command

[home](#)

| Command | | | | Description |
|---------|----------|-----------|------------------------------------|--------------------------------|
| ip | | | | |
| | address | | [addr] | display host ip address |
| | alias | | <iface> | alias iface |
| | aliasdis | | <0 1> | disable alias |
| | arp | | | |
| | | status | <iface> | display ip arp status |
| | dhcp | | <iface> | |
| | | client | | |
| | | | release | release DHCP client IP |
| | | | renew | renew DHCP client IP |
| | | status | [option] | show dhcp status |
| | dns | | | |
| | | query | | |
| | | stats | | |
| | | | clear | clear dns statistics |
| | | | disp | display dns statistics |
| | icmp | | | |
| | | status | | display icmp statistic counter |
| | | discovery | <iface> [on off] | set icmp router discovery flag |
| | ifconfig | | [iface] [ipaddr] [broadcast <addr> | configure network interface |

| | | | | |
|--|------------|------------|--|---|
| | | | mtu <value> dynamic] | |
| | ping | | <hostid> | ping remote host |
| | route | | | |
| | | status | [if] | display routing table |
| | | add | <dest_addr default>[/<bits>] <gateway> [<metric>] | add route |
| | | addiface | <dest_addr default>[/<bits>] <gateway> [<metric>] | add an entry to the routing table to iface |
| | | addprivate | <dest_addr default>[/<bits>] <gateway> [<metric>] | add private route |
| | | drop | <host addr> [/<bits>] | drop a route |
| | status | | | display ip statistic counters |
| | udp | | | |
| | | status | | display udp status |
| | tcp | | | |
| | | status | [tcb] [<interval>] | display TCP statistic counters |
| | traceroute | | <host> [ttl] [wait] [queries] | send probes to trace route of a remote host |
| | xparent | | | |
| | | join | <iface1> [<iface2>] | join iface2 to iface1 group |
| | | break | <iface> | break iface to leave ipxparent group |
| | urlfilter | | | |
| | | exemptZone | | |
| | | | display | display exemptzone information |
| | | | actionFlags [type(1-3)][enable/disable] | set action flags |
| | | | add [ip1] [ip2] | add exempt range |
| | | | delete [ip1] [ip2] | delete exempt range |
| | | | clearAll | clear exemptzone information |
| | | customize | | |
| | | | display | display customize action flags |
| | | | actionFlags [act(1-6)][enable/disable] | set action flags |
| | | | logFlags [type(1-3)][enable/disable] | set log flags |
| | | | add [string] [trust/untrust/keyword] | add url string |
| | | | delete [string] [trust/untrust/keyword] | delete url string |
| | | | clearAll | clear all information |
| | igmp | | | |
| | | debug | [level] | set igmp debug level |
| | | forwardall | [on off] | turn on/off igmp forward to all interfaces flag |

| | | | | |
|--|--|------------|-----------------------------|----------------------------------|
| | | querier | [on off] | turn on/off igmp stop query flag |
| | | iface | | |
| | | | <iface> grouptm <timeout> | set igmp group timeout |
| | | | <iface> interval <interval> | set igmp query interval |
| | | | <iface> join <group> | join a group on iface |
| | | | <iface> leave <group> | leave a group on iface |
| | | | <iface> query | send query on iface |
| | | | <iface> rsptime [time] | set igmp response time |
| | | | <iface> start | turn on of igmp on iface |
| | | | <iface> stop | turn off of igmp on iface |
| | | | <iface> ttl <threshold> | set ttl threshold |
| | | | <iface> v1 compat [on off] | turn on/off v1 compat on iface |
| | | robustness | <num> | set igmp robustness variable |
| | | status | | dump igmp status |

IPSec Related Command

[home](#)

| Command | | | | Description |
|---------|--------------------|----------|----------|--|
| ipsec | | | | |
| | debug | <1 0> | | turn on/off trace for IPsec debug information |
| | ipsec_log_di sp | | | show IPSec log, same as menu 27.3 |
| | route | lan | <on off> | After a packet is IPSec processed and will be sent to LAN side, this switch is to control if this packet can be applied IPSec again. |
| | | wan | <on off> | After a packet is IPSec processed and will be sent to WAN side, this switch is to control if this packet can be applied IPSec again. |
| | show_runti me | sa | | display runtime phase 1 and phase 2 SA information |
| | | spd | | When a dynamic rule accepts a request and a tunnel is established, a runtime SPD is created according to peer local IP address. This command is to show these runtime SPD. |
| | switch | <on off> | | As long as there exists one active IPSec rule, all packets will run into IPSec process to check SPD. This switch is to control if a packet should do |

| | | | | |
|--|------------------|-------------|--|---|
| | | | | this. If it is turned on, even there exists active IPsec rules, packets will not run IPsec process. |
| | timer | chk_my_ip | <1~3600> | - Adjust timer to check if WAN IP in menu is changed |
| | | | | - Interval is in seconds |
| | | | | - Default is 10 seconds |
| | | | | - 0 is not a valid value |
| | | chk_conn. | <0~255> | - Adjust auto-timer to check if any IPsec connection has no traffic for certain period. If yes, system will disconnect it. |
| | | | | - Interval is in minutes |
| | | | | - Default is 2 minutes |
| | | | | - 0 means never timeout |
| | | update_peer | <0~255> | - Adjust auto-timer to update IPsec rules which use domain name as the secure gateway IP. |
| | | | | - Interval is in minutes |
| | | | | - Default is 15 minutes |
| | | | | - 0 means never update |
| | | chk_input | <0~255> | - Adjust input timer to check if any IPsec connection has no inbound traffic for a certain period. If yes, system will disconnect it. |
| | | | | - Interval is in minutes |
| | | | | - default value is "disabled" |
| | | | | - 0 means means disable this timer |
| | updatePeerI p | | | Force system to update IPsec rules which use domain name as the secure gateway IP right away. |
| | dial | <rule #> | | Initiate IPsec rule <#> |
| | display | <rule #> | | Display IPsec rule # |
| | keep_alive | <rule #> | <on off> | Set ipsec keep_alive flag |
| | load | <rule #> | | Load ipsec rule |
| | save | | | Save ipsec rules |
| | config | netbios | active <on off> | Set netbios active flag |
| | | | group <group index1, group index2...> | Set netbios group |
| | | name | <string> | Set rule name |
| | | active | <Yes No> | Set active or not |

| | | | | |
|--|--|----------------------|--|---|
| | | keyAlive | <Yes No> | Set keep alive or not |
| | | lcIdType | <0:IP 1:DNS 2:Email> | Set local ID type |
| | | lcIdContent | <string> | Set local ID content |
| | | myIpAddr | <IP address> | Set my IP address |
| | | peerIdType | <0:IP 1:DNS 2:Email> | Set peer ID type |
| | | peerIdContent | <string> | Set peer ID content |
| | | secureGatewayAddress | <IP address Domain name> | Set secure gateway address or domain name |
| | | protocol | <1:ICMP 6:TCP 17:UDP> | Set protocol |
| | | lcAddrType | <0:single 1:range 2:subnet> | Set local address type |
| | | lcAddrStart | <IP> | Set local start address |
| | | lcAddrEndMask | <IP> | Set local end address or mask |
| | | lcPortStart | <port> | Set local start port |
| | | lcPortEnd | <port> | Set local end port |
| | | rmAddrType | <0:single 1:range 2:subnet> | Set remote address type |
| | | rmAddrStart | <IP> | Set remote start address |
| | | rmAddrEndMask | <IP> | Set remote end address or mask |
| | | rmPortStart | <port> | Set remote start port |
| | | rmPortEnd | <port> | Set remote end port |
| | | antiReplay | <Yes No> | Set antireplay or not |
| | | keyManage | <0:IKE 1:Manual> | Set key manage |
| | | ike | negotiationMode <0:Main 1:Aggressive> | Set negotiation mode in phase 1 in IKE |
| | | | authMethod <0:PreSharedKey 1:RSASignature> | Set authentication method in phase 1 in IKE |
| | | | preShareKey <string> | Set pre shared key in phase 1 in IKE |
| | | | certFile <FILE> | Set certificate file if using RSA signature as authentication method. |
| | | | p1EncryAlgo <0:DES 1:3DES> | Set encryption algorithm in phase 1 in IKE |
| | | | p1AuthAlgo <0:MD5 1:SHA1> | Set authentication algorithm in phase 1 in IKE |
| | | | p1SaLifeTime <seconds> | Set sa life time in phase 1 in IKE |
| | | | p1KeyGroup <0:DH1 1:DH2> | Set key group in phase 1 in IKE |
| | | | activeProtocol <0:AH 1:ESP> | Set active protocol in phase 2 in IKE |
| | | | p2EncryAlgo <0:Null 1:DES | Set encryption algorithm in phase 2 in IKE |

| | | | | |
|--|---------------------|------------|-------------------------------------|---|
| | | | 2:3DES> | |
| | | | p2AuthAlgo <0:MD5 1:SHA1> | Set authentication algorithm in phase 2 in IKE |
| | | | p2SaLifeTime <seconds> | Set sa life time in phase 2 in IKE |
| | | | encap <0:Tunnel 1:Transport> | set encapsulation in phase 2 in IKE |
| | | | pfs <0:None 1:DH1 2:DH2> | set pfs in phase 2 in IKE |
| | | manual | activeProtocol <0:AH 1:ESP> | Set active protocol in manual |
| | | manual ah | encap <0:Tunnel 1:Transport> | Set encapsulation in ah in manual |
| | | | spi <decimal> | Set spi in ah in manual |
| | | | authAlgo <0:MD5 1:SHA1> | Set authentication algorithm in ah in manual |
| | | | authKey <string> | Set authentication key in ah in manual |
| | | manual esp | encap <0:Tunnel 1:Transport> | Set encapsulation in esp in manual |
| | | | spi <decimal> | Set spi in esp in manual |
| | | | encryAlgo <0:Null 1:DES 2:3DES> | Set encryption algorithm in esp in manual |
| | | | encryKey <string> | Set encryption key in esp in manual |
| | | | authAlgo <0:MD5 1:SHA1> | Set authentication algorithm in esp in manual |
| | | | authKey < string> | Set authentication key in esp in manual |
| | swSkipOver lapIp | | <on off> | <ul style="list-style-type: none"> - When a VPN rule with remote range overlaps with local range, the switch decides if a local to local packet should apply this rule. - Default value is “off” which means “no skip”. |
| | adjTcpMss | | <off auto user defined value> | <ul style="list-style-type: none"> - After a tunnel is established, system will automatically adjust TCP MSS. - After all tunnels are drops, the MSS will adjust to the original value. - The default value is auto. |

Bridge Related Command

[home](#)

| Command | | | Description |
|---------|------|-------|---|
| bridge | | | |
| | cnt | | related to bridge routing statistic table |
| | | disp | display bridge route counter |
| | | clear | clear bridge route counter |
| | stat | | related to bridge packet statistic table |

| | | | | |
|--|--|-------|--|-------------------------------------|
| | | disp | | display bridge route packet counter |
| | | clear | | clear bridge route packet counter |

Firewall Related Command

[home](#)

| Command | | | | Description |
|---------|----------|---------|----------|---|
| sys | Firewall | | | |
| | | acl | | |
| | | | disp | Display specific ACL set # rule #, or all ACLs. |
| | | active | <yes no> | Active firewall or deactivate firewall |
| | | clear | | Clear firewall log |
| | | cnt | | |
| | | | disp | Display firewall log type and count. |
| | | | clear | Clear firewall log count. |
| | | disp | | Display firewall log |
| | | online | | Set firewall log online. |
| | | pktdump | | Dump the 64 bytes of dropped packet by firewall |
| | | update | | Update firewall |
| | | tcprst | | |
| | | | rst | Set TCP reset sending on/off. |
| | | | rst113 | Set TCP reset sending for port 113 on/off. |
| | | | display | Display TCP reset sending setting. |
| | | dos | | |
| | | | smtp | Set SMTP DoS defender on/off |
| | | | display | Display SMTP DoS defender setting. |
| | | | ignore | Set if firewall ignore DoS in lan/wan/dmz/wlan |
| | | ignore | | |
| | | | dos | Set if firewall ignore DoS in lan/wan/dmz/wlan |
| | | | triangle | Set if firewall ignore triangle route in lan/wan/dmz/wlan |

CNM Related Command

[Home](#)

| Command | | | | Description |
|---------|--------|--|------------------------|---|
| cnm | | | | |
| | active | | [1/0] (enable/disable) | display/set CNM features enable/disable |

| | | | | |
|--|-----------|--|------------------------|---|
| | sgid | | | display an identifier(sgid) to associate device and security policies residing in ZyCNM |
| | managerIp | | [ZyCNM server IP] | set/display ZyCNM server IP |
| | debug | | [1/0] (enable/disable) | display/set CNM features enable/disable debug mode |
| | reset | | | disconnect and re-register to ZyCNM server |
| | simulate | | <1/0> (enable/disable) | set simulating devices features enable/disable |
| | encrykey | | [ZyCNM Encryption Key] | Set/display ZyCNM encryption key |
| | encrymode | | <0 1 2>(none des 3des) | Set/display ZyCNM encryption mode |