



**Firmware Release Note**

**ZyWALL USG 2000**

**Release 2.20(AQW.1)**

Date: May 6, 2010

Author: Peter Wang

Project Leader: Peter Wang

## **ZyXEL ZyWALL USG 2000**

### **Release 2.20(AQW.1)**

#### ***Release Note***

---

**Date:** May 6, 2010

#### **Supported Platforms:**

---

ZyXEL ZyWALL USG 2000

#### **Versions:**

---

ZLD Version: V2.20(AQW.1) | 2010-05-06 11:37:21

BootModule Version: V1.21 | 2009-11-18 08:49:30

#### **Files lists contains in the Release ZIP file**

---

**File name: 220AQW1C0.bin**

Purpose: This binary firmware image file is for normal system update.

Note: The firmware update may take five or more minutes depending on the scale of device configuration. The more complex configuration will take more update time. Do not turn off or reset the ZyWALL while the firmware update is in progress. The firmware might get damaged, if device loss power or you reset the device during the firmware upload. You might need to refer to Appendix 3 of this document to recover the firmware.

**File name: 220AQW1C0.conf**

Purpose: This ASCII file contains default system configuration commands.

**File name: 220AQW1C0.db**

Purpose: This binary file contains default system signatures.

Note: The file is only needed when doing system recovery from damage.

**File name: 220AQW1C0.doc**

Purpose: This release file.

**File name: 220AQW1C0.ri**

Purpose: This binary firmware recovery image file is for emergent system firmware damage recovery only.

Note: The ZyWALL firmware could be damaged, for example by the power going off or pressing Reset button during a firmware update.

**File name: 220AQW1C0-enterprise.mib, 220AQW1C0-private.mib**

Purpose: The Enterprise and Private MIBs are to collect information about CPU and memory usage and VPN total throughput. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

**File name: firmware.xml**

Purpose: This file is needed by ZyXEL Centralized Network Management (CNM) 3.0 or after.

## Read Me First

---

1. The system default configuration is summarized as below:
  - The default device administration username is “admin”, password is “1234”.
  - The default LAN interface is ge1, which locates on the most left side of the front panel. The default LAN subnet is 192.168.1.0/24.
  - By default, WWW/SSH/SNMP service can only be accessed from LAN subnet.
  - The default WAN interface is ge2, and the secondary WAN interface is ge3. These two interfaces will automatically get IP address using DHCP by default.
  - The default DMZ interface is ge4, ge5 and ge6. These three DMZ interfaces by default are assigned to static IP 192.168.2.0/24, 192.168.3.0/24 and 192.168.4.0/24, respectively.
2. It is recommended that user backup the “startup-config.conf” file first before upgrading firmware. The backup configuration file can be used if user wants to downgrade to an older firmware version.
3. If it is difficult to configure via GUI (popup java script error, etc). It is recommended to logout the configuration window and clear browser cache first, then try to login and configure again.
4. To reset device to system default, user can press RESET button for 5 seconds and the device will reset itself to system default configuration then reboot automatically.
  - Note 1: After resetting, the original configuration will be removed. It is recommended to backup the configuration before performing this operation.
  - Note 2: After resetting, if user has subscribed to security licenses, user needs to connect to internet with myZyXEL.com and refresh license information.

5. If there is problem to reboot successfully after firmware upgrade, please refer to Appendix 3: Firmware Recovery.
6. Since BWM has been activated in system default since 2.20(AQW.0)b3, please remember to turn off BWM before you do the performance testing

## Known Issues:

---

### SSL VPN:

1. [SPR: 091022383] Since F/W version 2.11  
[Symptom] SSLVPN cannot work anymore if below case is true
  - 1) Configure one SSLVPN policy and activate the Network Extension
  - 2) Add network A into Network List
  - 3) User login SSLVPN from network A
  - 4) The SSLVPN cannot be established and cannot work anymore

[Workaround] Reboot DUT and remove network A from Network List
2. [SPR: 091021328] Since F/W version 2.20b1  
[Symptom] SecuExtender agent cannot be launched in Windows Vista and Windows 7 If the “Computer Management/Services and Applications/Services/ZyWALL SecuExtender Helper” is disabled on user’s computer before user tries to login SSLVPN.  
[Workaround] Enable ZyWALL SecuExtender Helper first before you try to login SSLVPN
3. [SPR: 090901070] Since F/W version 2.20b1  
[Symptom] Microsoft RDP Client Control may not work after user installs MS KB958469/958470/958471/956744. Using SSL VPN RDP function, after user install Remote Desktop Client Control (msrdp.cab), some PC may occur Javascript error.  
This problem cause by **MS KB958469/958470/958471/956744**. When user never uses RDP ActiveX control, and user install KB958469/958470/958471/956744, Windows will block the msrdp.cab installer.

## KB offer matrix based on the RDC version and platforms

RDC versions (in-band and Microsoft-supported out-of-band releases)

	RDC 5.0	RDC 5.1	RDC 5.2	RDC 6.0	RDC 6.1
Windows Vista RTM	x	x	x	KB956744*	x
Windows Vista SP1 and Windows Vista SP2	x	x	x	x	KB956744*
Windows XP SP2	x	KB958470*	KB958469	KB956744*	KB956744*
Windows XP SP3	x	x	KB958469	x	KB956744*
Windows Server 2003 SP2	x	x	KB958469*	KB956744*	x
Windows 2000 SP4	KB958471*	KB958470*	KB958470	x	x

**Note** In this table, x = not applicable.

**Note** In this table, almost all users are represented by the scenarios in the table that contain asterisks (\*).

### [Workaround]

To solve this problem, user can reinstall the KB958469/958470/958471/956744 after user failed to install msrdp.ocx. Go to Windows Update Site, the KB958469/958470/958471/956744 will reappear on the web site. To install the RDP function could be used.

More information can see Microsoft Support Site:

<http://support.microsoft.com/kb/958469>

<http://support.microsoft.com/kb/958470>

<http://support.microsoft.com/kb/958471>

<http://support.microsoft.com/kb/956744>

#### 4. [SPR: 100427864] Since F/W version 2.11

[Symptom] ActiveX cannot be installed successfully when using SSLVPN RDP function

[Condition]

- 1) PC environment: Windows XP with SP3, using IE7 as browser.
- 2) Edit Object>SSL Application , add rules  
- Type=Web Application , Server Type=RDP , Name=RDP\_Windows
- 3) Create one SSLVPN policy which selects the SSL Application we created
- 4) Login SSL VPN but can not open RDP\_Windows portal by Full Screen and 32-bit color.
- 5) GUI will ask user to install terminal services ActiveX Client continuously

[Workaround]

This is because IE7 doesn't allow previously unused ActiveX controls running by default. We need to change the default behavior to allow ActiveX controls in IE7. See below procedures

- 1) Click Tools > Internet Options
- 2) Select Security tab
- 3) Select Internet Zone and click "Custom level"
- 4) Enable the ActiveX option "Allow previously unused ActiveX controls to run without prompt"

#### 5. [SPR: 080430468] Since F/W version 2.11

[Symptom] Cannot install SSL VPN RDP web component in Vista and WIN 2000

[Workaround] Windows XP SP3/RDP 6.1 breaks RDP connection through Internet Explorer.

Following is the SSL VPN RDP limitation table.

Application Operation System	Reverse Proxy Mode	RDP / VNC	Full Tunnel Mode
	Web-based Application		
Windows XP SP3 JRE 1.6_18	Internet Explorer 7.0, 8.0+ (Passed) Firefox 3.5	Internet Explorer 7.0, 8.0+ (Passed) Firefox 3.5(RDP: not support; VNC: Passed)	Internet Explorer 7.0, 8.0+ (Passed) Firefox 3.5 (Passed)
Windows Vista SP1 JRE 1.6_18	Internet Explorer 7.0, 8.0+ (Passed) Firefox 3.5	Internet Explorer 7.0, 8.0+ (Passed) Firefox 3.5(RDP: not support; VNC: Passed)	Internet Explorer 7.0, 8.0+ (Passed) Firefox 3.5 (Passed)
Windows 7 JRE 1.6_18	Internet Explorer 8.0+ (Passed) Firefox 3.5	Internet Explorer 8.0+ (Passed) Firefox 3.5(RDP: not support; VNC: Passed)	Internet Explorer 8.0+ (Passed) Firefox 3.5 (Passed)
Linux OS	Firefox 3.5	RDP : not support , VNC:Passed	No Support
Apple MAC OS 10.4 JRE 11.9	Safari 4 + (Passed)	No Support	No Support
Apple MAC OS 10.5 JRE 12.5	Safari 4 + (Passed)	No Support	No Support

6. [SPR: 100210906] Since F/W version 2.20

[Symptom] Web Server cannot work with SSLVPN if disable Web Page Encryption in Web Application

[Condition]

- 6) Create an SSL Application which is Web Application Type
- 7) Disable Web Page Encryption in this SSL Application object
- 8) Create one SSLVPN policy with this SSL Application object
- 9) Login SSLVPN
- 10) The link on the SSLVPN portal cannot work

[Workaround]

Do not disable Web Page Encryption in the SSL Application object when using Web Application

7. [SPR: 100212995] Since F/W version 2.20

[Symptom] FireFox will have no response in a specific case

[Condition]

- 1) OSX 10.4 + Firefox 3.5.7 + J2SE 5.0
- 2) Login SSLVPN with EPS checking
- 3) One error message “Unsupported OS” will pop up and cannot finish EPS checking

8. [SPR: 100421301] Since F/W version 2.11

[Symptom] Web content cannot be displayed correctly via Reverse Proxy after login SSLVPN

again

[Condition]

- 1) Create one SSL application with OWA type
- 2) Create one SSLVPN policy with the SSL Application we just created
- 3) Login SSLVPN via FireFox
- 4) Access the OWA server via SSLVPN portal
- 5) Select one mail and display its content
- 6) Logout SSLVPN
- 7) Repeat step 3) ~ 5) and the mail content might not be displayed correctly sometimes

[Workaround]

Clear browser cache/cookie first before login SSLVPN again

### Anti-Virus:

1. [SPR: 070813118] Since F/W version 2.00

[Symptom] ZyWALL has the limitation on concurrent sessions for ZIP and RAR decompression. If the limitation has been reached (typically in HTTP traffic), the event would be logged and the action depends on the checkbox (Destroy compressed files that could not be decompressed) is checked or not. If checked, compressed files would be destroyed, otherwise, bypassed.

[Workaround] Unchecked the option of “Destroy compressed files that could not be decompressed” in the AV settings.

### Device HA:

1. [SPR: 071127734] Since F/W version 2.10

[Symptom] PC client may temporarily unable to connect to Device-HA backup device after backup taking over for master.

[Workaround] The virtual MAC address will be switch to backup device, and some PC clients does not accept GARP notification, so PC client may needs to wait its ARP entry timeout or refresh it manually.

2. [SPR: 100119576] Since F/W version 2.12

[Symptom] Preemption in device-ha AP mode cannot work when authentication is MD5

[Condition]

- 1) DUT1 enable device-ha, device role = backup, priority = 5, enable preemption, cluster id = 1, authentication = md5, password = 11111111, active interface = ge1, ge3
- 2) DUT2 enable device-ha, device role = backup, priority = 1, enable preemption, cluster id = 1, authentication = md5, password = 11111111, active interface = ge1, ge3
- 3) When DUT1 status is active, DUT2 is standby, disconnect the cable on DUT1's ge3.
- 4) The HA status will become DUT1: Fault, DUT2: Active

- 5) Connect the cable on DUT1's ge3, the HA status of DUT1: standby. DUT2: active, DUT1 should take the active back

[Workaround]

Do not use authentication for Device HA

## User Aware:

1. [SPR: 070202237] Since F/W version 2.00  
[Symptom] An access user could gain access right after signing in ZyWALL (if properly configured) and log out when he don't need to access the network resources anymore. But sometimes user stays in signing in state after he closes the access window directly and the resources could still be accessible.  
[Workaround] For access users, user logout button to logout instead of closing window directly. For administrations, enable user lease/idle detection for access users.
2. [SPR: 070813119] Since F/W version 2.00  
[Symptom] Device supports authenticating user remotely by creating AAA method which includes AAA servers (LDAP/AD/Radius). If a user uses an account which exists in 2 AAA server and supplies correct password for the latter AAA server in AAA method, the authentication result depends on what the former AAA server is. If the former server is Radius, the authentication would be granted, otherwise, it would be rejected.  
[Workaround] Avoid having the same account in AAA servers within a method.
3. [SPR: 100106335] Since F/W version 2.20  
[Symptom] EPS checking will be failed for Windows Server 2008R2  
[Condition]
  - 1) Add an Auth. Policy rule with EPS checking for Windows Auto Update on Windows Server 2008R2
  - 2) Login DUT via GUI from Windows Server 2008 R2 64-bit which Windows Auto Update is enabled
  - 3) The EPS checking will fail

## Interface

1. [SPR: 090918600] Since F/W version 2.12  
[Symptom] Cellular interface cannot connected if the authentication password is empty
2. [SPR: 100105242, 100105292] Since F/W version 2.12  
[Symptom] PPTP might not be able to connect successfully if it is configured via Installation Wizard/Quick Setup. This is because 1) Installation Wizard/Quick Setup only allows PPTP based interface to be configured with Static IP. 2) Installation Wizard/Quick Setup doesn't allow user to configure PPTP based interface's Gateway IP Address. This may caused PPTP cannot connect successfully if the PPTP Server IP is not at the same subnet with PPTP's based



interface

[Workaround]

Before dial PPTP connection, configure the Gateway IP of PPTP interface 's based interface

### Build in Service:

1. [SPR: 061208575] Since F/W version 2.00

[Symptom] If users change port for built-in services (FTP/HTTP/SSH/TELNET) and the port conflicts with other service or internal service, the service might not be brought up successfully. The internal service ports include 10443/1723/1701/2601-2604. Users should avoid using these internal ports for built-in services.

[Workaround] Users should avoid using these internal ports for built-in services.

### IPSec VPN:

1. [SPR: 070814168] Since F/W version 2.00

[Symptom] VPN tunnel could not be established when 1) a non ZyWALL peer gateway reboot and 2) ZyWALL has a previous established Phase 1 with peer gateway, and the Phase 1 is not yet expired. Under those conditions, ZyWALL will continue to use the previous phase 1 SA to negotiate the Phase 2 SA. It would result in phase 2 negotiation to fail.

[Workaround] User could disable and re-enable phase 1 rule in ZyWALL or turn on DPD function to resolve problem.

2. [SPR: 070814169] Since F/W version 2.00

[Symptom] PKI does not interoperate with Windows CA server, when using SCEP.

3. [SPR: 100428888] Since F/W version 2.20

[Symptom] GUI might be hanged under certain condition

[Condition]

- 1) Reset to factory default configuration
  - 2) Configure one VPN Connection properly and build it up
  - 3) Enter GUI page Monitor > VPN Monitor > IPSec
  - 4) Disconnect the VPN tunnel we just established
  - 5) After the VPN tunnel being disconnected successfully, the "Disconnect" icon is still able to be clicked. It should be able to be clicked since there is no VPN tunnel established anymore
  - 6) If we click the "Disconnect" when there is no VPN tunnel established, GUI will hang up
- [Workaround] We may need to login GUI again for following configuration

4. [SPR: 100429119] Since F/W version 2.11

[Symptom] VPN tunnel might be established with incorrect VPN Gateway

[Condition]

- 1) Prepare 2 ZyWALL and reset to factory default configuration on both ZyWALLs

- 2) On ZyWALL-A
    - (1) Create 2 WAN interfaces and configure WAN1 as DHCP Client
    - (2) Create 2 VPN Gateways. The “My Address” is configured as Interface type and select WAN1 and WAN2 respectively
    - (3) Create 2 VPN Connections named VPN-A and VPN-B accordingly which bind on the VPN Gateways we just created
  - 3) On ZyWALL-B
    - (1) Create one WAN interface
    - (2) Create one VPN Gateway. The Primary Peer Gateway Address is configured as WAN1 IP address of ZyWALL-A and the Secondary Peer Gateway Address is configured as WAN2 IP address of ZyWALL-A
  - 4) Connect the VPN tunnel from ZyWALL-B to ZyWALL-A and we can see VPN-A is connected on ZyWALL-A
  - 5) Unplug WAN1 cable on ZyWALL-A
  - 6) After DPD triggered on ZyWALL-B, the VPN Connection will be established again
  - 7) On ZyWALL-A, VPN-A is connected. But actually ZyWALL-B should connect to VPN-B after step 5)
- [Workaround] Change the WAN1 setting of ZyWALL-A to Static IP

## DHCP:

1. [SPR: 070912654] Since F/W version 2.10  
[Symptom] Reserve a IP-MAC of a DHCP client in DHCP table will cause reserved hostname turn to “none”, and after unreserved, this client will disappear from DHCP table.

## Object Reference

For those objects used by its own feature, we don't implement object reference function for it.  
Since F/W version 2.20(AQW.0)b1

For examples

1. Content Filter Profile is used by Content filter only. We don't implement object reference function for it
2. IDP/ADP Profile is used by IDP/ADP only. We don't implement object reference function for it

## Dynamic DNS

1. Peanut Hull DDNS cannot work if the account is not paid. Detail information please visit following link <http://www.oray.cn/News/269.html>

## Traffic Log

1. [SPR: 070912654] Since F/W version 2.20b1

[Symptom] When sending a log mail, three fields are gone. They are "Source Interface", "Destination Interface" and "Protocol"

### **Software Watchdog**

1. [SPR: 090720388] Since F/W version 2.20b1

[Symptom] show software-watchdog-timer log cannot work

### **Throughput**

1. [SPR: 091208524] Since F/W version 2.20b1

[Symptom] UTM has low throughput for UDP small packet

## Features:

---

Modifications in 2.20(AQW.1) - 2010/05/06

Modified for formal release

## Features:

---

Modifications in 2.20(AQW.1)b3 - 2010/05/04

1. [BUG FIX] 100504064

Symptom:

ZyWALL will be crashed while collecting diagnostic info sometimes

Condition:

- 1) Update IDP signature to the latest
- 2) Collect diagnostic info
- 3) Sometimes ZyWALL will be crashed

2. [BUG FIX] 100422392

Symptom:

ZyWALL SecuExtender cannot be terminated automatically by closing the SSLVPN portal window

Condition:

- 1) Login SSLVPN with Full Tunnel mode using Windows 7
- 2) Close the SSLVPN Portal window by clicking "X" on right corner of the window
- 3) The ZyWALL SecuExtender won't be terminated automatically

## Features:

---

Modifications in 2.20(AQW.1)b2 - 2010/04/16

1. [BUG FIX] 100119485

Symptom:

Under certain condition, connectivity check cannot work on cellular interface

Condition:

1. Insert AC880 card, edit the cellular1 interface in Interface> Cellular page, enable Nailed up, filling APN option into CMNET, Dial string option into \*99#, others keep default
2. The 3G can connect correctly
3. Edit cellular1 interface, enable Connectivity check, check method is icmp, check period is 5, check timeout is 2, check fail tolerance is 3, and enable check this address "1.1.1.1", apply
4. Ping check can work, and the 3G interface is inactive
5. Edit the 3G rule second time, Enable Budget Control=enable ; Time Budget=enable ; hours per month=30 ; Reset time and data budget counters=15 ; Actions when over budget/Log=log-alert ; Enable recurring every 1 minutes ; New 3G connection=Disallow ; Current 3G connection=Drop ; Actions when over 10 % of time budget or 10 % of data budget ; Log=log-alert ; Enable recurring every 1 minutes
6. Edit the Cellular1 interface third time, disable Connectivity check, and in Device setting field, select "Device Selection" as "Sierra Wireless AC880", "Band Selection" as "Auto", apply, the rule can be saved without warning
7. But the connectivity check function still works, capture the packets from Cellular1 interface, there are lots of packets about ping 1.1.1.1 request, and the traffic from LAN to Cellular1 cannot walk through

2. [BUG FIX] 100121946

Symptom:

Under bridge mode, traffic cannot pass through the VPN tunnel if Firewall is activated

Condition:

1. Configure ZyWALL with one bridge interface
2. Configure one IPSec tunnel which uses the bridge interface to build the IPSec tunnel
3. Configure one remote VPN gateway which WAN interface is not at the same network with the ZyWALL's WAN interface which is used to build up the IPSec tunnel
4. Enable Firewall on ZyWALL
5. Establish the IPSec tunnel between the ZyWALL and remote VPN gateway
6. The traffic cannot pass through the IPSec tunnel and dropped by Firewall

3. [BUG FIX] 100204388

**Symptom:**

Error message displayed on GUI after enabling Redirect HTTP to HTTPS

**Condition:**

1. Disable “Redirect HTTP to HTTPS”
2. Login ZyWALL GUI via HTTP service
3. Enter WWW page and enable “Redirect HTTP to HTTPS”
4. Click other page and the error message “URL request timeout. (3 minutes limit)” displayed

4. [BUG FIX] 100310758

**Symptom:**

Incorrect CLI commands applied under certain condition

**Condition:**

1. Create one Authentication Policy via GUI. Authentication = required and Force User Authentication is selected
2. Edit the Auth. Policy again and change the Authentication from “required” to “unnecessary”. Do not apply
3. Change the Authentication from “unnecessary” to “required” and apply
4. The “Authentication” field in summary page should be “force” instead of “required”

5. [BUG FIX] 100312072

**Symptom:**

SNMP cannot work through IPSec tunnel

**Condition:**

1. Create one IPSec tunnel between ZyWALLs
2. Enable SNMP service on remote ZyWALL
3. PC under local ZyWALL’s LAN cannot query remote ZyWALL’s LAN IP via SNMP

6. [BUG FIX] 100315140

**Symptom:**

After language changed, Site Map cannot be displayed anymore

**Condition:**

1. Change the language from English to Traditional Chinese
2. Click Site Map but it cannot be displayed

7. [BUG FIX] 100315227

**Symptom:**

The On Top icons cannot work after language changed

**Condition:**

1. Using FireFox 3.5 or 2.6 to login ZyWALL
2. Change the language from English to Traditional Chinese or Simplified Chinese
3. The On Top icons like “Help”, “About”, “Site Map” cannot work anymore

8. [BUG FIX] 100315275

Symptom:

SSL VPN's File Sharing menu bar's "up" button translate to a strange meaning in Traditional Chinese and Simplified\_Chinese

Condition:

1. Login DUT via SSLVPN
2. Change the SSLVPN language from English to Traditional Chinese or Simplified Chinese
3. The translation of menu bar's "up" is "上"
4. It should be translated to more readable wording like "上一層" or "上一頁"

9. [BUG FIX] 100316425

Symptom:

DHCP Service cannot work anymore after frequently modifying the DHCP server configuration

Condition:

1. Reset to default configuration
2. Connect one PC to LAN interface
3. Configure the DHCP lease time on LAN interface
4. Renew IP on the PC and check if the IP can be renewed
5. Repeat step 3~4 several times and the IP of the PC cannot be renewed anymore

10. [BUG FIX] 100317503

Symptom:

Incorrect Default Gateway Address displayed when configuring PPPoE interface's Connectivity Check

Condition:

1. Configure one PPPoE interface and make it connected
2. Edit the PPPoE interface again
3. Enable Connectivity Check and select Check Default Gateway
4. The Gateway IP address displayed is incorrect

11. [BUG FIX] 100317568

Symptom:

Session number cannot be queried via SNMP

Condition:

1. Session number cannot be queried via SNMP
2. Error log "ERROR: #configure terminal show \_zldmib session status, file not found!" found

12. [BUG FIX] 100318634

Symptom:



Extension Slot status for SEM card displayed incorrectly

Condition:

1. Insert SEM card
2. Boot up ZyWALL
3. Login ZyWALL via GUI
4. The Extension Slot status for SEM card in Dashboard is incorrect.

#### 13. [BUG FIX] 100319791

Symptom:

Port Grouping page will disappear after language being changed to Simplified-Chinese.

Condition:

1. Reset DUT to default configure file. Change language from English to Simplified\_Chinese
2. Go to Interface page, click "以太网" tag, the "端口群组" page will disappear. Only click Interface page again, the "端口群组" tag can show

#### 14. [BUG FIX] 100322908

Symptom:

Translation is incorrect about "MAC Address" in interface page

Condition:

1. Change DUT's language to Simplified\_Chinese
2. Go to 接口 > 以太网 page, edit ge1 interface, in "静态 DHCP 表", MAC Address has been translated to "媒体存取控制", it should be "MAC 地址"

#### 15. [BUG FIX] 100323027

Symptom:

The translation about "i" note in certificate adding page is totally wrong

Condition:

1. Change language from English to Simplified\_Chinese, go to Certificate page to add a certificate
2. There's an "i" note about "密钥类型", it's translation is totally wrong

#### 16. [BUG FIX] 100323045

Symptom:

The translation of Mapped Port Start is wrong in VPN connection

Condition:

1. Change language from English to Simplified\_Chinese,
2. in VPN Connection page, add a rule, the Mapped Port Start has been translated to "映射单口开始", it should be "映射端口开始".

#### 17. [BUG FIX] 100323106

Symptom:

In Simplified\_Chinese environment, some translation are still Traditional\_Chinese.

Condition:

1. Change language to Simplified\_Chinese.
2. In 证书 > 可信证书 page, click 导入 button, Import Trusted Certificates window will pop up, the button of "Browser" has been translated into Traditional\_Chinese instead of Simplified\_Chinese
3. The same problem happens in the page of 配置文件, 韧体上传 and Shell 脚本

18. [BUG FIX] 100323139

Symptom:

ZySH daemon will be terminated while issue CLI "no radius-server host "

Condition:

ZySH daemon will be terminated while issue CLI "no radius-server host "

19. [BUG FIX] 100325377

Symptom:

Translation is incorrect about "Host Port" in Packet Capture page

Condition:

Change language to Simplified\_Chinese. Go to Packet Capture page, "Host Port" has been translated to "主机名称", it should be "主机端口"

20. [BUG FIX] 100326493

Symptom:

EPS check will be failed when PC cannot pass the EPS object which is at the first priority

Condition:

1. Create 2 EPS objects they have different passing criteria
2. Create one SSLVPN rule with below EPS configuration
  - 1) Enable EPS check
  - 2) Select the 2 EPS objects we just created
  - 3) Login SSLVPN from a PC that will fail to pass the first EPS object we selected in previous setting but pass the 2<sup>nd</sup> EPS object
3. The EPS check will be failed due to EPS check failed on the first EPS object checking
4. Bug actually it should be successful because the PC will pass the 2<sup>nd</sup> EPS object checking

21. [BUG FIX] 100329625

Symptom:

VPN traffic related logs cannot be displayed on VRPT 3.5 server correctly

Condition:

VPN traffic related logs cannot be displayed on VRPT 3.5 server correctly

22. [BUG FIX] 100331777

Symptom:

ZySH daemon will be crashed when doing Content Filter URL testing

Condition:

1. Enter Anti-X > Content Filter > Filter Profile
2. Create one filter profile and enter <http://~@> in URL to test
3. After trying to test this special URL, ZySH will be crashed

23. [BUG FIX] 100401010

Symptom:

The outgoing interface of reply traffic is not the same as the incoming interface of the originated traffic

Condition:

1. Create multiple WAN interfaces, said WAN1 and WAN2
2. Create one Virtual Server rule and set its incoming interface as WAN1 interface
3. Access the Virtual Server via the WAN1 interface sometimes will be failed because the reply traffic from the Virtual Server will go back via WAN2 interface sometimes

24. [BUG FIX] 100302129

Symptom:

The object reference of the bridge interface will include Device HA even it is not monitored by Device HA

Condition:

1. Create one bridge interface
2. Add this bridge interface to DMZ zone
3. Click the object reference for the bridge interface we just created
4. We will find that Device HA is in the reference list but actually it is not monitored by Device HA

25. [BUG FIX] 100324212

Symptom:

The interface name cannot be displayed completely if the length of the interface name is more than 9 characters

Condition:

1. Rename one of the interfaces to have the length which is more than 9 characters
2. In interface summary table in Dashboard, the related interface name can be only displayed with the first 9 characters

26. [BUG FIX] 100401004

Symptom:

Incorrect login behavior when pressing “Enter” with Username and Password are correctly inputted in SSLVPN login page

Condition:

1. Configure SSLVPN Login Domain Name
2. Enter SSLVPN login page with SSLVPN Login Domain Name

3. Input correct Username and Password and press “Enter” key directly
4. The GUI will enter User Login page instead of SSLVPN login portal
5. The default behavior of pressing “Enter” key in SSLVPN login page should do the SSLVPN login process instead of normal user login

27. [BUG FIX] 100402137

Symptom:

PPTP tunnel cannot be connected successfully

Condition:

1. Connect PPTP tunnel from PC to PPTP server like below topology  
PC ----- (LAN)ZyWALL(WAN) ----- Internet ----- PPTP Server
2. The PPTP tunnel cannot be connected successfully

28. [BUG FIX] 100402124

Symptom:

The ZyWALL generated ICMP Redirect packet will be dropped by Firewall

Condition:

1. Reset to default configuration
2. Configure one Policy Route with Next Hop as Gateway Type and the Gateway address is in the LAN subnet
3. PC in LAN subnet sends ping traffic which will match the Policy Route we just created
4. The ZyWALL should generate one ICMP Redirect packet to tell the PC that there is another Gateway which we configured in Policy Route rule has faster path to reach the destination. But actually not

29. [BUG FIX] 100407319

Symptom:

Change the user type from limited-admin to ext-user or ext-group-user will be fail and popup the Error message

Condition:

1. Create one user with Limited-Admin user type
2. Change the user type of the Limited-Admin user we just created to ext-user or ext-group user
3. GUI will return error message “CLI Number: 0, Error number: -3014, Error Message: Add external type user has failed.”

30. [BUG FIX] 100318683

Symptom:

In CF, add a new profile without enabling anything. The action of category service will all be PASS

Condition:

1. In CF, add a new profile. Name = CF1 without enable anything.(By default, Action of unsafe web pages = Warn, Action of Managed web pages = Block, Action of Unrated web pages = Warn, Action when category server is unavailable = Warn) Then click OK
2. Edit the CF1 profile, the actions of CF category service will all be pass, Action of unsafe web pages = Pass, Action of Managed web pages = Pass, Action of Unrated web pages = Pass, Action when category server is unavailable = Pass

31. [BUG FIX] 100121930

Symptom:

Dashboard display abnormal if using IE browser from "Packet Capture" page to "DASHBOARD" page.

Condition:

1. Use IE browser to login device
2. Go to page MAINTENANCE > Diagnostics > Packet Capture page, then go to "DASHBOARD" page
3. DASHBOARD page display abnormal on "Virtual Device" and "Interface Status Summary" widget

32. [BUG FIX] 100407320

Symptom:

PC with Windows 7 installed can pass EPS check when the OS type is set to Windows 2008 or Windows 2008R2

Condition:

1. Create one EPS object to check the Window OS type as Windows 2008 or Windows 2008 or Windows 2008R2
2. Create one SSLVPN rule with EPS check as previous configured
3. Use a PC with Windows 7 installed to login SSLVPN
4. It should be failed to pass the EPS check due to OS type but passed

33. [BUG FIX] 100322989

Symptom:

Device HA Backup cannot dial up IPSec tunnel successfully after taking over

Condition:

1. Configure Device HA on Master and Backup properly and its monitored interface is an Ethernet interface
2. Configure VPN tunnel with FQDN type as its My Address
3. Configure the Mapped IP of the FQDN of step 2 as one of DUT's ethernet interface's IP address
4. Once Master is down, Backup cannot dial up the VPN tunnel successfully

34. [BUG FIX] 100113950

**Symptom:**

When the Mac Address format is "XX-XX-XX-XX-XX", the MAC clone function doesn't work

**Condition:**

1. Edit one specified interface
2. Click "Show Advanced Settings"
3. In Mac Address Setting section, select "Overwrite Default Mac Address" and configure the Mac Address with the format as "XX-XX-XX-XX-XX-XX"
4. Capture the packets on the specified interface, the Mac address of the specified interface is not changed to "XX-XX-XX-XX-XX-XX"

**35. [BUG FIX] 100407322**

**Symptom:**

If Group Identifier field have space, GUI will pop out a error message "Wrong CLI command device timeout or device logout"

**Condition:**

1. Go to Configuration -> User/Group -> Add an ext-group-user
2. Group Identifier field input DC=xxx,[space]DC=xxx -> press OK
3. GUI will pop out error message "Wrong CLI command device timeout or device logout"

**36. [BUG FIX] 100315249**

**Symptom:**

Test special URL in "Test Web Site Category" causes GUI keeps loading

**Condition:**

1. Create one Content Filter Profile
2. Enter this profile and input "http://" in "URL to test" field, click the "Test against content filter category server"
3. GUI will keep loading

**37. [BUG FIX] 100409424**

**Symptom:**

ZyWALL cannot be logged in

**Condition:**

1. Reset to default configuration
2. Enable SNMP service
3. Do SNMP Bulk request 1.3.6.1.1.890.1.6.22.1.4
4. Running for a while, ZyWALL cannot logged in and error message "Too many open files in system" occurred

**38. [BUG FIX] 100409426**

**Symptom:**

The SSLVPN tunnel will be disconnected unexpectedly

Condition:

1. Create one user and set its lease time to 1 minute
2. Create one SSLVPN rule with Full tunnel mode and allow the user we just created to access the SSLVPN tunnel
3. Enable “Allow renewing lease time automatically” in Configuration > Object > User/Group > Setting page
4. Establish the SSLVPN Full tunnel
5. Keep pingging ZyWALL’s interface from the SSLVPN client
6. The SSLVPN tunnel will be disconnected after one minute

39. [BUG FIX] 100413635

Symptom:

When login SSL VPN and open RDP\_Windows on portal to remote control server, remote server login GUI pops out very slow

Condition:

1. Create one SSL Application with RDP Web Application
2. Create one SSLVPN rule with the SSL Application object
3. Login SSLVPN with Windows 7(32-bit) + IE8
4. Open RDP on the SSLVPN portal and the response is very slow

40. [BUG FIX] 100325342

Symptom:

SecuExtender cannot install by ActiveX when using Windows 7 and IE 8 to login SSL VPN.

Condition:

1. Prepare a PC which is installed Windows 7 and make sure SecuExtender have not installed on this PC before
2. Login ZyWALL via SSLVPN using IE8 from the PC we prepared
3. The SecuExtender cannot be installed successfully and logout immediately

41. [BUG FIX] 090828851

Symptom:

ZySH daemon will be crashed when frequently refreshing Dashboard

Condition:

1. Reset to default configuration
2. Attached many PC on LAN subnet and get the IP addresses dynamically
3. Login ZyWALL via GUI and sometimes ZySH daemon will be crashed

## Features:

---

Modifications in 2.20(AQW.1)b1 - 2010/03/12

1. [BUG FIX] 091020199

Symptom:

One log of IDP custom signature displays incorrectly

Condition:

The IDP log content is not the same with the content when mouse over

2. [BUG FIX] 091022419

Symptom:

When change system name, user needs to reboot DUT to get correct system name by SNMP.

Condition:

1. Modify system name
2. Load ZLD private MIB file into MG-SOFT software and compile them
3. Use MG-SOFT to query DUT, got wrong system name which is not modified by step 1
4. If reboot DUT, MG-SOFT can query correct system name

3. [BUG FIX] 091029777

Symptom:

Under certain condition, the static DHCP record can't be released from DHCP Table.

Condition:

1. Reset to default configuration
2. PC get IP from LAN and reserve it via Dashboard > DHCP Table
3. Configure DMZ to be a DHCP server and disable Firewall
4. Connect the same PC to DMZ and get another IP
5. Reserve the IP got from DMZ DHCP server and the error message popped up
6. Release the DHCP record got from LAN will success but release the DHCP record got from DMZ will be fail

4. [BUG FIX] 091102056

Symptom:

DDNS HA didn't work if pull out Cellular card

Condition:

1. Interface > Ethernet , edit WAN interface
  - 1) Enable Interface: active
2. Interface > Cellular , edit cellular2
  - 1) Enable Interface: active



- 2) Zone: WAN
- 3) Profile Selection: Device; Profile1
- 4) PIN Code: 0000
3. Network > DDNS , add a rule
  - 1) Profile Name: ddns1
  - 2) DDNS type: DynDNS
  - 3) Username: xxxx
  - 4) Password: xxxx
  - 5) Domain name: test.dyndns.org
  - 6) Primary Binding Address: Interface(cellular2) ; IP address (Interface)
  - 7) Backup Binding Address: Interface(wan1) ; IP address (Interface)
4. When cellular2 up and the WAN interface up, DUT update the ddns with Cellular2's IP address
5. When pull out cellular2, DUT didn't update the ddns with WAN interface's IP address
5. [BUG FIX] 091105437

Symptom:  
The log of VPN ping check is not right

Condition:

  1. Configure IPSec Connectivity Check with ICMP method
  2. We can see one incorrect IPSec Ping Check log in log page like below
    - Receive an ICMP IPSec connectivity check packet "request"...
  3. "request" should be "reply"
6. [BUG FIX] 091118561

Symptom:  
3G pin code unlock from dashboard and monitor page can't be saved to configuration

Condition:

  1. When pin code locked, go to dashboard or monitor page to unlock pin code
  2. Once pin code unlocked successfully, reboot the device. But you will find the pin code is locked again
  3. The unlock action on dashboard and monitor should saved the configuration to cellular
7. [BUG FIX] 091126359

Symptom:  
PPTP and PPPoE Authentication Type can't be saved via Wizard

Condition:

  1. In Wizard, interface Encapsulation is PPTP, click Next button. Authentication type is PAP
  2. Configure other fields with necessary fields and finish the wizard

3. Go to ISP Account page, check corresponding account: the value of Authentication Type is still Chap/PAP, not PAP
4. PPPoE has the same problem
8. [BUG FIX] 091201110  
Symptom:  
Error string not found after issuing a debug CLI command  
Condition:
  1. Do not turn Boot Module debug flag
  2. Enter CLI command “debug service-register erase service all”
  3. ZySH return error message “ERROR: Error string not found”
  4. It should return a meaningful error message
9. [BUG FIX] 091204287  
Symptom:  
Strange log triggered when logout from SSH connection  
Condition:
  1. Login DUT via SSH service
  2. Logout SSH
  3. There are some strange logs triggered in log page
10. [BUG FIX] 091215063  
Symptom:  
Left panel doesn't expand when linking to system name page from Dashboard.  
Condition:
  1. Change system language to Traditional Chinese
  2. Left panel doesn't expand when linking to system name page from Dashboard
  3. This issue doesn't happen when system language is English
11. [BUG FIX] 091223729  
Symptom:  
GUI will pop up error message when displaying the cache of content filter  
Condition:
  1. Enable Content Filter
  2. Add one profile
  3. Create on Content Filter policy rule with the profile
  4. Access the web sites and make the number of cache grow to the Max number
  5. Try to display the last page of the cache
  6. GUI returns the error message like “Wrong CLI...”
12. [BUG FIX] 091224805  
Symptom:  
In QuickSetup, the title name is wrong in summary page.

Condition:

1. Click Quick Setup Web Help and select the “VPN setup”
2. Select the “Advanced” type of VPN policy
3. Anyone “Scenario” and go to next page, and setup phase1 and phase2 accordingly
4. In Summary page, the title shows “Express Settings”

13. [BUG FIX] 091224807

Symptom:

Invalid validation error message in log mail subject field

Condition:

1. Enter Configuration > Log & Report > Log Setting
2. Edit the System Log item
3. In E-mail Server 1, input more than 60 characters
4. The invalid field error message displays incorrect content

14. [BUG FIX] 091224808

Symptom:

VPN connection should not be able to dialed out when it is configured as Manual Key

Condition:

1. Enter Configuration > VPN > IPsec VPN
2. Create one VPN connection with Manual Key configured
3. The “Connect” icon of the VPN Connection table can be click
4. Actually the “Connect” icon should not be able to click when VPN Connection is configured as Manual Key

15. [BUG FIX] 091225951

Symptom:

Error message popped up when modifying the ADP profile name

Condition:

1. Change the default ADP profile name then press “Save” button
2. GUI will pop up error message like “CLI number :0 Error number: -32034, Error message: Show flood- detection failed”

16. [BUG FIX] 091228032

Symptom:

Mouse Over on HOST type address cannot show the basic content in NAT page.

Condition:

1. Create one NAT rule and assign Host Type address object to Original IP or Mapped IP
2. Mouse over on the address object but nothing displayed

17. [BUG FIX] 091228990

Symptom:

There is no invalid field error message to remind user what is the max characters that user can input

Condition:

1. Enter Configuration > Object > Certificate page
2. Click “Add” icon to create a certificate
3. Input more than 31 characters in the Name field
4. There is no invalid field error message to remind user what is the max characters that user can input

18. [BUG FIX] 091229084

Symptom:

Some wordings are not translated properly

Condition:

1. Change the system language to Simplified Chinese
2. Enter 监控->统计->切换至图形视图, the button “注册” need translate to “刷新”
3. Enter 监控->Anti-X 统计数据->防垃圾邮件, the table “状态” need use Simplified Chinese, it's use Traditional Chinese

19. [BUG FIX] 091229109

Symptom:

The warning message is incorrect in certificate import page.

Condition:

1. Enter Configuration > Object > Certificate page
2. Import a certificate
3. Select one PKCS#12 type certificate you want import from your disk
4. Leave the password empty and click OK
5. Error message popped up “errno:-17030; errmsg: Invalid PKI PKCS#12 password”. This is correct and click OK to close the error message window
6. GUI will mark the Password field invalid but there is no description for it
7. There is no need to mark the Password field invalid

20. [BUG FIX] 091229148

Symptom:

Incorrect summary content when adding PPPoE via installation wizard

Condition:

1. Reset to default configuration
2. Login to GUI and the installation wizard popped up
3. Select “I have Two ISP” and continue the configuration
4. Configure the first WAN as Ethernet interface
5. Configure the second WAN as PPPoE interface
  - 1) Service Name: aaa

2) User Name: aaa

3) Enable nail-up

6. In the summary page of Internet Access Configuration page, the content is incorrect

21. [BUG FIX] 091229169

Symptom:

There is no field error message to remind user when inputting more than 255 characters

Condition:

1. Enter System > DNS page
2. Create one A record with FQDN content more than 255 characters
3. Click OK but system cannot save the configuration successfully
4. GUI should have field invalid error message to remind user and cannot allow user to click OK button

22. [BUG FIX] 091230289

Symptom:

The custom signature still works even it was deleted

Condition:

1. Create one custom signature like below
  - 1) Severity: Low
  - 2) Platform: All
  - 3) Service: ICMP
  - 4) Policy Type: Scan
  - 5) Header Option: Transport Protocol = ICMP, Type = 8, Code = 0
2. Activate this custom signature in the related IDP profile and make sure this custom signature works
3. Delete the custom signature
4. We found the custom signature still works and it could be found in the IDP profile

23. [BUG FIX] 091230303

Symptom:

The error message for the invalid field is incorrect for some fields

Condition:

1. Try to add a NAT or DDNS rule
2. In rule name field, input more than 31 characters
3. There will be an error message for indicating the invalid field and remind the constraint of that field
4. The content of the error message is wrong that it said the max characters we can input is 30 but actually it should be 31

24. [BUG FIX] 091230376

Symptom:

The wording of the error message of the invalid field is incorrect

Condition:

1. Edit an Ethernet interface
2. Configure its Connectivity Check and assign the invalid IP address format to “Check this address”
3. The error message for this invalid field will be popped up and displays “The value should be an IP address or an FQDN”
4. “an FQDN” should be changed to “a FQDN”

25. [BUG FIX] 100104012

Symptom:

IP/MAC Binding cannot reset to default after applying system default configuration

Condition:

1. Apply default configuration file. Connect PC to LAN port and connect WAN port to Internet
2. Activate IP/MAC Binding for LAN and WAN
3. Apply system default configuration
4. We found the IP/MAC Binding for WAN are still activated

26. [BUG FIX] 100104093

Symptom:

The default value is different when adding a user object from different place

Condition:

1. Add a user object via Configuration > Object > User/Group > User page, GUI will assign default value for “Description” field
2. Add a user object via Configuration > VPN > SSL VPN > Access Policy Summary’s policy edit page, GUI won’t assign the default value for “Description” field

27. [BUG FIX] 100104124

Symptom:

The Force User Authentication is disabled when changing the Authentication status

Condition:

1. Add a EPS object “dd”
2. Add a Authentication policy “tt”,enable Enable EPS Checking,enable Periodical checking time=3, add dd to slected EPS object.do not apply
3. Change Authentication status from required to unnecessary, do not apply.
4. Change Authentication status from unnecessary to required again, you will find the checkbox of Force User Authentication change from enable to disable, the others setting are reserved

28. [BUG FIX] 100106345

Symptom:

Wording issue: the Warning Message: “Default L2TP crypto map is going to be deleted. You can recover it via L2TP CLI command.” has wrong word “going”, it should be “going”

Condition:

1. Enter into Configuration > VPN connection page
2. Remove the default VPN connection rule
3. The warning sentence “Warning Message: ‘Default L2TP crypto map is going to be deleted. You can recover it via L2TP CLI command.’” pops up
4. It has one wrong word “going”, it should be “going”

## 29. [BUG FIX] 100106358

Symptom:

Under certain condition, adding user object in L2TP VPN page is not right

Condition:

1. Enter into Configuration > L2TP VPN page
2. Add one user by clicking “Create new object”
  - 1) User name is “aa”
  - 2) Password is “1234”, Retype is “1234”
  - 3) Authentication Timeout Settings is “Use manual Settings”
  - 4) Lease time is “22”
  - 5) Reauthentication time is “22”
3. This rule can be saved without any warning, but checking this user, the “Authentication Timeout Setting” option is still “Use Default Settings”

## 30. [BUG FIX] 100106400

Symptom:

Extension Slot display issue for Huawei 3G card.

Condition:

1. Insert Huawei E220 3G card
2. 3G’s Status displayed error in Extension Slot as below

#	Slot	Device	Status
=====			
2	USB 1	Huawei E220/E270/E800/E18	0Inactive

## 31. [BUG FIX] 100107482

Symptom:

AV White/Black List cannot allow more than 80 characters filled in

Condition:

1. Enter into Configuration > Anti-Virus > Black/White list > Black list page
2. Add one rule, filling log characters (more than 80 characters) in File Pattern field, there is no any warning

3. Click OK button, one window “Wrong CLI command, device timeout or device logout” pops up

32. [BUG FIX] 100107487

Symptom:

Display setting change will affect Priority setting.

Condition:

1. In Monitor > View Log page, Show Filter. Display=Anti-Spam, Priority=alert, click search
2. Change Display=Anti-Virus, you will find that the Priority has been changed to any t the meanwhile

33. [BUG FIX] 100108579

Symptom:

In AV > Black/white list page, add one rule, under certain condition, the rule saved is not right

Condition:

1. Enter into Configuration > Anti-virus > Black/White list page
2. Add one black list rule (or white list rule), in adding window, uncheck “Enable” checkbox, fill in “1” in File Pattern, apply
3. Check the rule saved, this rule is still enabled

34. [BUG FIX] 100111680

Symptom:

Under certain condition, user can’t login DUT

Condition:

1. Create one Auth. Method including Radius Server(first), and Local(second)
2. Make the Radius Server can’t be reachable by DUT
3. Login DUT via GUI with a local user in DUT cannot be successful

35. [BUG FIX] 100111699

Symptom:

Under certain condition, ADP profile rule cannot be edited successfully

Condition:

1. Enter into Configuration > Anti-x > ADP > Profile page
2. Edit one profile
3. In Scan Detection field, select all rules, inactive them, the log option is “log alert”, the Action option is “block”, click “OK” button
4. One error message “Wrong CLI command, device timeout or device logout” pops up, and checking the rule saved, it is not right

36. [BUG FIX] 100112841

Symptom:



Under certain condition, PCs behind DUT cannot get IP address

Condition:

1. Reset to default configuration
2. Configure different DHCP Server setting on ge4 and ge5
3. Join Port 4 and Port 5 into ge4
4. Join Port 4 and Port 5 into ge5
5. PC connected to Port 4 and Port 5 cannot get the IP address from DUT

37. [BUG FIX] 100112888

Symptom:

When adding two user defined trunk into DUT which have long name, the name showed in Default WAN Trunk field is incomplete

Condition:

1. Enter into Configuration > Interface > Trunk page
2. In User Configuration, add two user defined trunks, "SYSTEM\_DEFAULT\_WAN\_TRUNK1" and "SYSTEM\_DEFAULT\_WAN\_TRUNK2"
3. These two trunks' name showed in Default WAN Trunk field is incomplete

38. [BUG FIX] 100113962

Symptom:

3G budget will be reset when 3G interface disconnected because of idle time out.

Condition:

1. Insert one 3G card, add a 3G interface.
  - 1) Disable Nailed-Up
  - 2) Configure the idle timeout value
  - 3) Configure the Time Budget
2. After the 3G interface disconnected due to idle timeout, the Time Budget will be reset also

39. [BUG FIX] 100113972

Symptom:

Wording issue, one log about ping check has wrong word "an", it should be "a"

Condition:

One log about TCP mode ping check "Receive an TCP IPSec Connectivity check packet request" has wrong word "an", it should be "a"

40. [BUG FIX] 100114086

Symptom:

Use MG-Soft Software look CPU information , log have Error Message "#configure terminal show \_zldmib session status, file not found"

Condition:

1. Enable SNMP

2. Server Port=161, Get Community=public, Set Community=private, Trap/Community=blank, Destination=blank
3. Use MG-Soft Software look CPU information
4. Log have Error Message “#configure terminal show \_zldmib session status, file not found”

41. [BUG FIX] 100114100

Symptom:

Configure static PPPoE based on ge3 via Quick Setup, the dns order is incorrect in DNS page

Condition:

1. Configure PPPoE interface via Quick Setup
2. Configure this PPPoE interface with static IP Address
3. Configure two DNS servers for its first and second DNS server
4. Configure other settings accordingly
5. After finish the setup, the DNS order is incorrect

42. [BUG FIX] 100114134

Symptom:

Outgoing traffic from DUT itself cannot follow Policy Route configuration

Condition:

1. Configure two WAN interfaces, one is Ethernet and another is 3G interface
2. Add one Policy Route, from ZyWALL to Any, next hop is the 3G interface
3. Configure Syslog Email Server properly and click “E-mail Now”
4. We found sometimes the mail traffic goes out via the Ethernet interface or goes out via the 3G interface but carry the incorrect interface IP address

43. [BUG FIX] 100118397

Symptom:

Sometimes HTTPS cannot follow Firewall configuration

Condition:

1. Reset to default configuration
2. Create Firewall rule to allow some services from WAN to ZyWALL without HTTPS
3. Change the default Firewall rule to be deny
4. Accessing ZyWALL via HTTPS should not work but sometimes it works after reboot DUT several times

44. [BUG FIX] 100119445

Symptom:

There is not content displayed when mouse over the Local/Remote Policy in VPN Connection

Condition:

1. Create one VPN Connection Local/Remote Policy assigned
2. Move mouse over the Local/Remote Policy but there is not object content displayed

45. [BUG FIX] 100119492

Symptom:

The “Window Size” item can’t be saved correctly when editing a custom signature

Condition:

1. Anti-x > IDP > Custom Signatures, add a new signature
  - 1) name = Test
  - 2) Severity = low
  - 3) Platform = all
  - 4) Service = ICMP
  - 5) Policy Type = Scan
  - 6) Transport Protocol = TCP, Window Size equals to 16190, other settings are default
2. Edit this signature again, in “Window Size” item, the ”equal” is not selected

46. [BUG FIX] 100119517

Symptom:

Interface Status Summary at Dashboard always displays Dialing

Condition:

1. Configure one PPP interface and activate it
2. Click the dial icon of the PPP interface in Interface Status Summary table in Dashboard
3. The pop up window always display “Dialing...”

47. [BUG FIX] 100120705

Symptom:

There is no warning message when user intends to upload the startup-config.conf

Condition:

1. There is no warning message when user intends to upload the startup-config.conf
2. There is one warning message popped up when user intends to upload the startup-config.conf in before 2.20

48. [BUG FIX] 100120721

Symptom:

Static DHCP IP/MAC binding cannot work for bridge interface

Condition:

1. Create one bridge interface with all interfaces joined
2. Configure this bridge interface as a DHCP server
3. Connect one PC to DUT and can get the IP address A from DUT correctly
4. Create one Static DHCP IP/MAC binding “IP-B<->PC’s MAC” in the bridge interface
5. Renew the IP address on the PC but the PC still gets IP address A

49. [BUG FIX] 100120740

**Symptom:**

The sorting result is not correct in AppPatrol Statistics

**Condition:**

1. Enable Application Patrol and make some traffic through DUT
2. Enter MONITOR > AppPatrol Statistics
3. In Protocol Statistics, sorting result is not correct

**50. [BUG FIX] 100120784**

**Symptom:**

Test one empty URL in “Test Web Site Category” causes GUI keeps loading

**Condition:**

1. Create one Content Filter Profile
2. Enter this profile and input nothing in “URL to test” field
3. GUI will keep loading

**51. [BUG FIX] 100121844**

**Symptom:**

When add a pppoe account in ISP Account, the Service Name can't be saved correctly

**Condition:**

1. Add one ISP account as below
  - 1) Profile Name = pppoe
  - 2) Protocol = pppoe
  - 3) Authentication Type = Chap/PAP
  - 4) User Name = testzywall
  - 5) Password = 1234
  - 6) Service Name = pppoe
  - 7) Idle timeout = 0
2. Check this pppoe account just you added, you will find the Service name is blank, not “pppoe”.

**52. [BUG FIX] 100121849**

**Symptom:**

In PPTP interface , the ISP Setting did not show the corresponding content of pptp account

**Condition:**

1. Create one ISP account with PPTP protocol
2. Create one PPP interface with this PPTP ISP account
3. The ISP Setting in the PPP interface edit page does not display the corresponding configuration

**53. [BUG FIX] 100121930**

**Symptom:**

Dashboard display abnormal if using IE browser from "Packet Capture" page to "DASHBOARD" page

Condition:

1. Use IE browser to login device
2. Go to page MAINTENANCE > Diagnostics > Packet Capture page, then go to "DASHBOARD" page
3. DASHBOARD page display abnormal on "Virtual Device" and "Interface Status Summary" widget

54. [BUG FIX] 100125239

Symptom:

DHCP configuration could not be saved when DHCP relay has a wrong value

Condition:

1. Edit DMZ interface
2. Set it as DHCP Relay and server is 192.168.8.2. Apply it
3. Edit the DMZ interface again
4. Change the DHCP Relay server IP to "192.168" first
5. Change the DHCP setting to DHCP Server. Start Address is 192.168.2.33 and pool size is 25. Apply it
6. Edit the DMZ interface again
7. The DHCP setting is still DHCP Relay instead of DHCP server

55. [BUG FIX] 100126382

Symptom:

IPSec SA won't be removed in remote gateway when IPSec Fallback successfully

Condition:

1. Create one VPN Connection with Primary and Secondary gateway and IPSec Fallback is activated
2. Make DUT Fail Over and Fallback once
3. Check the secondary gateway and found the SA on remote secondary gateway was not removed

56. [BUG FIX] 100201066

Symptom:

The configuration won't be saved correctly when configuring PPPoE via Quick Setup

Condition:

1. Configuring PPPoE interface via Quick Setup and sets its service name including "%" character
2. After finishing the PPPoE configuration via Quick Setup, the PPP interface setting is not correct when editing that PPP interface

57. [BUG FIX] 100203203

Symptom:

Device will apply lastgood.conf or system-default.conf after reboot

Condition:

1. Create one user named “abcde” via GUI
2. Create one user named “abcd” which user type is “ext-user” or “ext-group-user” via GUI
3. Reboot DUT
4. DUT will try to apply lastgood.conf or system-default.conf

58. [BUG FIX] 100204340

Symptom:

Site Map window might be closed when clicking a specific area in the Site Map window

Condition:

1. Open Site Map window
2. Click some empty area in the Site Map window
3. The Site Map window might be closed

59. [BUG FIX] 100205425

Symptom:

The signature version of IDP/AV in License Service Status table in Dashboard is abnormal

Condition:

1. Login DUT via GUI
2. Refresh the table of License Service Status
3. The signature version of IDP/Av displayed abnormally

60. [BUG FIX] 100205463

Symptom:

Some characters are overlapped when using Traditional Chinese or Simplified Chinese

Condition:

1. Add a Static DHCP rule for LAN interface
2. Edit the LAN interface again and found the wording of the grid of the DHCP static setting is overlapped

61. [BUG FIX] 100207588

Symptom:

VLAN interface cannot be applied successfully in a specific case

Condition:

1. Create one VLAN interface called vlan0 with a Static DHCP setting record
2. Remove the VLAN interface vlan0
3. Create one VLAN interface called vlan3 with the same setting as vlan0 we just removed
4. The VLAN interface vlan3 cannot be applied successfully with one warning message popped up

62. [BUG FIX] 100207599

Symptom:

3G Budget will be reset every 30 seconds in a specific case

Condition:

1. Create one 3G interface with below setting
  - 1) Enable Budget Control
  - 2) Enable Time Budget and Data Budget
  - 3) Reset time and data budget counters on the 5<sup>th</sup> day of each month
2. Configure the system date to the date which is configured in item 3 of step 1
3. 3G Budget will be reset every 30 seconds

63. [BUG FIX] 100208653

Symptom:

Device will apply lastgood.conf or system-default.conf after reboot

Condition:

1. Create maximum number of DNS MX records
2. Create additional one DNS MX record and it should be failed
3. Reboot DUT
4. DUT will try to apply lastgood.conf or system-default.conf

64. [BUG FIX] 100209721

Symptom:

The release date of the EPS signature is wrong

Condition:

1. The release date of EPS signature in 2.20 B4 is 2009/11/19
2. The release date of EPS signature in 2.20 B5 is 2009/1/21. It is incorrect

65. [BUG FIX] 100209767

Symptom:

EPS check with Avira\_Antivir\_Personal\_v2009 traditional Chinese edition will always fail

Condition:

1. Configure one EPS object with checking Avira\_Antivir\_Personal\_v2009
2. PC installs Avira\_Antivir\_Personal\_v2009 Traditional Chinese version
3. Create one SSLVPN policy with checking this EPS object
4. PC logs in to SSLVPN will always fail due to EPS checking

66. [BUG FIX] 100210895

Symptom:

EPS checking will be still performed even the Auth. Policy is not in the schedule

Condition:

1. Create one Auth. Policy with EPS checking required and schedule assigned
2. Login DUT via GUI at the time which is not in the schedule
3. The EPS checking will be still performed

67. [BUG FIX] 100222079

Symptom:

SSL VPN's File Sharing menu bar's "up" button to translate wrong Traditional Chinese word

Condition:

1. Login DUT via SSLVPN
2. Change the SSL VPN GUI language to Traditional Chinese, the menu bar's "up" was to translate wrong Traditional Chinese word = 運作中

68. [BUG FIX] 100224215

Symptom:

3G interface cannot be activated in a specific case

Condition:

1. Create one 3G interface via GUI and disable it at first
2. Edit this 3G interface again
3. Activate this interface and click Apply
4. GUI will return "No need to apply" and this is not correct

69. [BUG FIX] 100301012

Symptom:

PC can PING Internet host even PING service is removed from Exceptional Service table in Auth. Policy page

Condition:

1. Reset to default configuration
2. Enable Authentication Policy
3. Create one Auth. Policy rule. From LAN\_SUBNET to ANY, Authentication = force
4. Remove all rules in Exceptional Service table
5. Add PING service first then DNS Service
6. Remove PING service from Exceptional Service table
7. We found PC under LAN\_SUBNET can still PING Internet hosts



## Features:

---

Modifications in 2.20(AQW.0) - 2010/02/25

Modify for formal release

## Features:

---

Modifications in 2.20(AQW.0)b6 - 2010/02/23

1. [BUG FIX] 100211949

Symptom:

In Device-HA mode, Backup cannot build up VPN tunnels successfully after it took over

Condition:

1. Configure Device HA properly on Master and Backup and its monitored interface is a bridge interface
2. Configure one VPN rule on both Master and Backup with My Address configured as FQDN type
3. Make sure the VPN tunnel can be dialed up in Master
4. Make Backup take over but the VPN tunnel on Backup cannot be dialed up successfully

2. [BUG FIX] 100211954

Symptom:

In Device-HA mode, Master cannot build up the VPN tunnel successfully if the My Address in VPN Gateway is configured as IP address

Condition:

1. Configure Device HA AP Mode properly on Master
2. Configure one VPN rule properly and My Address in VPN Gateway is configured as IP address
3. The interface which owned the My Address is monitored by Device HA
4. The VPN tunnel cannot be dialed up

## Features:

---

Modifications in 2.20(AQW.0)b5 - 2010/01/29

1. [ENHANCEMENT]

PPTP ALG supports PPTP Server at LAN

2. [ENHANCEMENT]

Update Java certificate expiration date to 2012/1/20

3. [BUG FIX] 091222674

Symptom:

Login DUT with a normal user will be fail after Login DUT over 50 times with different users

Condition:

1. Use different users to login DUT over 50 times
2. Login DUT with a new user and cannot login successfully

4. [BUG FIX] 091229192

Symptom:

Webpage will stay in "loading" status after special operation.

Condition:

1. Reset DUT to system-default configuration file
2. Go to Log Setting page, edit Remote Server 1: Server Address=172.25.22.36, Active

Log=enable normal logs, apply

3. Go to Object > Schedule page, the webpage will stay in "loading" status

5. [BUG FIX] 091229204

Symptom:

DUT will apply system-default configuration when F/W from v2.12 upgrade to 2.20b4 and then reboot DUT.

Condition:

1. Upgrade to 2.20 B4
2. Downgrade to 2.12
3. Apply system-default configuration, and change system name via GUI
4. Upgrade to 2.20 B4
5. Reboot DUT
6. Failed to apply startup-config.conf, Because " ERROR: force-auth default-rule authentication allow no log ".

6. [BUG FIX] 091230324

Symptom:

Under certain condition, Ping Check doesn't work

Condition:

PC --- LAN(DUT)WAN--- Internet

1. Use system default configuration
2. Leave WAN port unplug
3. Enable Ping Check on WAN interface, the check period is 5, others keep default
4. Plug back the WAN interface
5. The PC can access Internet but there is no Ping packet sent out via WAN interface

7. [BUG FIX] 091231492

Symptom:

EPS check of KAV 2009/2010 always fail in Windows 2000

Condition:

1. Create EPS object to check KAV 2009 or KAV 2010
2. Create one Auth. Policy to check the EPS
3. Login DUT from host which runs Windows 2000 and always fail

8. [BUG FIX] 100104033

Symptom:

EPS Failure for checking Kaspersky\_Internet\_Security\_v2009

Condition:

1. Add a EPS rule for check Kaspersky\_Internet\_Security\_v2009
  - 1) Endpoint Operating System : Windows
  - 2) Window Version : Windows XP2
  - 3) Endpoint must have Personal Firewall installed : Enable
  - 4) Allowed Personal Firewall List : Kaspersky\_Internet\_Security\_v2009
  - 5) Endpoint must have Anti-Virus software installed : Enable
  - 6) Allowed Anti-Virus Software List : Kaspersky\_Internet\_Security\_v2009
2. Install KIS v8.0.0.523 on Windows XP2, and login device will always checking failure

9. [BUG FIX] 100104076

Symptom:

All button of File Sharing can't work via SSL VPN

Condition:

1. Edit Object > User/Group > User , add a test1
2. Edit Object > SSL Application , add rules
  - 1) Name=Filesharing\_NAS ; Shared Path=\\172.25.25.240\sic
3. Edit web eWC/SSL VPN/Access Privilege , add rules
  - 1) Name=File\_share , User / Group Member=test1 , SSL Application List /

Member=Filesharing\_NAS

4. test1 can browse Windows file sharing folder but can't use all of button: New Folder,renam,upload,remove,download,up

10. [BUG FIX] 100104109

Symptom:

AUX cannot work.

Condition:

1. Enable aux interface
2. Click the connect icon, but nothing happened

11. [BUG FIX] 100105162

Symptom:

If the quick setup PPPoE's username include symbol '%' will can't save the setting.

Condition:

1. Press the Quick setup button to setup PPPoE with username = az%99 then press next to finish
2. Check the interface- > PPP interface's setting is not saved

12. [BUG FIX] 100113049

Symptom:

Dial up L2TP over IPSec tunnel cause DUT crazily sends hello packets to client.

Condition:

1. Reset to default configuration
2. Create 2<sup>nd</sup> VPN connection
3. L2TP client dials up the L2TP tunnel and found there are lots of L2TP hello packet

sends to L2TP client

## Features:

---

Modifications in 2.20(AQW.0)b4 - 2009/12/25

1. [ENHANCEMENT]

GUI Web Help is ready

2. [ENHANCEMENT]

Multi-Language is ready

3. [ENHANCEMENT]

New CLI command “*policy-route controll-virtual-server-rules*”. Below is the short description for the CLI command

1) In the past, 2.1x firmware, NAT 1-1 and NAT-Loopback functionality is achieved by creating additional Policy Route rules on TOP of Policy Route table automatically. The content of Policy Route table is possibly like below

(1) From LAN\_SERVER1 to any, nexthop is WAN1, SNAT: outgoing interface

(2) From LAN\_SERVER2 to any, nexthop is WAN2, SNAT: outgoing interface

(3) From LAN to any, nexthop is WAN\_TRUNK, SNAT: outgoing interface

2) In 2.20 release, the Routing and Source NAT priority of NAT 1-1 and NAT-Loopback is lower than Policy Route

3) If user configured several NAT 1-1 and NAT-Loopback rules in 2.1x firmware, there is one possibility to let the new created NAT 1-1 and NAT-Loopback cannot work anymore after upgrading to 2.20 firmware.

When creating a new NAT 1-1 or NAT-Loopback NAT rule in 2.20 firmware, DUT won't create the related Policy Route rule for that NAT rule but create the accordingly NAT 1-1 or NAT-Loopback Routing/SNAT rules automatically with lower priority than Policy Route. But it might not work because some OLD Policy Route Rule created in 2.1x firmware might overwrite its functionality like 1)→ (3) above

4) We create one CLI command to make the Routing/SNAT priority of NAT rule higher than Policy Route to avoid this situation

5) *policy-route controll-virtual-server-rules activate*

Make the priority of Routing/SNAT of NAT rules lower than Policy Route

6) *no policy-route controll-virtual-server-rules activate*

Make the priority of Routing/SNAT of NAT rules higher than Policy Route

7) If system detects firmware upgrading from those before 2.20, system will make the priority of Routing/SNAT of NAT rules higher than Policy Route

8) System will make the priority of Routing/SNAT of NAT rules lower than Policy Route by default configuration

4. [ENHANCEMENT]

Add i-note to tell user that creating a certificate with DSA-2048 will take long time

## 5. [ENHANCEMENT]

Remove two obsolete categories and automatically maps them to related new categories

- 1) sexuality-alternative-lifestyles → alternative-sexuality-lifestyles
- 2) alcohol-tobacco → alcohol and tobacco

## 6. [FEATURE CHANGE]

WAS

Japanese is one of the supported languages

IS

Japanese is not supported anymore

If user uses Japanese in former firmware, it will be set to English automatically after upgrading to 2.20 B4 firmware

## 7. [BUG FIX] 090827638

Symptom:

IDP custom signatures can be exported, but cannot imported by default name:

custom.rules

Condition:

1. Anti-x > IDP > Custom Signatures, click the checkbox of Export, then Export it which filename called custom.rules
2. Anti-x > IDP > Custom Signatures, delete all custom signatures
3. Anti-x > IDP > Custom Signatures, add a new signature
4. Anti-x > IDP > Custom Signatures, import the custom

5. All custom signatures are disappeared

8. [BUG FIX] 090828859

Symptom:

VPN of PFS group behavior is incorrect.

Condition:

1. Setting the PFS use DH1 group on DUT1 phase2 rule
2. Setting the PFS use none on DUT2 phase2 rule
3. VPN tunnel still can establish between DUT1 and DUT2

9. [BUG FIX] 090901031

Symptom:

Manual key VPN of policy enforcement function cannot work.

Condition:

PC1 --- DUT1 --- VPN --- DUT2 --- PC2

1. Add a manual key rule on DUT1, and enable policy enforcement by CLI command
2. Add a policy route on DUT1 from Any to Remote Subnet
3. Add a manual key rule on DUT2
4. The policy enforcement cannot work. because the PC1 still can ping to PC2

10. [BUG FIX] 091124142

Symptom:

GUI service object of ICMP protocol cannot see "User Defined ICMP type" ICMP type.

Condition:

1. Go to page Configuration > Object > Service, add a service object
2. In ICMP protocol does not see that "User Defined ICMP type" type

11. [BUG FIX] 091124212

Symptom:

The encryption ESP packet always send wrong interface if the DUT have two WAN interfaces.

Condition:

1. This issue happens on PQA gateway
2. PQA gateway has two wan interfaces that pppoe1 and pppoe2
3. Establish IPSecVPN tunnel by pppoe1 interface
4. Make sure IPSecVPN tunnel established, but the encryption ESP packet always send out from pppoe2 interface
5. The issue cannot solve by any method (e.g. policy route or metric).

12. [BUG FIX] 091126385

Symptom:

When address range ip more than three ,SNAT don't work

Condition:



1. Create one address object with Range Type and over three IP addresses
2. Configure one Policy Route rule which do the SNAT with the Range Type address object just created

3. PC on LAN cannot access Internet

13. [BUG FIX] 091203243

Symptom:

After enable AS, sending Mail via VPN cannot work

Condition:

Mail Server --- DUT1 --- VPN --- DUT2 --- Mail Client

1. Build on Site-To-Site VPN between DUT1 and DUT2
2. Create one Any to Any AS rule
3. Send mail via this VPN tunnel cannot success

## Features:

---

Modifications in 2.20(AQW.0)b3 - 2009/11/20

### 1. [ENHANCEMENT]

EPS Signature Update to 1.0.0.1 for supporting more AV/Firewall signatures

The new supported signatures are listed as below

- 1) Norton\_AntiVirus 2010
- 2) Norton\_Internet\_Security 2010
- 3) Norton\_360 Version, version 3
- 4) TrendMicro\_PC-Cillin\_Internet\_Security 2010
- 5) TrendMicro\_PC-Cillin\_Internet\_Security\_Pro 2010
- 6) TrendMicro\_PC-Cillin\_AntiVirus 2010
- 7) Avria AntiVir Personal 2009
- 8) Microsoft\_Security\_Center
- 9) Windows\_Firewall

To update EPS signature to 1.0.0.1, please enter below CLI command after firmware upgrade

Router> debug eps signature load-def

And you will find the EPS signature is updated via below CLI command

Router> show eps signature status

EPS signature information:

Current version : 1.0.0.1

Release date : 2009-11-19

Signature numbers : 18

### 42. [ENHANCEMENT]

Synchronize the system default configuration for all models. This enhancement will make the system default configurations between all models similar with the common policies

- 1) User guest is removed
- 2) The default lease time for admin is set to 30 minutes
- 3) Add default PPPoE ISP accounts for each default PPP interfaces
- 4) Bind the default PPPoE ISP accounts to the default PPP interfaces
- 5) Add GRE service object by default
- 6) Remove default user customized trunks
- 7) Remove default user configurable service control rules for HTTP/HTTPS/SSH/TELNET/FTP/DNS/SNMP
- 8) Synchronized the default firewall rules for all models

- 9) Remove LAN\_ADP, DMZ\_ADP and ZyWALL\_ADP anomaly profiles from default configuration
- 10) Add ADP\_PROFILE into default configuration and bind to default anomaly rules
- 11) Bind ADP\_PROFILE to default anomaly rules
- 12) Add default AV rules
- 13) Activate BWM by default(For performance testing, please turn off BWM first)

#### 43. [ENHANCEMENT]

There are some GUI enhancements for GUI

- 1) The wording of “SEM-UTM” on dashboard is changed to “SEM”. This is for USG2000 only
- 2) Mouse Over Enhancement  
When moving the mouse pointer on an object, GUI will display the basic content of that object. Supported objects are User Group/Address/Address Group/Service/Service Group/Zone/Schedule
- 3) Invalid Field Error Message Description Enhancement  
When user enters an invalid value checked by accordingly GUI pages, the error messages describing why they are invalid will be more user-readable.
- 4) Add State(Province) and Town(City) fields when creating a new certificate
- 5) Configuration Apply enhancement.  
When applying a configuration via GUI, GUI will pops up a window with 4 options for selecting
  - (1) Immediately stop applying the configuration file
  - (2) Immediately stop applying the configuration file and roll back to the previous configuration
  - (3) Ignore errors and finish applying the configuration file
  - (4) Ignore errors and finish applying the configuration file and then roll back to the previous configuration

#### 44. [ENHANCEMENT]

There will a log generated when interface renamed

#### 45. [ENHANCEMENT]

Add Object reference for OSPF

#### 46. [ENHANCEMENT]

Add CLI command to display URL Cache by range

Example

Router# show content-filter url-cache begin 1 end 5

No.	Category	TTL	URL
-----	----------	-----	-----

=====

1 Computers/Internet 4320

[http://sales.liveperson.net/hc/74453203/?&visitor=4180599234632&msessionkey=3003569313150301289&site=74453203&cmd=mTagInPage&lpCallId=958684555889-7231948013&protV=20&lpjson=1&page=http%3A//www-europe.cisco.com/cisco/web/solutions/small\\_business/cisco\\_small\\_business\\_pro/index.html&id=6323223163&javaSupport=true&visitorStatus=INSITE\\_STATUS&defInvite=chat-samba-sales-english&activePlugin=none&cobrowse=true&pageWindowName=seq](http://sales.liveperson.net/hc/74453203/?&visitor=4180599234632&msessionkey=3003569313150301289&site=74453203&cmd=mTagInPage&lpCallId=958684555889-7231948013&protV=20&lpjson=1&page=http%3A//www-europe.cisco.com/cisco/web/solutions/small_business/cisco_small_business_pro/index.html&id=6323223163&javaSupport=true&visitorStatus=INSITE_STATUS&defInvite=chat-samba-sales-english&activePlugin=none&cobrowse=true&pageWindowName=seq)

2 Social Networking 4235

<http://www.plurk.com/Poll/getResponseCount/159975383>

3 Social Networking 3910 <http://www.plurk.com/Poll/getResponsesN/3178044>

4 Search Engines/Portals 4295 <http://www.baidu.com/>

5 Proxy Avoidance 4320

<http://teuchi.net/browse.php?b=5&u=Oi8vd3d3LmZhY2Vib29rLmNvbQ%3D%3D>

#### 47. [ENHANCEMENT]

Support IPSec ESP ALG

The peer GWs have no need to enable NATT if ZyWALL in between. Below is an example scenario

ZyWALL-A  $\longleftrightarrow$  (WAN) DUT (LAN)  $\longleftrightarrow$  ZyWALL-B

(Acts as an NAT Router)

ZyWALL-A and ZyWALL-B can establish the VPN tunnel because DUT has IPSec ESP ALG supported (IPSec Pass Through)

#### 48. [ENHANCEMENT]

SSLVPN Windown 7 Support for both 32-bit and 64-bit

#### 49. [FEATURE CHANGE]

WAS

For USG2000, the Max VLAN number is 256

IS

For USG2000, the Max VLAN number is 512

#### 50. [FEATURE CHANGE]

WAS

User can't set empty string in eWC->Content Filter->Denied Access Message.

IS

User can set empty string in eWC->Content Filter->Denied Access Message.

When user set Denied Access Message empty and access the internet,

if the URL matches the category which should be blocked, web browser would

redirect to the Redirect URL directly without showing any Denied Access Message and category.

#### 51. [FEATURE CHANGE]

## WAS

In GUI, Maintenance > Diagnostics > Packet Capture > Capture > Interface

The left side interface list named “Interfaces” and the right side interface list named “Allowed interface”

## IS

In GUI, Maintenance > Diagnostics > Packet Capture > Capture > Interface

The left side interface list named “Available Interfaces” and the right side interface list named “Capture Interfaces”

### 52. [FEATURE CHANGE]

## WAS

In GUI page, Configuration > Auth. Policy > Authentication Policy Summary

The default rule displays “action” with “allow”, “drop” and “deny”

## IS

In GUI page, Configuration > Auth. Policy > Authentication Policy Summary

The default rule displays “Authentication” with “required” and “unnecessary”

And Log with “no”, “log” and “log alert”

### 53. [FEATURE CHANGE]

## WAS

Via CLI, default mode of the interface group is “normal” when creating a new interface-group

## IS

Via CLI, default mode of the interface group is “trunk” when creating a new interface-group

### 54. [BUG FIX] 090814172

#### Symptom:

Ping Check section cannot be configured anymore after enabling Ping Check

#### Condition:

1. Enter VPN/ IPsec/ VPN connection
2. Add or Edit a rule
3. Enable the ping check section and apply
4. Edit the rule again
5. Cannot disable Ping Check anymore

### 55. [BUG FIX] 090915152

#### Symptom:

SIP phone register FAIL when SIP ALG use port 5070

#### Condition:

1. Edit Configuration > Network > ALG , Enable SIP ALG
2. Set SIP Signaling Port = 5070

3. V300 use 5070 port register to SIP server FAIL

56. [BUG FIX] 090929397

Symptom:

IP/Mac Binding cannot work properly

Condition:

1. Apply default configuration
2. Create/enable a correct IP/MAC binding item on ge1 and make sure the host can access

Internet

3. Edit the IP/MAC binding item and replace a wrong MAC
4. The host shouldn't access Internet but it could

57. [BUG FIX] 091020246

Symptom:

The "Customized Access Page" setting can't be apply correctly.

Condition:

1. Apply default configuration
2. Configuration > System > WWW > Login Page, use "Use Customized Login Page"
3. Upload a picture as "Customized Access Page" and apply the setting after upload

successfully

4. Exit this page and then enter this page again, you will see the setting of "Customized Access Page" is "color" not "picture".

58. [BUG FIX] 091020250

Symptom:

3G interface in Default WAN Trunk sometime works incorrcet.

Condition:

1. Enable AUX interface
2. Insert E270 3G card in USB 1 slot
3. Configuration > Network > Interface > Cellular, enable cellular2 and Fill in necessary setting, then dial up 3G connection
4. Unplug WAN1 & WAN2 physical line
5. Configuration > Network > Interface > Trunk, check

SYSTEM\_DEFAULT\_WAN\_TRUNK have cellular2 interface, but LAN host's traffic can't out to internet

59. [BUG FIX] 091021311

Symptom:

The button 'Show Advance Settings/Hide Advance Settings' in Vlan page is abnormal.

Condition:

1. In VLAN page, add a new vlan interface

2. Click 'Show Advance Settings' button. You will see advanced settings is shown on page and the button 'Show Advance Settings' is changed into 'Hide Advance Settings'

3. Click the 'Hide Advance Settings'. Advanced settings is hidden on page but the button is not changed into 'Show Advance Settings' again

4. Then the button is useless. Click it, nothing will change

60. [BUG FIX] 091021313

Symptom:

after enabling "Auto Destination Address" checkbox, the policy rule saved is not right

Condition:

1. Add one policy rule in Routing page, select "Next-Hop" to dynamic VPN(except Default L2tp vpn rule), enable "Auto Destination Address", save it

2. check this policy again, the "Auto Destination Address" checkbox disappears, it is not right

61. [BUG FIX] 091022366

Symptom:

After dial L2TP successfully, PC cannot ping(or ftp) DUT through its LAN IP address

Condition:

1. Build one L2TP VPN successfully

2. Add one Policy Route rule, the source is DUT LAN subnet, the destination is L2TP pool, next hop is "Default\_L2TP\_VPN tunnel"

3. PC can ping LAN hosts, but cannot ping (or ftp) DUT LAN IP address

62. [BUG FIX] 091023471

Symptom:

PPP interface of PPTP protocol cannot work.

Condition:

1. In 2.20 default configuration, the PPTP connection always fails

2. If will firmware downgrade to 2.12 and apply 2.12 default configuration will work fine

3. If running 2.12 configuration on 2.20 firmware, it will work fine

63. [BUG FIX] 091026533

Symptom:

Click Dashboard twice, the GUI will hang

Condition:

1. Enter into GUI of DUT, the default page will be "Dashboard"

2. Click "Dashboard Tab"

3. The GUI will keep loading and have no response

64. [BUG FIX] 091027644

Symptom:

L2TP over IPSec with NAT-T doesn't work

Condition:

1. Connect L2TP from a host which is under a NAT Router
2. The L2TP tunnel will not connect successfully



## Features:

---

Modifications in 2.20(AQW.0)b2 - 2009/10/17

1. [ENHANCEMENT]

Turn on NAT Loopback when creating NAT rules via GUI

2. [ENHANCEMENT]

GUI Site Map is ready

3. [ENHANCEMENT]

GUI Login Page Customization is ready

4. [ENHANCEMENT]

EPS signature KAV 2009/2010 is ready. For updating the new EPS signature, please enter below CLI command after upgrading to 2.20 b2 firmware

Router> debug eps signature load-def

Router> show eps signature anti-virus

No.	Name	Detection
=====		
1	Kaspersky_Anti-Virus_v2009	yes
2	Kaspersky_Anti-Virus_v2010	yes

5. [ENHANCEMENT]

New 3G card support for Huawei E180 and E800

6. [ENHANCEMENT]

In VLAN edit page, add Zone selection for user quick configuration

7. [ENHANCEMENT]

There will be a log messages for Interface renaming

8. [ENHANCEMENT]

There is some enhancement for App.Patrol rules in GUI

1) In policy summary page, the “BWM In/Out/Priority” field will show “no/no/7” if Inbound and outbound BWM of the policy are disabled(0 is disable)

2) In policy edit page, the “Priority” field and “Maximize Bandwidth Usage” selection will be hidden if both Inbound and Outbound BWM setting are disabled

3) In policy edit page, the default Priority will be 4 for configuring BWM

9. [ENHANCEMENT]

GUI I-Note is ready

10. [ENHANCEMENT]

In GUI dashboard, add Interface status and Extension slot information

11. [ENHANCEMENT]

For L2TP authentication, supports special characters “!@#\$\$%^&\*()” as password

12. [FEATURE CHANGE]

WAS

There is help page in GUI right panel and old GUI link

IS

Remove the GUI right panel help page and old GUI link

13. [FEATURE CHANGE]

WAS

In GUI configuration page, click “Show All Setting” and “Show Basic Setting” will display advanced setting and hide advanced setting accordingly

IS

In GUI configuration page, click “Show Advanced Setting” and “Hide Advanced Setting” will display advanced setting and hide advanced setting accordingly

14. [BUG FIX] 090818327

Symptom:

User Group cannot be edited via GUI

Condition:

1. add on user which name is "user1"
2. add one user group which name is group1
3. edit the group1 rule, add the user "user1" to this rule, click "apply"
4. the rule cannot be saved, one error message showed "Wrong CLI command, device timeout or device logout"

15. [BUG FIX] 090819548

Symptom:

System time is not correct after rebooting the DUT

Condition:

1. In system Date/Time page
2. set the time and date setup is manual
3. set time zone is GMT+8
4. reboot DUT
5. DUT system time will be added more 8 hours compared with original time

16. [BUG FIX] 090819549

Symptom:

The first login wizard cannot be completed

Condition:

1. Reset to system default configuration
2. Login to DUT and the wizard will be popped up
3. Configure WAN as Ethernet or PPPoE mode
4. It always failed and error messages displayed

17. [BUG FIX] 090819699

Symptom:

IPSec tunnel cannot be built up again using IxVPN

Condition:

1. Build one IPSec tunnel using IxVPN
2. Disconnect the IPSec tunnel and the tunnel cannot be built up again
3. Reboot DUT and the IPSec tunnel can be built up again

18. [BUG FIX] 090820772

Symptom:

External group user cannot work

Condition:

1. Add a external group type user
2. Relate the external group user to AD server
3. Add the AD server object to the default Auth Method
4. Login DUT from GUI with the external group user
5. Browser shows Internal Server Error

19. [BUG FIX] 090820784

Symptom:

Test external group user will always fail

Condition:

1. Add an external group user
2. Test this external group user in Configuration Validation will always fail

20. [BUG FIX] 090820819

Symptom:

Modem common comand " & " can't be saved in Initial String.

Condition:

1. Edit Configuration > Network > Interface > Auxiliary, Initial String= AT&F!0m0,

Apply

2. Check Configuration > Network > Interface > Auxiliary, Initial String= AT

21. [BUG FIX] 090820940

Symptom:

If the checking failure message includes “”, the web page cannot be opened successfully when EPS check failed

## Features:

---

Modifications in 2.20(AQW.0)b1 - 2009/08/17

1. [ENHANCEMENT]  
ZLD Packet Flow 2.0
2. [ENHANCEMENT]  
Web GUI 2.0
3. [ENHANCEMENT]  
SSLVPN Portal for Web GUI 2.0
4. [ENHANCEMENT]  
Customized Log Page for Web GUI 2.0
5. [ENHANCEMENT]  
Object Reference Query
6. [ENHANCEMENT]  
SIP ALG 1.2
7. [ENHANCEMENT]  
Disable According Policy Route Rule while Interface Link Down or Ping Check Failed
8. [ENHANCEMENT]  
Block non-SNATed Packet by Firewall
9. [ENHANCEMENT]  
Device DNS Query Bind with Specific Interface
10. [ENHANCEMENT]  
Unified Interface Enhancement
11. [ENHANCEMENT]  
Packet Capture using GUI
12. [ENHANCEMENT]  
Cellular Budget Support
13. [ENHANCEMENT]  
Device HA Bridge Interface Support
14. [ENHANCEMENT]  
Device HA Easy Configuration for VLAN Interface
15. [ENHANCEMENT]  
Bypass Content Filter for VPN Traffic
16. [ENHANCEMENT]  
RIP & OSPF VLAN Interface Support
17. [ENHANCEMENT]  
MSN Login/Logout Log Support

- 18. [ENHANCEMENT]  
EPS (End Point Security)
- 19. [ENHANCEMENT]  
Authentication Policy
- 20. [ENHANCEMENT]  
IPSec Fall Back Support
- 21. [ENHANCEMENT]  
AAA Enhancement for External Group User
- 22. [FEATURE CHANGE]  
MAX VLAN Number reduced from 512 to 256

## Appendix 1. Firmware upgrade / downgrade procedure

The following is the firmware **upgrade** procedure:

1. If user did not backup the configuration file before firmware upgrade, please follow the procedures below:
  - Use Browser to login into ZyWALL as administrator.
  - Click Maintenance > File Manager > Configuration File to open the Configuration File screen. Use the Configuration File screen to backup current configuration file.
  - Find firmware at [www.zyxel.com](http://www.zyxel.com) in a file that (usually) uses the system model name with the .bin extension, for example, “210AQW0C0.bin”.
  - Click Maintenance > File Manager > Firmware Package to open the Firmware Package screen. Browser to the location of firmware package and then click Upload. The ZyWALL automatically reboots after a successful upload.
  - After several minutes, the system is successfully upgraded to newest version.

The following is the firmware **downgrade** procedure:

1. If user has already backup the configuration file before firmware upgrade, please follow the procedures below:
  - Use Console/Telnet /SSH to login into ZyWALL.
  - Router>**enable**
  - Router#**configure terminal**
  - Router(config)#**setenv-startup stop-on-error off**
  - Router(config)#**write**
  - Load the older firmware to ZyWALL using standard firmware upload procedure.
  - After system uploads and boot-up successfully, login into ZyWALL via GUI.
  - Go to GUI → “File Manager” menu, select the backup configuration filename, for example, statup-config-backup.conf and press “Apply” button.
  - After several minutes, the system is successfully downgraded to older version.
2. If user did not backup the configuration file before firmware upgrade, please follow the procedures below:
  1. Use Console/Telnet /SSH to login into ZyWALL.
  2. Router>**enable**
  3. Router#**configure terminal**
  4. Router(config)#**setenv-startup stop-on-error off**
  5. Router(config)#**write**
  6. Load the older firmware to ZyWALL using standard firmware upload procedure.
  7. After system upload and boot-up successfully, login into ZyWALL via Console/Telnet/SSH.
  8. Router>**enable**
  9. Router#**write**

Now the system is successfully downgraded to older version.

Note: ZyWALL might lose some configuration settings during this downgrade procedure. It is caused by configuration conflict between older and newer firmware version. If this situation happens, user needs to configure these settings again.

## Appendix 2. SNMPv2 private MIBS support

SNMPv2 private MIBs provides user to monitor ZyWALL platform status. If user wants to use this feature, you must prepare the following step:

1. Have ZyWALL mib files (zywall.mib and zyxel-zywall-ZLD-Common.mib ) and install to your MIBs application (like MIB-browser). You can see zywallZLDCommon (OLD is 1.3.6.1.4.1.890.1.6.22).
2. ZyWALL SNMP is enabled.
3. Using your MIBs application connects to ZyWALL.
4. SNMPv2 private MIBs support three kinds of status in ZyWALL:
  - (A) CPU usage: Device CPU loading (%)
  - (B) Memory usage: Device RAM usage (%)
  - (C) VPNIpsecTotalThroughput: The VPN total throughput (Bytes/s), Total means all packets(Tx + Rx) through VPN.

## Appendix 3. Firmware Recovery

In some rare situation, ZyWALL might not boot up successfully after firmware upgrade. The following procedures are the steps to recover firmware to normal condition. Please connect console cable to ZyWALL.

### 1. Restore the Recovery Image

- If one of the following cases occur, you need to restore the “recovery image”

- Booting failed, device show error code while uncompressing “Recovery Image”.

```

DRAM POST: Testing: 262144K
DRAM Test SUCCESS !

Kernel Version: V2.4.27-AQE-2007-07-04 | 2007-10-08 13:19:57
ZLD Version: V2.00(AQE.0)-1 | 2007-10-08 15:14:27

Press any key to enter debug mode within 3 seconds.
.....

Linux/PPC load: console=ttyS0,115200 root=/dev/ram init=zyinit ""
Uncompressing Linux...inflate returned FFFFFFFD
exit
  
```

- Device reboot infinitely.

```

BootModule Version: V1.011 | 2007-03-30 12:22:57
DRAM: Size = 510 Mbytes
DRAM POST: Testing: 522240K OK
DRAM Test SUCCESS !

Kernel Version: V2.4.27-kernel-2007-10-08 | 2007-10-08 10:44:31
ZLD Version: V2.01(XL.0)b1 | 2007-10-08 11:37:52

Press any key to enter debug mode within 3 seconds.
.....

BootModule Version: V1.011 | 2007-03-30 12:22:57
DRAM: Size = 510 Mbytes
DRAM POST: Testing: 522240K OK
DRAM Test SUCCESS !

Kernel Version: V2.4.27-kernel-2007-10-08 | 2007-10-08 10:44:31
ZLD Version: V2.01(XL.0)b1 | 2007-10-08 11:37:52
  
```

- Nothing displays after “Press any key to enter debug mode within 3 seconds.” for more than 1 minute.

```

BootModule Version: V1.011 | 2007-03-30 12:22:57
DRAM: Size = 510 Mbytes
DRAM POST: Testing: 522240K OK
DRAM Test SUCCESS !

Kernel Version: V2.4.27-kernel-2006-08-21 | 2006-08-21 19:54:00
ZLD Version: V1.01(XL.0) | 2006-09-11 17:41:56

Press any key to enter debug mode within 3 seconds.
.....
  
```

- Startup message displays “Invalid Recovery Image”.



```

BootModule Version: V1.012 | 2007-05-10 21:05:27
DRAM: Size = 510 Mbytes
DRAM POST: Testing: 522240K OK
DRAM Test SUCCESS !

Kernel Version: V2.4.27-XL-2007-05-10 | 2007-05-10 02:15:31
ZLD Version: VZW1050_DailyBuild_New_Trunk | 2007-05-10 03:12:49

Press any key to enter debug mode within 3 seconds.
.....

Invalid Recovery Image

ERROR

Enter Debug Mode

>

```

- The message here could be “Invalid Firmware”. However, it is equivalent to “Invalid Recovery Image”.

```

Invalid Firmware!!!

ERROR

```

- Press any key to enter debug mode

```

BootModule Version: V1.011 | 2007-03-30 12:22:57
DRAM: Size = 510 Mbytes
DRAM POST: Testing: 522240K OK
DRAM Test SUCCESS !

Kernel Version: V2.4.27-kernel-2006-08-21 | 2006-08-21 19:54:00
ZLD Version: V1.01(XL.0) | 2006-09-11 17:41:56

Press any key to enter debug mode within 3 seconds.
.....
Enter Debug Mode

> █

```

- Enter atuk. The console prompts warning messages and waiting for the confirmation. Answer ‘Y’ and start to upload “recovery image” via Xmodem.

```

> atuk
This command is for restoring the "recovery image" (xxx.ri).
Use This command only when
1) the console displays "Invalid Recovery Image" or
2) the console freezes at "Press any key to enter debug mode within 3 seconds"
   for more than one minute.

Note:
Please exit this command immediately if you do not need to restore the
"recovery image".

Do you want to start the recovery process (Y/N)? (default N) █

```

- Use the Xmodem feature of terminal emulation software to upload the file.
- Wait for about 3.5 minutes until finishing Xmodem.

```
programming .....
.....
.....
.....
.....
.....
.....
```



- ```
> atkz -f -l 192.168.1.1
```

- ```
> atgo
Booting...
```

```
Building ...
Connect a computer to port 1 and FTP to 192.168.1.1 to upload the new file.
```

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220-=(<*>)=-.: << Welcome to PureFTPd 1.0.11 >> .:.-=<*>=-
220-You are user number 1 of 50 allowed
220-Local time is now 03:21 and the load is 0.00. Server port: 21.
220-Only anonymous FTP is allowed here
220 You will be disconnected after 15 minutes of inactivity.
User <192.168.1.1:<none>>:
230 Anonymous user logged in
ftp> bin
200 TYPE is now 8-bit binary
ftp> put E:\ftproot\ZLD_FW\101XL\101XL0C0\1.01(XL.0)C0.bin
```

```
200 PORT command successful
150 Connecting to port 3675
226-213.7 Mbytes free disk space
226-File successfully transferred
226 1.057 seconds (measured here), 33.06 Mbytes per second
ftp: 36642350 bytes sent in 1.068seconds 34503.15Kbytes/sec.
ftp>
```

- The console session displays “Firmware received” after the FTP file transfer is complete. Then you need to wait while the ZyWALL recovers the firmware (this may take up to 4 minutes).

```
Firmware received ...

[Update Filesystem]
  Updating Code
  ..
```

- The message here might be “ZLD-current received”. Actually, it is equivalent to “Firmware received”.

```
ZLD-current received ...

[Update Filesystem]
  Updating Code
  ..
```

- The console session displays “done” when the firmware recovery is complete. Then the ZyWALL automatically restarts.

```
.....
done

[Update Kernel]
  Extracting Kernel Image
  ..
  done
  Writing Kernel Image ... done
Restarting system.
```

- The username prompt displays after the ZyWALL starts up successfully. The firmware recovery process is now complete and the ZyWALL is ready to use.
- If one of the following cases occurs, you need to do the “firmware recovery process” again. Note that if the process is done several time but the problem remains, please collect all the console logs and send to ZyXEL for further analysis.
  - Refer to Step 1 “Restore the Recovery Image” and if there is similar case, the process must be performed again.
  - One of the following messages appears on console, the process must be performed again.
    - ◆ /bin/sh: /etc/zyxel/conf/ZLDconfig: No such file
    - ◆ Error: no system default config file, system configuration stop!!