



**Firmware Release Note**

**ZyWALL USG 200**

**Release 3.30(AQU.7)C0**

Date: Jan. 13, 2015

Author: Shang Lee

Project Leader: Shang Lee

## Contents

---

<b>Supported Platforms:</b>	<b>4</b>
<b>Versions:</b>	<b>4</b>
<b>Files lists contains in the Release ZIP file</b>	<b>4</b>
<b>Read Me First</b>	<b>6</b>
<b>Design Limitations:</b>	<b>7</b>
Anti-Virus	7
Build in Service	7
Certificate	8
EPS (Endpoint Security)	8
GUI	8
Interface	8
IPSec VPN	9
SSL VPN	9
L2TP VPN	15
User Aware	15
USB Storage	15
IPv6	16
Anti-Spam	16
Content Filter	16
App Patrol	16
<b>Known Issues:</b>	<b>17</b>
SSL VPN	17
Auth Policy	17
EPS	17
IPv6	17
IPSec VPN	18
Policy Route	18
PPPoE	18
<b>Features: 3.30(AQU.7)C0</b>	<b>19</b>
<b>Features: 3.30(AQU.6)C0</b>	<b>23</b>
<b>Features: 3.30(AQU.5)C0</b>	<b>29</b>
<b>Features: 3.30(AQU.4)C0</b>	<b>30</b>
<b>Features: 3.30(AQU.3)C0</b>	<b>31</b>
<b>Features: 3.30(AQU.2)C0</b>	<b>37</b>
<b>Features: 3.30(AQU.1)C0</b>	<b>38</b>
<b>Features: 3.30(AQU.0)C0</b>	<b>39</b>

<b>Appendix 1. Firmware upgrade / downgrade procedure .....</b>	<b>59</b>
<b>Appendix 2. SNMPv2 private MIBS support .....</b>	<b>60</b>
<b>Appendix 3. Firmware Recovery .....</b>	<b>61</b>

## ZyXEL ZyWALL USG 200

### Release 3.30(AQU.7)C0

#### Release Note

---

Date: Jan. 13, 2015

#### Supported Platforms:

---

ZyXEL ZyWALL USG 200

#### Versions:

---

ZLD Version: V3.30(AQU.7) | 2015-01-13 16:31:04

BootModule Version: V1.13 | 12/10/2010 05:20:17

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

---

**File name: 330AQU7C0.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: 330AQU7C0.conf**

Purpose: This ASCII file contains default system configuration commands.

**File name: 330AQU7C0.doc**

Purpose: This release file.

**File name: 330AQU7C0.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: 330AQU7C0-enterprise.mib, 330AQU7C0-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 lan1, which are P2 and P3 ports on the rear panel. The default IP address of lan1 is 192.168.1.1/24.
  - By default, WWW/SSH/SNMP service can only be accessed from LAN subnet.
  - The default WAN interface is wan1. This interface will automatically get IP address using DHCP by default.
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 user upgrades from previous released firmware to this version, there is no need to restore to system default configuration.
4. After upgrade firmware, please remember to clear browser cache to avoid the GUI cache issue.
5. 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.
6. 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.
7. If there is problem to reboot successfully after firmware upgrade, please refer to Appendix 3: Firmware Recovery.
8. Since BWM has been activated in system default configuration, please remember to turn off BWM before you do the performance testing.

## Design Limitations:

---

Note: These design limitations will be removed on next release once it is created into announced knowledge base.

### Anti-Virus

1. [SPR: 070813118]  
[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.
2. [SPR:100408336 ]  
[Symptom] DUT can't detect Virus if the compress file includes virus file and encryption file. And the encryption file is list as first in the compress file. This is our design issue that AV will ignore detection when encounter encryption file.
3. [SPR: 111027822]  
[Symptom] AV black/white list functionality abnormal with special HTTP URL (such as <http://1.1.1.1/download/?command=download&filename=abc.zip>)  
[WORKAROUND] Add wildcard rule “\*abc.zip” to support this case

### Build in Service

1. [SPR: 061208575]  
[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 10443/10444/1723/2601-2604. Users should avoid using these internal ports for built-in services.  
[Workaround] Users should avoid using these internal ports for built-in services.
2. [SPR: 100419981]  
[Symptom] DNS doesn't resolve 2nd level domain name.  
Example:  
System->DNS->Address/PTR Record, add two record  
a) testdomain.com 192.168.10.100  
b) www.testdomain.com 192.168.10.100  
DUT does NOT resolve the testdomain.com

## Certificate

1. [SPR: 080509434]  
[Symptom] Cannot input L (locality name) & ST (state or province name) etc when create a certificate request.

## EPS (Endpoint Security)

1. [SPR: 090805245]  
[Symptom] PC OS is 64 bits. EPS always fail when checking Firewall, Anti-virus and Windows auto update.  
We current not support EPS on Windows 64bit Operation System.

## GUI

1. [SPR: 100914249]  
[Symptom] IE7/8 sometimes shows “Stop running this script? A script on this page is causing Internet Explorer to run slowly. If it continues to run, your computer may become unresponsive.” when configuring device. Please update IE patch:  
<http://support.microsoft.com/kb/175500> for fixing this issue
2. IE7/8 sometimes shows "A script on this page is causing Internet Explorer to run slowly..." when configuring device. Please update IE patch : <http://support.microsoft.com/kb/175500> for fixing this issue
3. [SPR: 110216901]  
[Symptom] When the admin logged in via web interface, the admin will be logged out by clicking the “refresh” button of the browser
4. [SPR: 110512912]  
[Symptom] When there are more than 10000 sessions in DUT, open session monitor page will caused GUI to return ”Device Error” message

## Interface

1. [SPR: 100105242, 100105292]  
[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



## IPSec VPN

1. [SPR: 070814169]  
[Symptom] PKI does not interoperate with Windows CA server, when using SCEP.
2. [SPR: 070814168]  
[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.
3. [SPR: 100429119]  
[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

## SSL VPN

1. [SPR: 091022383]  
[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.

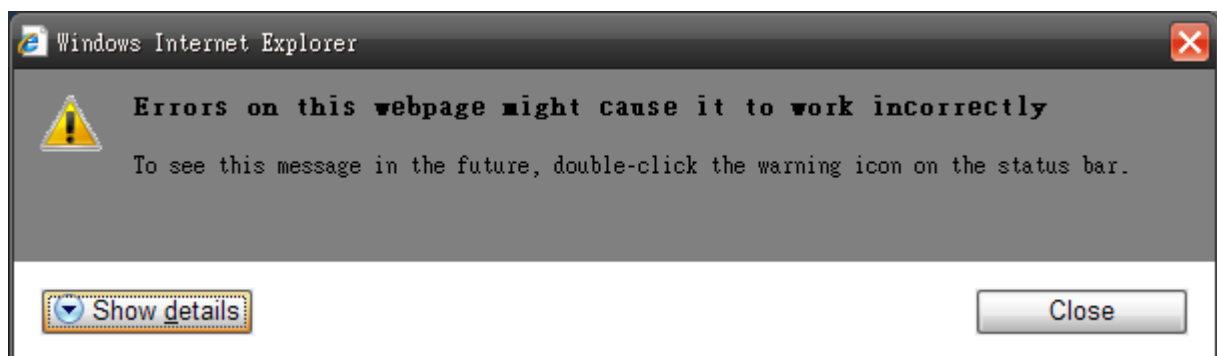
2. [SPR: 091021328]

[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]

[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 encounter JavaScript error.



This problem caused 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)

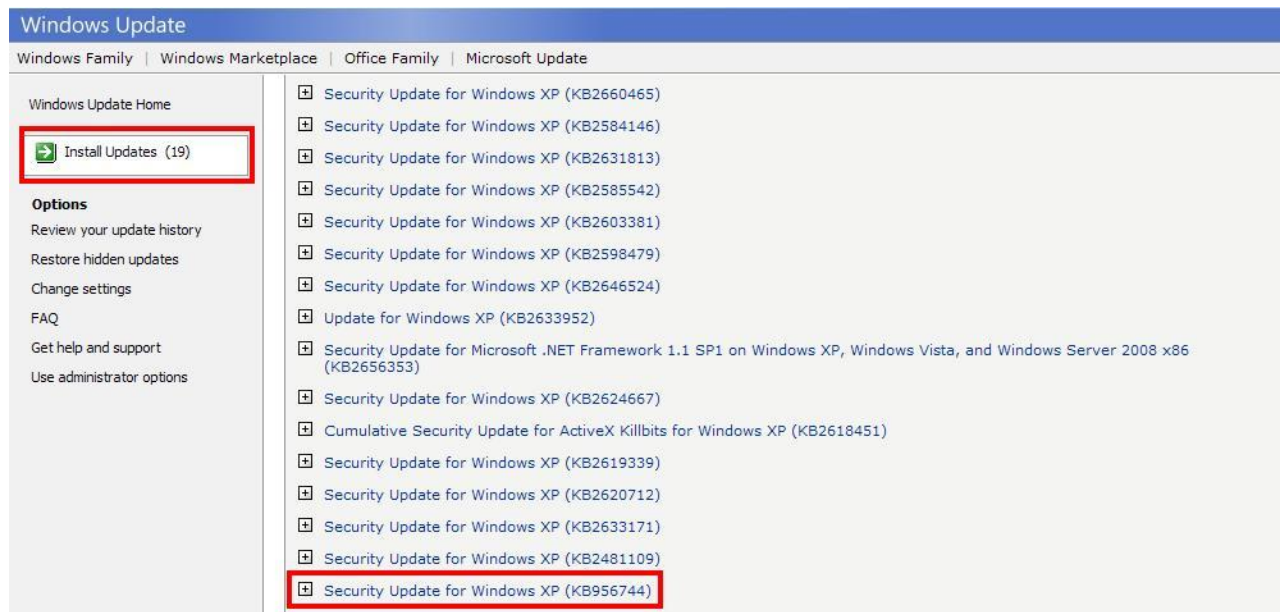
	RDC 5.0	RDC 5.1	RDC 5.2	RDC 6.0	RDC 6.1
Windows Vista RTM	x	x	x	KB956744*	x
Windows Vista SP1 and Windows Vista SP2	x	x	x	x	KB956744*
Windows XP SP2	x	KB958470*	KB958469	KB956744*	KB956744*
Windows XP SP3	x	x	KB958469	x	KB956744*
Windows Server 2003 SP2	x	x	KB958469*	KB956744*	x
Windows 2000 SP4	KB958471*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

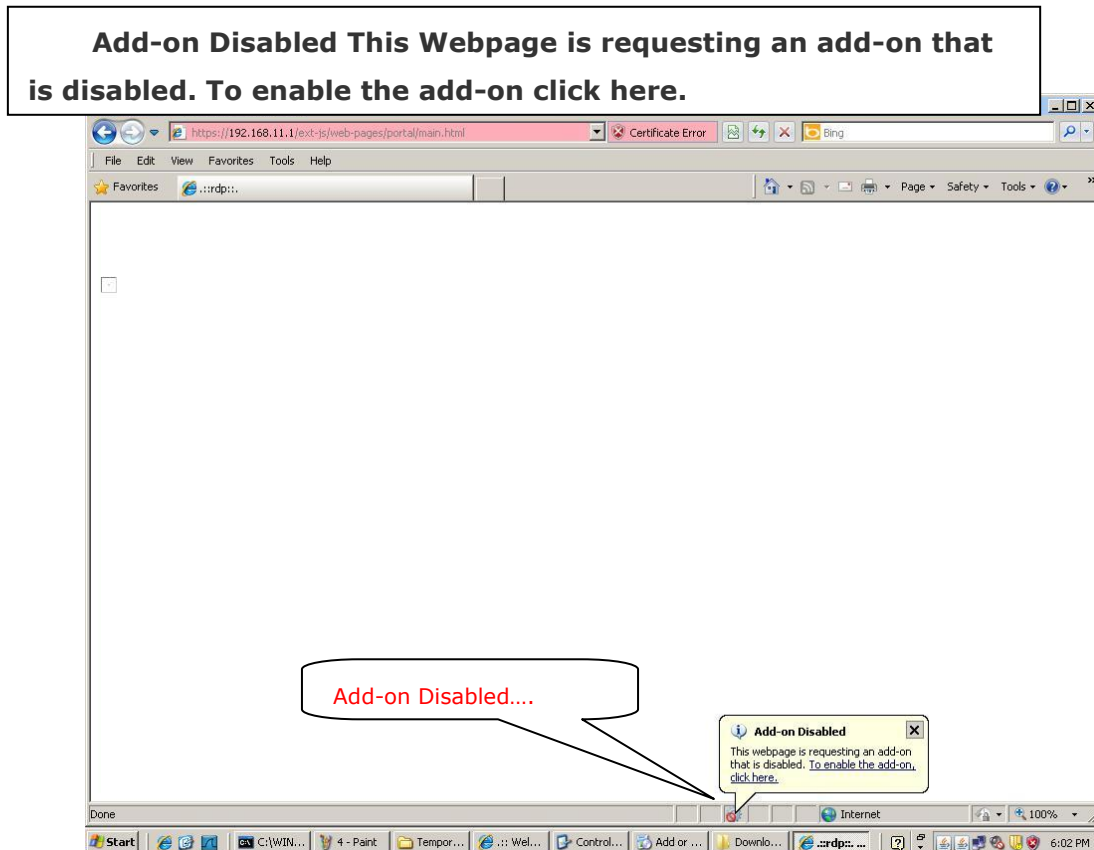
4. [SPR: 100413593]

[Symptom] Can not login remote RDP server via SSLVPN

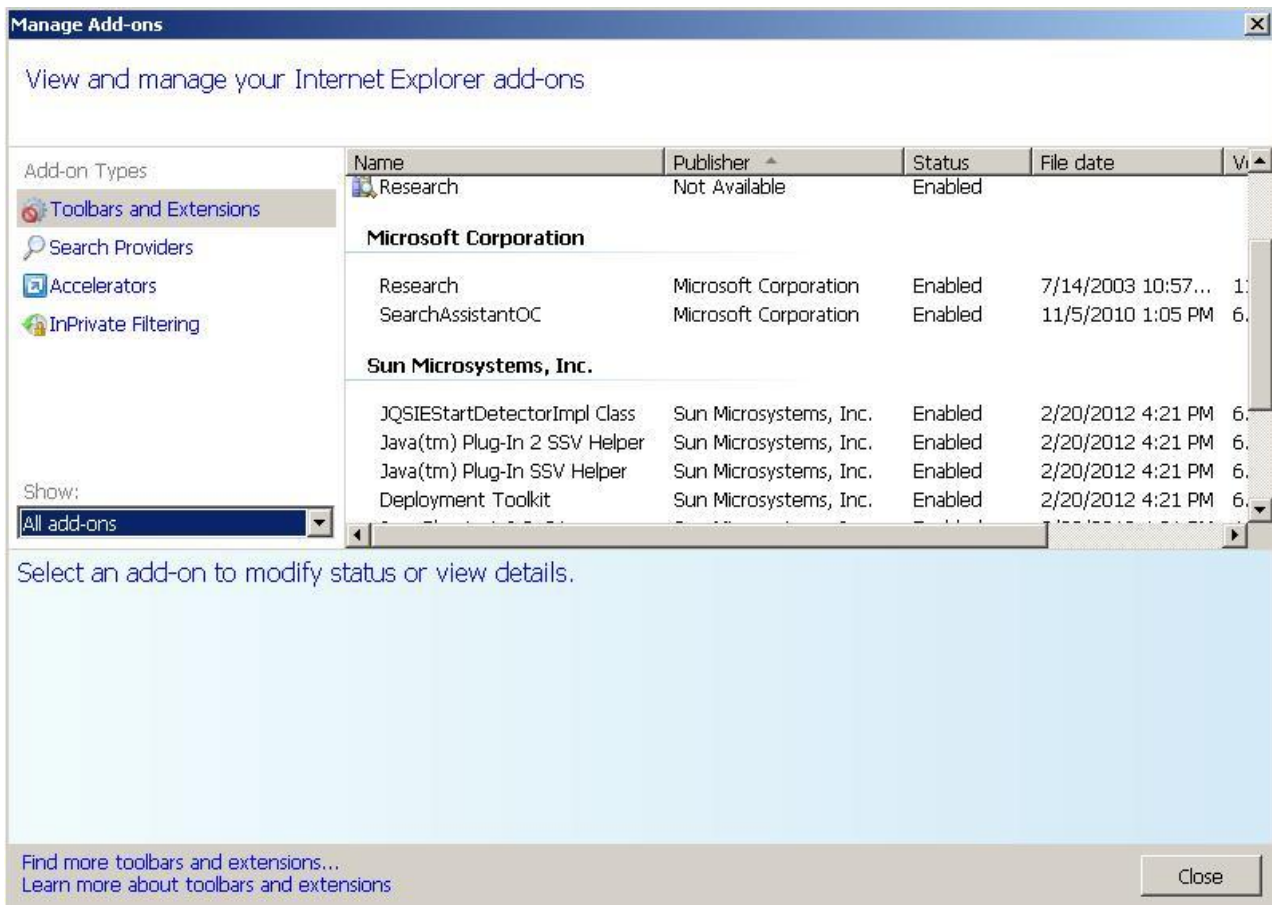
**Microsoft RDP Client Control may not work in IE7/IE8 after WinXP SP3**

To use SSLVPN Portal RDP function, the web page must load the Microsoft RDP Client Control. This ActiveX control must be set to enable, or the function would not work. In IE6, we can find the option in [Tools→Manage Add-ons] and set the option to enable.

After WinXP SP3 Microsoft RDP Client Control is set disable as default value. If user never used the RDP control in IE6 and set to enable. After upgrade to IE7/IE8, user may get the message:



But when click the add-on, The RDP Client Control couldn't be found in Manage Add-ons.



### [Solution]

Microsoft provides the solution to solve this problem in their official support website. User can follow the official to enable the RDP ActiveX control.

<http://support.microsoft.com/kb/951607>

1) Click Start, Run. Type Regedit.exe and press ENTER.

2) Remove the following registry key:

**HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{9059f30f-4eb1-4bd2-9fdc-36f43a218f4a}**

3) Restart Internet Explorer, and try to connect to the RDP application again.

For IE7 user may encounter browser always remind you to install related Active X; this owing to the security policy, you need set the value of Allow previously unused ActiveX controls to run without prompt to Enable. Please see the following step:

a) From the **Tools** menu, click **Internet Options**.

b) On the **Security** tab, select the zone that contains the Web Interface server and click **Custom level**.

c) Set **Allow previously unused ActiveX controls to run without prompt** to enable

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

[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.

Applications Operating System	Full Tunnel Mode	Reverse Proxy Mode	RDP	VNC
		File Sharing(Web-based Application)		
Windows 7 (X64) (SP1) JRE 1.6.x Java 7	Internet Explorer 8.x, 9.x Chrome latest version Firefox latest version Opera latest version	Internet Explorer 8.x, 9.x Chrome latest version Firefox latest version -	Internet Explorer 8.x, 9.x	Internet Explorer 8.x, 9.x Chrome latest version Firefox latest version -
Windows 7 (X32) (SP1) JRE 1.6.x Java 7	Internet Explorer 8.x, 9.x Chrome latest version Opera latest version	Internet Explorer 8.x, 9.x Chrome latest version Firefox latest version	Internet Explorer 8.x, 9.x	Internet Explorer 8.x, 9.x Chrome latest version Firefox latest version
Windows 8 /8.1 (X64) Java 7	Internet Explorer 10.x Chrome latest version Firefox latest version Opera latest version	Internet Explorer 10.x Chrome latest version Firefox latest version	Internet Explorer 10.x	Internet Explorer 10.x Chrome latest version Firefox latest version
Windows 8 / 8.1 (X32) Java 7	Internet Explorer 10.x Chrome latest version Firefox latest version Opera latest version	Internet Explorer 10.x Chrome latest version Firefox latest version	Internet Explorer 10.x	Internet Explorer 10.x Chrome latest version Firefox latest version

6. [SPR: 100419034]

[Symptom] SSLVPN of VNC cannot work if user connects VNC application by FQDN.

7. [SPR: 100427864]

[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"

8. [SPR: 101125986]

[Symptom] Cannot install SecuExtender on IE x86 64-bit.

[Solution] Use Java or 32-bit IE to install SecuExtender

9. [SPR: 110509643]

[Symptom] In SSL-VPN file sharing configure object page, if user tries to preview an unreachable file sharing site, you need to wait for GUI response about 3 ~ 5 minutes.

[WORKAROUND] You can press refresh to cancel the preview action.

10. [Symptom] SSL-VPN file sharing not support NTLMv2 and SMBv2

11. [SPR: 130815220]

[Symptom] The SecuExtender will disconnect automatically around 30 seconds and pop up message "If Windows Incoming Connections already exist or Routing and Remote Access Service is activated, please remove it or deactivate it and retry again" on Windows 8 32bit OS and Windows 8 64bit OS while user's PC has Incoming Connections settings.

[Workaround] Please remove the Incoming Connections settings or deactivate the service of Remote Access Service and login again.

## L2TP VPN

1. [Symptom] L2TP connection will break sometimes with Android device. This issue comes from the L2TP Hollow packet will not be replied by Android system.

## User Aware

1. [SPR: 070813119]

[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.

## USB Storage

1. [SPR: 100708070]

[Symptom] When rename system name, the USB storage can not work.

## IPv6

1. HTTP/HTTPS not support IPv6 link local address in IE7 and IE8.
2. Windows XP default MS-DOS FTP client cannot connection to device's FTP server via IPv6 link-local address.
3. [SPR: 110803280]  
[Symptom] Safari cannot log in web with HTTPS when using IPv6
4. [SPR: 110803293]  
[Symptom] Safari fails to redirect http to https when using IPv6
5. [SPR: 110803301]  
[Symptom] Safari with IPv6 http login when change web to System > WWW, it pop up a logout message. (HTTP redirect to HTTPS must enable)

## Anti-Spam

1. [SPR: 110418626]  
[Symptom] Google DNS server (8.8.8.8) may not answer the DNSBL query.

## Content Filter

1. [SPR: 111028006]  
[Symptom] In CF warning page, the button (exit) cannot work with warning body message in Firefox  
[Workaround] User can take following steps to solve this issue in Firefox.
  - a. Open Firefox and input URL with “about:config”
  - b. Input “dom.allow\_scripts\_to\_close\_windows” as search condition and press enter
  - c. The filtered rule value is false. Double click it to turn it as true.

## App Patrol

1. [SPR: 130613006]  
[Symptom] App Patrol function can't set actions such as block, drop, log.....etc. on the traffic go into DUT. For example, if we set an app patrol rule that is SNMP with log and block action, using a MIB browser to scan DUT will not see any log and it also can scan successfully.
2. [SPR: 130618302]  
[Symptom] Some network access behavior may hit several kinds of applications, for example, if you are using Google Chrome to access Yahoo website, you may hit both Chrome and Yahoo application rules. If you set block Chrome and forward Yahoo traffic, DUT probably will pass the traffic going to Yahoo even using Chrome browsers. The hit decision policy for a multiple match connection would be choosing more specific app rule first.



## Known Issues:

---

Note: These known issues represent current release so far unfixed issues. And we already plan to fix them on the future release.

### SSL VPN

1. [SPR: N/A]

[Symptom] Windows 7 users cannot use SSL cipher suite selection as AES256.

[Workaround] You can configure Windows cipher with following information

<http://support.microsoft.com/kb/980868/en-us>

2. [SPR: 120110586]

[Symptom] Some Win8 PC will pop out Dial-in message after login to SSLVPN.

This is an IOP issue between the function “Force all client traffic to enter SSL VPN tunnel” and Windows8

[Workaround] please change another client PC, if still have the same problem or can't change it, disable the function on USG.

3. [SPR: 131225714]

[Symptom] Login SSLVPN full tunnel mode with Windows 8.1 x 64 clients, when logout SecuExtender will pop out a warning box, “SecuExtender Agent is stopped due to SSL connection closed unexpectedly”. Note: It only has to happen once, i.e. after you install the SecuExtender in your PC, the first time you logout the device via SSL-VPN.

[Workaround] Please re-login the SSL-VPN or change another PC that already exist SecuExtender.

### Auth Policy

1. [SPR: 110804598]

[Symptom] When add an exceptional rule to pass TCP ports range 1024~65535 in force authentication, the client doesn't need to login DUT and can open yahoo or other internet web

### EPS

1. [SPR: 120209992]

[Symptom] EPS rule selects Avira Premium 2009 but use PC with Avira Premium 2010 can pass EPS checking

2. [SPR: 120209000]

[Symptom] EPS rule selects Norton Internet Security 2011 but use PC with Norton Internet Security 2010 can pass EPS checking

### IPv6

1. [SPR: 130423291]

[Symptom] All IPv6 Features with user aware can't work now.

## **IPSec VPN**

1. [SPR: 120110586]

[Symptom] When set IPSec VPN with certificate and enable x.509 with LDAP, the VPN session must dial over two times and the session will connect successful

## **Policy Route**

1. [SPR: 140919787]

[Symptom] IPv6 Policy Route cannot work well while choosing 6in4 or 6to4 tunnel as next hop interface.

## **PPPoE**

1. [SPR: 140916598]

[Symptom] PPPoE account name has grave accent (`) character will cause PPP interface create failed

## Features: 3.30(AQU.7)C0

---

### Modifications in 3.30(AQU.7)C0

#### 1. [ENHANCEMENT] eITS# 140701132, SPR: N/A

Add SNMP VPN status and connection counter MIBs.

The VPN status MIB is a MIB table containing the following information:

Connection name, VPN gateway, IP version, active status, and connected status.

The VPN connection counter is a MIB group containing:

Total VPN connection configured, number of activated connection, number of connected connection, and number disconnected connection.

Followings are the example of snmpwalk for the added MIBs;

VPN status MIB table:

1.3.6.1.4.1.890.1.6.22.2.4.1.1.1 = INTEGER: 1 --> table index

1.3.6.1.4.1.890.1.6.22.2.4.1.1.2 = INTEGER: 2

1.3.6.1.4.1.890.1.6.22.2.4.1.1.3 = INTEGER: 3

1.3.6.1.4.1.890.1.6.22.2.4.1.2.1 = STRING: "vpnconn1" --> name

1.3.6.1.4.1.890.1.6.22.2.4.1.2.2 = STRING: "vpnconn2"

1.3.6.1.4.1.890.1.6.22.2.4.1.2.3 = STRING: "vpn6conn1"

1.3.6.1.4.1.890.1.6.22.2.4.1.3.1 = STRING: "usg110\_1" --> gateway

1.3.6.1.4.1.890.1.6.22.2.4.1.3.2 = STRING: "usg110\_1"

1.3.6.1.4.1.890.1.6.22.2.4.1.3.3 = STRING: "vpn6\_1"

1.3.6.1.4.1.890.1.6.22.2.4.1.4.1 = STRING: "IPv4" --> IP version

1.3.6.1.4.1.890.1.6.22.2.4.1.4.2 = STRING: "IPv4"

1.3.6.1.4.1.890.1.6.22.2.4.1.4.3 = STRING: "IPv6"

1.3.6.1.4.1.890.1.6.22.2.4.1.5.1 = INTEGER: 0 --> active status

1.3.6.1.4.1.890.1.6.22.2.4.1.5.2 = INTEGER: 1

1.3.6.1.4.1.890.1.6.22.2.4.1.5.3 = INTEGER: 1

1.3.6.1.4.1.890.1.6.22.2.4.1.6.1 = INTEGER: 0 --> connected status

1.3.6.1.4.1.890.1.6.22.2.4.1.6.2 = INTEGER: 0

1.3.6.1.4.1.890.1.6.22.2.4.1.6.3 = INTEGER: 0

VPN connection counters:

1.3.6.1.4.1.890.1.6.22.2.5.1.0 = Counter32: 3 --> total connection configured

1.3.6.1.4.1.890.1.6.22.2.5.2.0 = Counter32: 2 --> number of active connection

1.3.6.1.4.1.890.1.6.22.2.5.3.0 = Counter32: 0 --> number of connected connection

1.3.6.1.4.1.890.1.6.22.2.5.4.0 = Counter32: 2 --> number of disconnected connection

The number of disconnected connection is equal to the number of active connection minus the number of connected connection L2TP over IPsec cannot support authentication via Windows AD 2012.

2. [ENHANCEMENT] eITS# N/A, SPR: N/A  
Default turn off SSLv3 Support in Built-in Service. Using CLI “ip http secure-server sslv3” to turn on it.
3. [ENHANCEMENT] eITS# N/A, SPR: N/A  
Update the bash binary to fix BASH Vulnerability issue, CVE-2014-6271 (original shellshock), CVE-2014-7169 (taviso bug), CVE-2014-7186 (redir\_stack bug), CVE-2014-7187 (nested loops off by one), CVE-2014-6277 (lcamtuf bug #1), and CVE-2014-6278 (lcamtuf bug #2).
4. [ENHANCEMENT] eITS# 140900236, SPR: N/A  
Show IPsec debug message to SSH.
5. [ENHANCEMENT] eITS# 141100664, SPR: N/A  
PKI support import certificate with SHA384 and 512 hash algorithm.
6. [ENHANCEMENT] eITS# 141100032, SPR: N/A  
Support "space" for certificate in the following field: Organizational Unit, Organization, Town, State (Province), Country.
7. [ENHANCEMENT] eITS# 141000443, SPR: N/A  
The session will be automatically disconnected (Firewall rule takes effect immediately) when reaching the schedule.
8. [ENHANCEMENT] eITS# 141100097, SPR: N/A  
Enhance IPsec Authentication with certificate to validate X509v1 CA certificate.
9. [ENHANCEMENT] eITS# 140800581, SPR: N/A  
Add CLI command 'app-watch-dog mem-drop-cache-threshold XX', where XX is in the range 50..90, to configure app watchdog to inform kernel to drop caches in order to free more memory when memory usage exceeds the threshold.
10. [ENHANCEMENT] eITS# 141100648, SPR: N/A  
Diagnostic info enhancement.
11. [ENHANCEMENT] eITS# 140800119, SPR: N/A  
Enlarge the value of nf\_ct\_expect\_max to avoid SIP packets from dropping.
12. [FEATURE][CHANGE] eITS# 141000032, SPR: N/A  
Description: Modify usg100-plus maximum disk threshold  
WAS: maximum disk threshold was 95%  
IS: maximum disk threshold is 99%.
13. [BUGFIX] eITS# 120600947, 140900338, SPR: N/A  
Symptom:  
IPsec sshipsecpm daemon is dead. The issue is usually happened while VPN failover and fallback is triggered.
14. [BUGFIX] eITS# 141000155, SPR: N/A  
Symptom:

IKE packet sent from wrong interface and wrong IP.

15. [BUGFIX] eITS#140900251, SPR: 140922847

Symptom:

[File Manager] rename configuration file to 64 characters will fail.

16. [BUGFIX] eITS# 140900380, SPR: N/A

Symptom:

L2TP can't login user and with crazy log message.

17. [BUGFIX] eITS# 141000460, 141000461, 141000462, SPR: N/A

Symptom:

Static ARP entry will disappear if enabling device HA.

18. [BUGFIX] eITS# 140800642, SPR: 140714684, 140804120, 141103007

Symptom:

VPN connect fail and hang.

19. [BUGFIX] eITS# 141001045, SPR: N/A

Symptom:

It shows incorrect expiration date of licenses on GUI.

20. [BUGFIX] eITS# 141000951, SPR: N/A

Symptom:

When using SHA256 as intermediate certificate, the certificate path shows "incomplete path".

21. [BUGFIX] eITS# 141100282, SPR: N/A

Symptom:

CPU high issue caused by CCD daemon on 3.30 patch6.

22. [BUGFIX] eITS# 141100177, SPR: N/A

Symptom:

Fix IPsec VPN IOP issue with FortiGate: VPN cannot build after rekeying.

23. [BUGFIX] eITS# 141200132, SPR: 141229525

Symptom:

[GUI] The DHCP pool size didn't update immediately after changing the IP / subnet mask setting.

24. [BUGFIX] eITS# 141200336, SPR: 141216860

Symptom:

DynDNS DNS update fail if the password length is longer than 31 digitals.

25. [BUGFIX] eITS# 141100945, SPR: N/A

Symptom:

Device HA fails to synchronize backup device with master device if master configuration has CLI command "client-side-vpn-failover-fallback activate".

26. [BUGFIX] eITS# 141100552, SPR: N/A

Symptom:

IDP signature cannot be updated in China.

27. [BUGFIX] eITS# 141000415, SPR: 141211698

Symptom:

Traffic cannot pass through VPN tunnel while fallback to primary gateway.

28. [BUGFIX] eITS# 140800486, SPR: N/A

Symptom:

DDNS profile doesn't allow username with leading numbers such as "266oSx-vam" but in real case DynDNS server allow this kind of username to register.

## Features: 3.30(AQU.6)C0

---

### Modifications in 3.30(AQU.6)C0

1. [ENHANCEMENT] eITS# 140103540, SPR: 140205030  
L2TP over IPsec cannot support authentication via Windows AD 2012.
2. [ENHANCEMENT] eITS# 140500409, SPR: 1405201712  
Let Port 1 in system log messages represent P1 on the dashboard, Port 2 in log message represent to P2 on the dashboard, and so on.
3. [BUGFIX] eITS# 131202199 , SPR: 1401241253  
Symptom:  
When customer choose option as “GPRS/EDGE (GSM) only”, but they using Monitor on device, still stay in WCDMA.
4. [BUGFIX] eITS# 140101349 , SPR: 140220557  
Symptom:  
SSL VPN Full tunnel mode does not work. It will show the error message, “SecuExtender Agent is stopped due to internal error”.
5. [BUGFIX] eITS# 130902058 , SPR: 1401231174  
Symptom:  
The device has hang issue.  
Condition:  
IPsec daemon causes CPU high and let the device no response.
6. [BUG FIX] eITS# 140103025 , SPR: 1401281429  
Symptom:  
USG cannot change default password after first set up.  
Condition:  
USG in defaults, customer log in and change password to different one based WEB GUI request, this new password work fine but USG save it only in running configuration and not to startup config, and after switch off/on or reboot USG it will back to original password.
7. [BUG FIX] eITS# 140104045 , SPR: 140210113  
Symptom:  
DDNS provider ”NO-IP” have changed URL format will cause negotiation behavior failed.
8. [BUG FIX] eITS# 140201672 , SPR: 140214325  
Symptom:  
When add new VLAN interface and fill in necessary fields, the OK button cannot be click.
9. [BUG FIX] eITS# 140103024, SPR: 1401291457  
Symptom:

At USG20 & USG20W, when PPPOE interface disconnect and re-connect, the log message displays an error message "alter System App Watchdog reach 97%"

10. [BUGFIX] eITS# 140200748 , SPR: 140219483

Symptom:

The customer usually gets the message "Cannot create Tap routing interface. Please logout and retry again." after SSL VPN is logged in.

11. [BUGFIX] eITS# 140201667 , SPR: 140604061

Symptom:

PCI Compliance failed in the following case:

**Apache HTTP Server http Only Cookie Information Disclosure www (443/tcp) CVE-2012-0053**

Symptom:

When enable CF service and download file from internet. The download speed is decreased with 0K ~ 32K. Before enable the service, the download speed can reach around 2000KB

12. [BUGFIX] eITS# 140203512 , SPR: 1403261035

Symptom:

Customer daily reports on mail message can't sync with real license status.

13. [BUGFIX] eITS# 140203590 , SPR: 140312365

Symptom:

The customer gets the error message "show open file fail!" on USG100-PLUS after a while (around 10 minutes) when he is logged on to the dashboard.

14. [BUGFIX] eITS# 140204106 , SPR: 140314501

Symptom:

The ZAV & KAV signature version does not display in dashboard properly.

15. [BUGFIX] eITS# 140203489 , SPR: 140310265

Symptom:

Static IP address on ZLD 3.30 Device-HA legacy mode will be 0.0.0.0, and the LAN traffic cannot go out.

16. [BUGFIX] eITS# 140300657 , SPR: 140324875

Symptom:

When using wizard to create a new VPN policy, there is a risk of overwriting and old address object if it has the same policy name as the new policy.

17. [BUGFIX] eITS# 140201212 , SPR: 140320783

Symptom:

Issue 1:

1 Create an IPv6 Subnet Object, e.g. "Crash\_Test\_Subnet" = fe80::/101.

2 Create an IPv6 Address Group, e.g. "Crash\_Test\_Group" and have the above Subnet as part of the group1.



3 modify the prefix of IPv6 Subnet Object "Crash\_Test\_Subnet" to fe80::/64 When clicking OK, the Zysh will die/hang.

Issue 2: Incorrect firewall filtering, step same as issue 1,

A firewall rule includes IPv6 subnet object and change this object's prefix, before the change, ping traffic from LAN to WAN is fine. After changing, the ping will be failure.

18. [BUGFIX] eITS# 131102290 , SPR: 131203072

Symptom:

Customer's USG2000 is sometimes at high memory usage.

19. [BUGFIX] eITS# 140302321, SPR: 1404231176

Symptom:

Customer configuration file at Policy BWM #127 becomes default due to reach maximum policy rule

20. [BUGFIX] eITS# 140302055, SPR: 140416756

Symptom:

When booting the device, the registration page should change to myzyxel.com 2.0 even the internet connection is fail.

21. [BUGFIX] eITS# 140302259, SPR: 140414636

Symptom:

When IPv6 firewall activate, the firewall function blocks traffic even the source IP is not defined in the firewall rule.

22. [BUG FIX] eITS# 140301445, SPR: 140414632

Symptom:

When enabled Anti-Spam function. The mail with big attach files (3MB); the client can't receive the mail success.

23. [BUGFIX] eITS# 140300757 , SPR: 1404301886

Symptom:

In German language platform, the main login page 4th note does not translate.

24. [BUGFIX] eITS# 140400393 , SPR: 1404221138

Symptom:

Use the customer's configuration, and change the Auth Policy rule 1 to unnecessary. After rebooting, the rule will revert back to force.

25. [BUG FIX] eITS# 140201613 , SPR: 1404241321

Symptom:

The L2TP tunnel goes up without any issues and traffic can be sent via the VPN tunnel. After approximately 1 minute to 60 minutes the L2TP VPN tunnel suddenly goes down.

26. [BUG FIX] eITS# 140300566 , SPR: 140409386

Symptom:

When connecting through RDP by SSL VPN and then surfing the Internet, the user loses connection to RDP machine.

27. [BUG FIX] eITS# 140400954 , SPR: 1404221160

Symptom:

When enable Content Filter function, it will pop out the error message, and cause the internet disconnection.

28. [BUG FIX] eITS# 140400954, SPR: 1405131004

Symptom:

Dhcpd causes CPU high.

29. [BUG FIX] eITS# 140302644, SPR: 140506301

Symptom:

Daily-report does not work as well.

30. [BUG FIX] eITS# 140400564, SPR: 1405191638

Symptom:

Customer needs SSL Server address can be sorted by alphabetical order from A to Z.

31. [BUG FIX] eITS# 140500164, SPR: 140513944

Symptom:

Username over 30 characters cannot login SSLVPN after device's firmware upgrading from 3.00 patch2 to 3.30 patch4.

32. [BUG FIX] eITS# 140500365, SPR: 1405272032

Symptom:

No SNMP information.

Condition:

This can duplicate by "iReasoning MIB Browser" to setting maximum MAX Repetitions value and sending with getBulk.

33. [BUG FIX] eITS# 140302499, SPR: 1404231170

Symptom:

The error message "Error Number: -18000 Error Message: Internal database error!" pops up on the GUI.

34. [BUG FIX] eITS# 140500238, SPR: 140605149

Symptom:

When sending the daily report email, the email is sent with the value "localhost" under the EHLO packet. The customer wants to know if it is possible to change this value to a FQDN or an IP.

Condition:

According to the customer's feedback, he cannot receive any Email if EHLO value is localhost. He also mentioned that the localhost value is normally used by spammers.

35. [BUG FIX] eITS# 140500954, SPR: 140613506

Symptom:

When enable anti-spam function, the mail subject including \r\n will be cut.

36. [BUG FIX] eITS# 140500193, SPR: 1405231879

Symptom:

3G card U760 cannot work.

37. [BUG FIX] eITS# 140600349, SPR: 140702050

Symptom:

Device upgrade firmware from 3.0 to 3.3 will cause Content Filter engine keep in unselect status.

38. [BUG FIX] eITS# 140600427, SPR: 140714690

Symptom:

After enabling Anti-Virus, the CPU will be high.

39. [BUG FIX] eITS# 1406261273, SPR: 1406261273

Symptom:

DUT cannot synchronize with myzyxel.com 2.0 with error message “device is synchronizing now”

40. [BUG FIX] eITS# 140600333, SPR: 140710641

Symptom:

If WAN interface was set to down via connectivity-check for around 15~30 minutes, after the WAN interface is up, the traffic will not pass through this interface unless I do some change in the WAN trunk.

Condition:

Reproduce steps.1. Confirm both WAN1 and WAN2 interface is up. 2. Let the WAN2 interface be dead via connectivity-check fail. 3. Wait around 15~30 minutes. Let the WAN2 interface is up via connectivity-check. 4. All traffic will pass through WAN1, not WAN2. The WAN2 only got the traffic as WAN connectivity-check.

41. [BUG FIX] eITS# 140600040, SPR: 1407291192

Symptom:

Device reboots when Anti-Spam on

Condition:

- 1) Sometimes device crashes when anti-spam is processing the mail subject name.
- 2) A possible deadlock in kernel when device try to do TCP MSS adjustment on local out traffic.

42. [BUG FIX] eITS# 140701233, SPR: 1407311342

Symptom:

Bridge interface includes two interfaces ”vlan6” and ”Zydmz\_p2” and all DHCP offer only comes on ”Zydms\_p2” (physical interface) Bridge interface cannot get IP address successfully but after reboot USG one or more times, bridge interface gets IP address.

43. [BUG FIX] eITS# 140800030, SPR: 1408291057

Symptom:

log message shows an error "Detect unexpected WLAN problem"

## Features: 3.30(AQU.5)C0

---

### Modifications in 3.30(AQU.5)C0

1. [BUG FIX] eITS#140400954, 140401175 SPR#: N/A

Symptom: Content filter cannot work correctly

Condition:

- a. Add a new domain zone forwarder to customer DNS server 195.175.39.40.
- b. Enable CF and with Bluecoat service.
- c. All http traffic cannot pass through device.

2. [BUG FIX] eITS#140200748, SPR#: N/A

Symptom: Cannot access device

Condition:

- a. Go to MAINTENANCE → Diagnostics → Diagnostics
- b. Press “Collect Now” button
- c. After a while, Zysh daemon is dead. Cannot access device anymore but traffic can pass through.

## Features: 3.30(AQU.4)C0

---

Modifications in 3.30(AQU.4)C0

1. [FEATURE][CHANGE]

Change Commtouch URL link to check category on CF configuration and block page.

2. [BUG FIX] eITS# 140102361, SPR: N/A

Symptom:

Apply configuration failed after reboot.

Condition:

Add CF Commtouch service profile and activate. Save and reboot, device will apply configure fail.

## Features: 3.30(AQU.3)C0

---

### Modifications in 3.30(AQU.3)C0

1. [ENHANCEMENT]

SSLVPN agent 3.0.16 to support Windows 8.1.

2. [BUG FIX] SPR: 131204318, 131206558, 131206567

Symptom: Cannot switch AV and CF engine even valid license exist.

Condition:

(1) Once ZAV expired, device cannot use KAV engine even KAV license is valid.

(2) Once BCCF expired, device cannot use CTCF engine even CTCF license is valid.

3. [BUG FIX] eITS# 131005908, SPR: 1311201126

Symptom:

FW 3.30 cannot achieve same performance as FW 3.00

Condition:

In 3.30 patch 2 firmware, enabling BWM will cause HTTP throughput lower than 3.00.

4. [BUG FIX] eITS# 131100133, SPR: 1312171095

Symptom:

Dynu premium not working

Condition:

In Dynu Premium setting of DDNS, the warning note should hind in user name check box.

5. [BUG FIX] eITS# 131002462, SPR: 1312171094

Symptom:

CPU high when deleting several phase 1 or phase 2 VPN rules.

Condition:

The customer's concern is if delete few IPSec rules (phase 1 or phase 2), the device will not response any more.

6. [BUG FIX] eITS# 130701485, SPR: 1307221709

Symptom:

SNMP Status

Condition:

Link state and speed appears to be wrong on SNMP.

7. [BUG FIX] eITS# 130801770, SPR: 1308303581

Symptom:

HA Backup FW 99% CPU

Condition:

HA backup CPU will rise to 99%

8. [BUG FIX] eITS# 130802428, SPR: 130903138

Symptom:

HA synch. Does not work

Condition:

We add an enhancement that Device-HA sync will include IDP customize signature.

9. [BUG FIX] eITS# 130803743, SPR: 130903152

Symptom:

USG-20W / NAT can't work to Server with BR1 WIFI

Condition:

USG will not save the MAC address.

10. [BUG FIX] eITS# 130905885, SPR: 131004288

Symptom:

USG 300 and alerts

Condition:

Customer concern that there is not needed in HA "alert" that "Version for Certificates is the same, skip update"; this can be ok like log.

11. [BUG FIX] eITS# 131001353, SPR: 131001353

Symptom:

USG 3.30 / Dynu DDNS cannot work as with .net

Condition:

Dynu DDNS cannot work as with .net

12. [BUG FIX] eITS# 131004038, SPR: 131106304

Symptom:

USG FW 3.30 (Patch 1) ESP fragmentation

Condition:

When packet size larger than MTU value, the Don't Fragment bit of ESP packet is still setup on and then USG gets a "destination unreachable (Fragmentation needed)" from WAN's gateway.

13. [BUG FIX] eITS# 130900205, SPR: 130904308

Symptom:

Https management on port 10444

Condition:

The customer change the HTTPs port as 10444, then the GUI can't open any more.

14. [BUG FIX] eITS# 131003539, SPR: 1311281673

Symptom:

Content Filter - Incorrectly displayed Deny message in Windows 7

Condition:

If there is configured Content filtering HTTP Web Category Filtering and users issues denied Web Page, in Internet Explorer is not correctly displayed Denied Access Message



which is configured on USG, and only displays "Page cannot be displayed" which not the Denied Access Message.

15. [BUG FIX] eITS# 131102290, SPR: 131203072

Symptom:

USG 2000 - Memory/CPU usage

Condition:

Customer's USG2000 is very often at very high memory usage, at the moment 96%.

There is no command to show the details of the memory usage.

We add a new CLI command "debug system drop-caches" to drop the inactive memory.

16. [BUG FIX] eITS# 131103596, SPR: 131204321

Symptom:

BWM doesn't work ok

Condition:

When set up BWM: Incoming Interface: lan1; Outgoing Interface: wan1;

Inbound/Outbound: 512kbps, But only download Bandwidth can be controlled as speedtest result (0.55Mbps/13.42Mbps).

17. [BUG FIX] eITS# 131005943, SPR: 131111615

Symptom:

USG 100 and daily logs

Condition:

Email Daily Report logs graphs are empty.

18. [BUG FIX] eITS# 131102399, SPR: 131202059

Symptom:

Problems with port statistics

Condition:

1. When PC1 is connected to USG port2 we have normal port statistics (graphic and grid).

2. When we connect PC2 to the port3 the statistics for port2 still appears but the graphic for port3 doesn't work.

Tx B/s and Rx B/s still= 0 for port3 (as attached "pic-1") even if we are sure the traffic from PC2 currently exists.

After reboot of USG the statistics shows for both ports in normal way.

19. [BUG FIX] eITS# 131006197, SPR: 131107446

Symptom:

Copyright information of DUT shows 1995 -2007...

Condition:

When DUT sends Daily report, ending of daily report information, there is a sentence makes customer feel bad.

20. [BUG FIX] eITS# 131004935, SPR: 1311271491

Symptom:

Request for SOP

Condition:

The customer used Win8.1 to establish the SSL full tunnel mode. And enabled “Force all client traffic to enter SSL VPN tunnel” function, but it seems not work.

21. [BUG FIX] eITS# 131100618, SPR: 131209614

Symptom:

Change Device-HA setting cause WEB GUI timeout after enabling this function

Condition:

We have to wait the WEB GUI back if adding monitor interface after enabling Device-HA.

22. [BUG FIX] eITS# 131005922, SPR: 131105256

Symptom:

[USG 100] AD Alternative Login Attribute

Condition:

AD Alternative Login Name Attribute can't work on firmware 3.30, it works on firmware 3.00.

23. [BUG FIX] eITS# 130905233, SPR: 131104173

Symptom:

USG-2000 / WK27 and WK33 crash by boot progress or first tunnel established

Condition:

Device HA is disabled on both devices before upgrading to debug FW WK37.

After FW upgrading, the Zysh daemon dead.

After removing the configuration of device HA then uploading the revised configuration to the device, it works and is back to normal.

24. [BUG FIX] eITS# 131000402, SPR: 131000402

Symptom:

USG 300 some config are missing

Condition:

Some configurations such as IP MAC binding and content filtering policy can't be completely uploaded to device after the attached configuration file is applied.

25. [BUG FIX] eITS# 130401361, SPR: n/a

Symptom:

Sometimes device will reboot.

Condition:

(1) It only happens in customer environment, it's related to bridge traffic to cause device crash, we found the invalid skb buffer all are multicast packets.

(2) Sometimes, in customer environment, device will reboot.

26. [BUG FIX] eITS# 130802620, SPR: n/a

Symptom:

USG300 Online Helps has wrong description in Content filter.

Condition:

The description for “Forbidden Web Sites” is incorrect in the online help.

It should be \*bad-site.com, not bad-site.com.

27. [BUG FIX] eITS# 130103364, SPR: n/a

Symptom:

[AIM SOFTWARE] USG-1000 / SNMP with High Ping/CPU and Throughput Issue

Condition:

SNMP will occupy CPU resource.

28. [BUG FIX] eITS# 131100487, SPR: n/a

Symptom:

IOP issue between USG 20/100/200 and ZyWALL 110 Ethernet WAN port and Genexis FiberXport OCG-1012m\_v1.

Condition:

If we connect USG WAN port to Genexis FiberXport OCG-1012m\_v1, USG can't get WAN IP. If we setup a switch between USG WAN port and Genexis FiberXport OCG-1012m\_v1, then USG can get WAN IP.

29. [BUG FIX] eITS# 130803915, SPR: n/a

Symptom:

Traffic will be dropped randomly

Condition:

The traffic of server 192.168.10.5 will be dropped by the firewall rule randomly. The customer needs to reboot the USG to recover it.

30. [BUG FIX] eITS# 131005078, SPR: n/a

Symptom:

USG200 Problems with WAN1 when setup connectivity-check

Condition:

WAN1 is DHCP client role and configured connectivity-check for its gateway. From syslog, it shows WAN1 is set to DEAD frequently without reason.

31. [BUG FIX] eITS# 131003516, SPR: n/a

Symptom:

On FW 3.30, ADP does not detect and prevent portscan attack.

Condition:

Affected model: USG20/20W.

Feature ADP need the files in idp\_def\_db.tar.bz2, but we add compiler flag to mark these related action as comments for USG20/20W

33. [BUG FIX] eITS# 130704361, SPR: n/a

Symptom:

ADP log problem

Condition:

The source address of ADP log will be the IP address which is after NAT.

## Features: 3.30(AQU.2)C0

---

Modifications in 3.30(AQU.2)C0

1. [ENHANCEMENT]  
BWM Performance Enhancement.

## Features: 3.30(AQU.1)C0

---

### Modifications in 3.30(AQU.1)C0

1. [BUG FIX] eITS# 130903164

Symptom:

Actions in IDP profile can't be correctly saved after reboot.

Condition:

It occurs when the rule action default is none and then set to reject-both.

2. [BUG FIX]

Symptom:

It occurs to kernel crash when enabling BWM service.

Condition:

1. Create a service group contains at least 2 service objects which belong to TCP protocol.
2. Enable BWM service and add an BWM rule with the following setting:
  - a. Choose "Service Object" as service type.
  - b. Select the service group just been created from the Service Object drop-down list.
3. It will occur to kernel crash later when you have TCP traffic pass through device.

## Features: 3.30(AQU.0)C0

---

### Modifications in 3.30(AQU.0)C0

1. [ENHANCEMENT]  
IDP 3.0: Improving IDP engine with next-generation Application Intelligence technology.
2. [FEATURE][CHANGE]  
Combine core dump to diagnostic info.
3. [FEATURE][CHANGE]  
License Reminding days change from 10, 20, 30 to 10, 30, 180 days.
4. [FEATURE][CHANGE]  
Adjust the precedence of VPN rule for rule swap friendly. The priority of rule swap: Site-to-site VPN > Dynamic VPN = L2TP. (> means prior to)
5. [FEATURE][CHANGE]  
Modify application scenario pictures in VPN quick setup wizard.
6. [ENHANCEMENT]  
VPN Gateway edit page enhancement.
  - (1) Add inote for Static Address & Dynamic Address.
  - (2) When select Static Address, Negotiation mode will change to Main mode,  
When select Dynamic Address, Negotiation mode will change to Aggressive mode.
  - (3) Move Negotiation mode to Basic setting from Advance setting.
7. [ENHANCEMENT]  
SSLVPN SecuExtender supports Windows 8
8. [ENHANCEMENT]  
Backup system's startup-config.conf while firmware update from 3.00 to 3.30 in the name of startup-config-(current time).conf, such as startup-config-07290725.conf
9. [ENHANCEMENT] eITS# 130102441  
Add CLI support to change service port of external syslog server.
  1. Router(config)# logging syslog <1..4> port <1..65535> ; to change service port.
  2. Router(config)# no logging syslog <1..4> port ; to reset service port to 514.
  3. Router# show logging status ; to show server port information.
10. [ENHANCEMENT] eITS#130100397  
Add CLI to get higher security when SIP ALG is on.
  1. Router(config)# alg sip direct-signaling
  2. Router(config)# alg sip direct-media  
When the two options are yes, it will change the original sip ALG behavior.  
direct-signaling will expect incoming calls from register only.  
direct-media will expect media streams between signaling endpoints only.
11. [FEATURE] [CHANGE]

Clear "Don't Fragment Bit" of ESP packet when outgoing ESP packet has "Don't Fragment Bit".

12. [FEATURE] [CHANGE]

System default setting change, enable IPv4/IPv6 firewall session limit per host and set limit to 1000.

Add the following configuration in the system-default.conf:

session-limit activate

session-limit limit 1000

session-limit6 activate

session-limit6 limit 1000

13. [BUG FIX] eITS# 120705400 , SPR: 1207312247

Symptom:

Customer can't login successfully anymore.

Condition:

Even customers disconnect L2TP over IPSec connection, but device also shown the related connection. In addition, customer can't login successfully anymore.

14. [BUG FIX] eITS# 120601651 , SPR: 1208271529

Symptom:

USG stop to authorize users to login (both login and SSL VPN)

Condition:

After login to USG by using SSL VPN few times per day, USG will stop to authorize users

15. [BUG FIX] eITS# 120801928 , SPR: 1208271530

Symptom:

User can't establish L2TP over IPSec VPN to device, when check device, there are many L2TP over IPSec VPN tunnel's time out are "0"

Condition:

When user established many time L2TP over IPSec tunnel, he will meet that he can't establish tunnel to device successfully. And in the device Monitor, he find there are many L2TP tunnel's time out "0". It looks the tunnel is zombie.

16. [BUG FIX] eITS# 120601651 , SPR: 1208271529

Symptom:

Device will crash and reboot, look like VPN is the root cause.

Condition:

Customer wants to use certification for VPN criteria, but device will crash.

17. [BUG FIX] eITS# 120901338 , SPR: 121005306

Symptom:

L2TP setup auto MSS can't work.

Condition:



We have resolve auto MSS issue on IPsec VPN but not on L2tp.

18. [BUG FIX] eITS# 130101731 , SPR: 1301181941

Symptom:

Windows auto update session will kept in the HTTP daemon

Condition:

If enabled force authentication, the HTTP daemon will kept all of the sessions. This symptom is coming from windows auto update, and PC not authenticated with device yet.(windows auto update session will kept in the HTTP daemon)

19. [BUG FIX] eITS# 130202138 , SPR: 130304171

Symptom:

BWM cannot detect the DSCP packet.

Condition:

BWM cannot detect the DSCP packet.

20. [BUG FIX] eITS# 120303465 , SPR: 1206211366

Symptom:

ESP traffic can't pass through VPN tunnel.

Condition:

Establish a VPN tunnel1, and try to establish another VPN in tunnel1. It will fail because the nego traffic can't pass through tunnel.

21. [BUG FIX] eITS# 120601411 , SPR: 120703086

Symptom:

Content Filter BC URL testing can't query.

Condition:

Customer can't use it for testing.

22. [BUG FIX] eITS# 120604140 , SPR: 120709508

Symptom:

Device will get CPU high with anti-virus decompress.

Condition:

Customers have to disable this setting to avoid CPU high.

23. [BUG FIX] eITS# 120600858 , SPR: 1207171148

Symptom:

DNS traffic will still pass through passive interface even the corresponding active interface is up.

Condition:

Set up WAN1 and WAN2 in the Trunk as Active and Passive. While WAN1 is down, all traffic will pass through WAN2. While WAN1 is back, DNS traffic will still pass through WAN2.

24. [BUG FIX] eITS# 120601407 , SPR: 1207181340

Symptom:

Enable anti-virus will CPU high

Condition:

Because customer enable decompress cause device CPU high.

25. [BUG FIX] eITS# 120603369 , SPR: 1207181349

Symptom:

After establishing several IPsec VPN tunnels, users can't log into device or the tunnel which uses X-Auth won't build-up anymore.

Condition:

Use X-Auth in IPsec VPN, and build-up several VPN tunnels. After few days, users can't log into devices.

26. [BUG FIX] eITS# 120402410 , SPR: 1207241710

Symptom:

Nail-up doesn't work.

Condition:

While the VPN tunnel disconnected, even though the nail-up is enable, the tunnel won't be established automatically.

27. [BUG FIX] eITS# 120705775 , SPR: 1207261898

Symptom:

In IPsec VPN setting, when select FQDN for peer gateway IP, after reboot, device will spend long time for apply configuration.

Condition:

Based on Firmware:3.00 patch2. In IPsec VPN setting, select FQDN for peer gateway IP, after reboot, device will spend long time for apply configuration.

28. [BUG FIX] eITS# 120707485 , SPR: 1207261902

Symptom:

Customer setup L2TP and can establish it, but after device reboot it will failed.

Condition:

- 1.) Set a PSK in L2TP GW like "12345678"
- 2.) Connect to this L2TP with any Client try User: tobiass Pass: 12345678\
- 3.) Your connection is established now.
- 4.) Reboot USG-20W
- 5.) Try again L2TP connection, it will fail query with "Authentication failed" in Log
- 6.) Change to another PSK then change back in Phase 1 L2TP "12345678" Apply
- 7.) L2TP works back to normal

29. [BUG FIX] eITS# 120707647 , SPR: 120801011

Symptom:

After changing policy route destination criteria, rule won't work.

Condition:

1. Take USG200 with 3.00(xxx4).b3-r34073 Firmware (or a version before – it worked on the ITS firmware up the beginning of June) and create a default config.
2. Create a SNAT policy route based on the source IP and check if it's working
3. Change the destination field of that policy route to some host
4. Change the destination field of that policy to "Any".
5. The policy route does not work anymore.

30. [BUG FIX] eITS# 120403087 , SPR: 120808412

Symptom:

The user will be logged out after few minutes.

Condition:

The customer enabled Auth. Policy. After logging in few minutes, users will be logged out and redirected to log in page. It is because PC which doesn't log in will send out 7~ 8 ports 80 sessions, and these sessions will occupy and release slowly. If there are 5 users like this, then the port 80 sessions will be full. Other users can't log in anymore or will be logged out.

31. [BUG FIX] eITS# 120600291 , SPR: 120808425

Symptom:

Dynamic IPsec VPN can't always build-up successfully.

Condition:

If using DDNS to build-up dynamic IPsec VPN, it will be successful in the beginning. After reboot, it will be failed because USG will use the wrong phase.

32. [BUG FIX] eITS# 120707372 , SPR: 1208201049

Symptom:

SSL RDP will blank after 74 days.

Condition:

Customer found their SSL RDP will suddenly blank and only restart can resolve it.

33. [BUG FIX] eITS# 120700861 , SPR: 1208201051

Symptom:

L2TP can't connect.

Condition:

Customer setup L2TP on USG1000, but they found it can't work after 14 days, reboot can't resolve issue they have to inactive then active rule.

34. [BUG FIX] eITS# 120802538 , SPR: 1208281642

Symptom:

VPN will drop package.

Condition:

After using a period of time, device will start drop VPN package.

35. [BUG FIX] eITS# 120708217 , SPR: 1208291812

Symptom:

Using this firmware will cause CPU high.

Condition:

Using this firmware will cause CPU high.

36. [BUG FIX] eITS# 120800018 , SPR: 1208312144

Symptom:

It is sometimes failed to establish L2TP tunnel.

Condition:

When create for dynamic VPN and L2TP tunnel at the same time, the device will select wrong rule when establishing the L2TP tunnel.

37. [BUG FIX] eITS# 120704432 , SPR: 1208312171

Symptom:

After upgrade from 2.20 to 3.00, lot of L2TP clients can't login.

Condition:

Customer has about 1000 L2TP access at the same time, but in ZLD3.00 it only can let about 80-90 user login, others will failed.

38. [BUG FIX] eITS# 120804388 , SPR: 120904165

Symptom:

When downloading the large size mails, the device will hang.

Condition:

When downloading the large size mails, the device will hanging.(Need setting outlook Express to sending mail with HTML Base64 encoding, and resend it with multiple type attachment files. (Ex: xxx1.zip, test1.eml, xxx1.rar, test2.eml,xxx2.zip,xxx3.eml)

39. [BUG FIX] eITS# 120803878 , SPR: 1209211470

Symptom:

Reboots automatically two times per day

Condition:

1. This can't be easily reproduced. 2. In my surrounding, I can reproduce the issue and the reproduced step is: (1) Configure a Site-to-Site IPsec VPN rule with Enable Replay Detection. (2) Trigger dial. (3) Disconnect the tunnel. (4) Use CLI "debug ipsec crypto-layoff disable" to force software to encrypt/decrypt IPsec traffic. (5) Trigger dial. (6) Disconnect the tunnel. (7) Use CLI "debug IPsec crypto-layoff enable" to force hardware to encrypt/decrypt IPsec traffic. (8) Modify VPN rule and uncheck the Enable Replay Detection. (9) Trigger dial again and you will see kernel oops and then kernel panic.

40. [BUG FIX] eITS# 120900317 , SPR: 1209241564

Symptom:

There is no device in the USG LAN network, but the DHCP client list still shown before status even clear those IP by using CLI command, when wait a period time, the IP comes back.

Condition:

Customer only setup DHCP pool-size 15 and there is no setup DHCP-IP binding function

41. [BUG FIX] eITS# 120600528 , SPR: 1209251690

Symptom:

DNS will query failed.

Condition:

Users can't access websites, but if flush DNS cache or add DNS zone forward, device will work fine.

42. [BUG FIX] eITS# 120903430 , SPR: 1210181413

Symptom:

PC which is using Intel Centrino Card 2200B/G can't connect to the Wi-Fi.

Condition:

PC which is using Intel Centrino Card 2200B/G can't connect to the Wi-Fi.

43. [BUG FIX] eITS# 121000748 , SPR: 1210221657

Symptom:

L2TP error log USG Send:[HASH][NOTIFY:INVALID\_SPI]

Condition:

L2TP error log USG Send:[HASH][NOTIFY:INVALID\_SPI]

44. [BUG FIX] eITS# 120903942 , SPR: 1210292477

Symptom:

PPTP connection to ISP will disconnect in few seconds.

Condition:

Based on WK37 firmware, the PPTP connection to ISP will disconnect in few seconds.

When rollback to 3.00(BDQ.2) version, the PPTP connection is fine.

45. [BUG FIX] eITS# 121007904 , SPR: 121105247

Symptom:

There is no limitation for the username quantity when setup SMTP authentication but at SYSLOG setting, the username name has limitation only for 31 characters when setup SMTP authentication.

Condition:

There is no limitation for the username quantity when setup SMTP authentication but at SYSLOG setting, the username name has limitation only for 31 characters when setup SMTP authentication.

46. [BUG FIX] eITS# 121101047 , SPR: 121108859

Symptom:

Virus Signature "MW.MAGNUM.A.GEN". will destroy attached Files (doc and xls and zip)

Condition:

Engine ZyXEL v2.0, Version 3.167, Released 2012-11-06 15:19:00Virus Signature "MW.MAGNUM.A.GEN". will destroy attached Files (doc and xls and zip) which send from SMTP/POP3.Test step:1. Send an email from live.com to a SMTP/POP3 email server which is located in LAN, and attach a excel file(.xls)2. Connect my PC to LAN side and tried to receive the email.3. The excel file will be destroyed.

47. [BUG FIX] eITS# 121101078 , SPR: 121109994

Symptom:

Anti-virus destroys the attachment of the mail.

Condition:

N/A

48. [BUG FIX] eITS# 121007853 , SPR: 1211191544

Symptom:

Device will hang or crash if changing the SSL VPN address pool the same with vlan interface subnet.

Condition:

Change the SSL VPN address range with the vlan interface subnet, the device will hang or crash.

49. [BUG FIX] eITS# 121102153 , SPR: 1211201679

Symptom:

IDP 8001773 will block downloading

Condition:

The customer replied IDP 8001773 will block the file from the link as below. I can reproduce the symptom and have reported to Lionix. Ticket ID is 501.Here is the test steps.1. Enable IDP.2. Try to download the "Public Beta Firmware". In the beginning, the connection was successful. After few minutes, around 15%, the download will be stuck.<http://www.auerswald.de/de/service/service-produkte/telefone/127-service/publicbeta/1089-publicbeta-comfortel-3500-voip-de.html>

50. [BUG FIX] eITS# 121005323 , SPR: 1211211751

Symptom:

Two L2TP clients from the same source can't establish the second tunnel.

Condition:

1. Two Windows PC are behind the same NAT router and tried to establish L2TP to the same USG.2. The first L2TP tunnel can establish successfully, but the second will be failed.

51. [BUG FIX] eITS# 121003144 , SPR: 1211221813

Symptom:

Please see the topology file. If the SIP ALG turn on, from [additional branch] to [branch ] or [branch] to [branch], one-side hearing. If the SIP ALG turns off, from [branch] to [branch], they can communicate well but sip-phone in [additional branch] can't register on the sip-server.

Condition:

There is a USG1000 and SIP server in HQ. There are USG 20 in branch office, and additional branch on the internet(static IP or PPPoE).The customer hope that from [branch] to [branch] and [additional branch] to [branch] can communicate each other. If the SIP ALG turn on, from [additional branch] to [branch ] or [branch] to [branch], one-side hearing. If the SIP ALG turns off, from [branch] to [branch], they can communicate well but sip-phone in [additional branch] can't register on the sip-server.

52. [BUG FIX] eITS# 121006856 , SPR: 1211221814

Symptom:

2 clients behind the same NAT can't connect to the USG1000 by L2TP.

Condition:

2 clients behind the same NAT can't connect to the USG1000 by L2TP.

53. [BUG FIX] eITS# 121100863 , SPR: 1211221830

Symptom:

The device sometimes hangs and can't not access. There is a coredump about IPsec.

Condition:

If DNS query failed, there will be empty space in the kernel.

54. [BUG FIX] eITS# 121101600 , SPR: 1211292214

Symptom:

The monitor of users will show wrong IPs.

Condition:

Establish 3 more SSL or L2TP.Go to dashboard to show the users, it will appear wrong information. Please refer to the attachment.

55. [BUG FIX] eITS# 121007288 , SPR: 121203004

Symptom:

NAT loopback is not working on bridge interface.

Condition:

The customer configured NAT virtual server, the rule is WAN IP(46.226.101.130) mapping to RDP server IP(192.168.0.5) and enable NAT loopback. The client can't access WAN IP, but if access RDP server IP, it can work.

56. [BUG FIX] eITS# 121101853 , SPR: 121204120

Symptom:

Windows 7 32 bit run SecuExtender version 2.5.17, when PC does hibernate, it will hang.

Condition:

Windows 7 64 bit run SecuExtender version 2.5.17, it has no problem. Windows 7 32 bit run SecuExtender version 2.5.17, in hibernate mode, when I power on again, it will reboot. When I try to uninstall it, the PC will hang or blue screen.

57. [BUG FIX] eITS# 121103708 , SPR: 1212201565

Symptom:

L2TP client can't access internet via USG if the WAN is PPTP.

Condition:

Adding a policy route to allow L2TP to access the internet via USG; however, it will be failed. PPPoE is fine, but PPTP will be failed.

58. [BUG FIX] eITS# 130103200 , SPR: 1301292756

Symptom:

When enabling bridge interface and create a NAT rule, the NAT loop back function is not work.

Condition:

When enabling bridge interface and create a NAT rule, the NAT loop back function is not work. The issue is resolved by 300BDR4ITS-WK46-2012-11-27-121007288.bin

59. [BUG FIX] eITS# 130102152 , SPR: 1301302910

Symptom:

When enabling UTM services (AV, AS, ADP), DUT will drop SMTP SYN packet from Internet to LAN. It caused email cannot arrived to LAN mail server.

Condition:

When packet includes TCP option 30 info without any description in the packet DUT will return this packet by UTM scan flow. Uncommon issue.

60. [BUG FIX] eITS# 130104634 , SPR: 130204222

Symptom:

Device crashed and generated a coredump.

Condition:

The issue happened when QuickSec deals with L2TP establishing and deleting for a client at the same time.

61. [BUG FIX] eITS# 130200456 , SPR: 130218686

Symptom:

If disconnecting VPN tunnel not correctly, the packet flow won't delete the old routing.

Condition:

1. USG300 is the server role. Configure a dynamic rule on it. 2. USG200 is the client. Establish a site-site VPN to USG300.3. After establishing the tunnel, unplug the cable. USG200 will show the connection is interrupt, then reconnect the tunnel.4. There will be one tunnel in the Monitor, but two routing in the packet flow.

62. [BUG FIX] eITS# 130202795 , SPR: 1302251314



Symptom:

The crash issue was caused by DNS query and configuration change at the same time.

Condition:

The crash issue was caused by DNS query and configuration change at the same time.

63. [BUG FIX] eITS# 130201157 , SPR: 1302251367

Symptom:

USG-100 VPN Monitor entry is wrong

Condition:

After establishing VPN tunnel, the policy will be wrong in the log entry. Please refer to the attachment for the topology and test result.

64. [BUG FIX] eITS# 130100097 , SPR: 1302251392

Symptom:

SIP traffic from internet will pass firewall rule checking even there is no related NAT rule or firewall rule.

Condition:

When a SIP server behind USG and it acts SIP proxy server (Server will establish the SIP traffic by itself) Other SIP traffics from internet will pass through USG and arrive to the LAN SIP server directly.

65. [BUG FIX] eITS# 130200602 , SPR: 1302261428

Symptom:

USG200 -- VPN -- USG2000 -- Radius Server. There are some users will X-Auth via Radius server which is behind USG2000. After around 50 users, the USG cannot be logged in anymore.

Condition:

Test X-Auth and Force Auth at the same time, after around 50 users, no more users can log in.

66. [BUG FIX] eITS# 121100139 , SPR: 1302261483

Symptom:

SIP function behaves incorrectly.

Condition:

When LAN has a SIP proxy server and establish SIP traffic by itself, if there are others SIP traffic arrive to USG from internet, even there is no related NAT rule and firewall rule, the SIP traffic will arrive to the LAN SIP server directly

67. [BUG FIX] eITS# 130203088 , SPR: 130304104

Symptom:

The dynamic routing rule will always exist in packet flow table.

Condition:

The dynamic routing rule will always exist in packet flow table even disconnected the VPN rule.

68. [BUG FIX] eITS# 130203762 , SPR: 130304154

Symptom:

If using custom APN authentication type, USG cannot detect the USG dongle.

Condition:

If using custom APN authentication type, USG cannot detect the USG dongle.

69. [BUG FIX] eITS# 130202140 , SPR: 130304177

Symptom:

BWM cannot detect ICMP packet.

Condition:

BWM cannot detect ICMP packet.

70. [BUG FIX] eITS# 120903746 , SPR: 121001016

Symptom:

When create BWM rules and reboot device, there are error messages in log page.

Condition:

When create BWM rules and reboot device, there are error messages in log page. Error messages describe BWM rule binding IPsec VPN tunnel interface.

71. [BUG FIX] eITS# 121003517 , SPR: 1210292417

Symptom:

The CPU high caused by Commtouch library libasapsdk.so.7.3.

Condition:

The CPU high caused by Commtouch library libasapsdk.so.7.3. When we click "Send Report Now" on FW version "3.00(AQQ.4)b3ITS-r3407", it will have a CPU high issue.

72. [BUG FIX] eITS# 121006060 , SPR: 1210292421

Symptom:

The user will be logged out after few minutes.

Condition:

Same issue as SPR #120808412. The customer enabled Auth. Policy. After logging in few minutes, users will be logged out and redirected to log in page. It is because PC which doesn't log in will send out 7~ 8 ports 80 sessions, and these sessions will occupy and release slowly. If there are 5 users like this, then the port 80 sessions will be full. Other users can't log in anymore or will be logged out.

73. [BUG FIX] eITS# 121002066 , SPR: 121101002

Symptom:

The device hangs while it happens to rekey in the L2TP VPN connection with user connect to device.

Condition:

The device hangs while it happens to rekey in the L2TP VPN connection with user connect to device.

74. [BUG FIX] eITS# 121100068 , SPR: 121105227

Symptom:

Graphic view of port statistics can't display.

Condition:

In the Statistics Table, there are packets statistics for port 1 and port 2. However, graphic view of port statistics can't display.

75. [BUG FIX] eITS# 121101184 , SPR: 1211191579

Symptom:

If more VPN connections are added and shutdown the device, it takes long time to get USG100-PLUS rebooted.

Condition:

If more VPN connections are added and shutdown the device, it takes long time to get USG100-PLUS rebooted. In customer's config files, there are three gateways using DDNS as the peer gateway address, and these three gateways are applied to several VPN connections.

76. [BUG FIX] eITS# 121005321 , SPR: 1211211753

Symptom:

The two clients are behind the same NAT router. After establishing L2TP, another user can't access the WEB GUI of USG via WAN.

Condition:

1. Client A and Client B are behind the same NAT router.
2. Client A established L2TP to USG.
3. Client B can't access the WEB GUI of USG via WAN.

77. [BUG FIX] eITS# 121000722 , SPR: 1211231899

Symptom:

When login as User on USG, get sometimes the message: "You will be redirected to the login page due idle timeout or network problem."

Condition:

USG will keep the PC's http session, and cause Apache can't accept log in user.

78. [BUG FIX] eITS# 121007802 , SPR: 1211272073

Symptom:

The customer reported the ticket regarding the memory usage high when numbers of user login to the device over 170. When the symptom happening, the device will hanged. Until you reboot the device.

Condition:

- (1) There is a core dump about ctcpd.bin

(2) Also I have noticed there are many “XXX\_mem\_wd.dbg” file under temp folder when using FTP.

(3) I have collected the diag-info on the customer’s device. RDs think it may be similar to [eITS#120403087]: When the customer activates authentication policy after few seconds, users aren’t redirect to login page”.

79. [BUG FIX] eITS# 121200800 , SPR: 1212211595

Symptom:

1. After activating the authentication policy few seconds, the users (in the LAN) aren’t directed to the login page.
2. The users will see the white page when waiting to the redirect.
3. Sometimes user can’t direct to the login page and got the error page when no direct.

Condition:

Step 1: Enable authentication policy

Step 2: Try to login USG=> Cannot be direct to the login page.

80. [BUG FIX] eITS# 121200350 , SPR: 1212262058

Symptom:

No internet traffic through L2TP tunnel.

Condition:

No internet traffics go through L2TP tunnel. The L2TP client internet traffic can’t pass throughput the USG. I have captured the packet on wan1\_ppp interface. It is a PPTP interface.

81. [BUG FIX] eITS# 130203846 , SPR: 130301025

Symptom:

AutoVPN doesn’t delete the old policy rule for dynamic VPN.

Condition:

AutoVPN doesn’t delete the old policy rule for dynamic VPN, it caused the traffic can’t pass through the VPN tunnel. Unless you reboot the USG, it will work well immediately.

82. [BUG FIX] eITS# 130203857 , SPR: 1303151215

Symptom:

AutoVPN doesn’t delete the old policy rule for dynamic VPN.

Condition:

AutoVPN doesn’t delete the old policy rule for dynamic VPN, it caused the traffic can’t pass through the VPN tunnel. Unless you reboot the USG, it will work well immediately.

83. [BUG FIX] eITS# 130402893 , SPR: 1304191992

Symptom:

After upgrade the firmware WK11, while establishing VPN tunnel, the Lan1 interface of device will show inactivate via console, and stop DHCP server on Lan1 interface.

- 1.site to site
2. SSLVPN(pool IPsec LAN)
- 3.Enable NetBIOS broadcast over IPsec

Condition:

After upgrade the firmware WK11, while establishing VPN tunnel, the Lan1 interface of device will show inactivate via console, and stop DHCP server on Lan1 interface. This is the same with ticket #130400573.

84. [BUG FIX] eITS# 71847 , SPR: 120322844

Symptom:

Device boot very slow

Condition:

If customers configure DDNS for IPsec criterion, it will slow down boot speed.

85. [BUG FIX] eITS# 120400091 , SPR: 1206211372

Symptom:

Device get hang due to L2TP tunnel.

Condition:

After establishing a L2TP tunnel, if the establishing time over the lease time that the customer set, then device will hang.

86. [BUG FIX] eITS# 120601715 , SPR: 1206261565

Symptom:

Device will crash using when build the VPN

Condition:

Two lacks of exceptions, can be protected by merging the exceptions from QuickSec 5.2.

87. [BUG FIX] eITS# 120603509 , SPR: 120702009

Symptom:

DDNS can't use number for account.

Condition:

Customer use pure number for account but GUI didn't let it saved.

88. [BUG FIX] eITS# 120603431 , SPR: 120709515

Symptom:

After upgrade to ZLD 3.0, customer can't use LDAP for authentication server.

Condition:

Because customer's LDAP password use SSHA for encrypt algorithm, so our device can't recognize.

89. [BUG FIX] eITS# 120502681 , SPR: 1207171277

Symptom:

Changing App "From" criteria can't work.

Condition:

If customer didn't use default "any" for this criteria, this rule can't work because if change to other rule us

90. [BUG FIX] eITS# 120403253 , SPR: 120718132

Symptom:

Customer use XAUTH build VPN tunnel, after few days will fail.

Condition:

Device didn't flush the counter, if counter full clients can't login anymore.

91. [BUG FIX] eITS# 120703738 , SPR: 1207191427

Symptom:

Device CPU high

Condition:

After checking, this is another decompress issue.

92. [BUG FIX] eITS# 120504199 , SPR: 1207201537

Symptom:

Using for certificate to establish the tunnel, device will crash.

Condition:

Using for certificate to establish the tunnel, device will crash.(Fixed crash issue when dialing certificate tunnel. The exceptions is merged from QuickSec 5.2.The crash is due to QuickSec received the peer request outside IKE negotiation.)

93. [BUG FIX] eITS# 120703349 , SPR: 1207201542

Symptom:

USG20W not accepting MS Windows 7 ICS DHCP lease.

Condition:

USG20W not accepting MS Windows 7 ICS DHCP lease. We resolve this issue with Date Firmware.

94. [BUG FIX] eITS# 120502879 , SPR: 1207201544

Symptom:

Using for PSK and certificate to establish the tunnel will cause the VPN rule swapping.

Condition:

Using for PSK and certificate to establish the tunnel will cause the VPN rule swapping.

95. [BUG FIX] eITS# 120502123 , SPR: 1207231642

Symptom:

Anti-Spam service(port 5678) causes the device CPU high.

Condition:

Anti-Spam service(port 5678) causes the device CPU high.

96. [BUG FIX] eITS# 120705833 , SPR: 1207312225

Symptom:

Too much time to apply configuration

Condition:

This configuration file has setting FQDN in ISAKMP policy. When you apply the configuration file, it need more time to query domain name.

97. [BUG FIX] eITS# 120300323 , SPR: 120803134

Symptom:

The file sharing function can't work when file server is NAS.(NAS server forbidden anonymous login, and return unexpected error code.)

Condition:

The file sharing function can't work when file server is NAS.(NAS server forbidden anonymous login, and return unexpected error code.)

98. [BUG FIX] eITS# 120304369 , SPR: 120803143

Symptom:

Sometimes the DNS daemon will dead.(query will fail)

Condition:

Sometimes the DNS daemon will dead.(query will fail)

99. [BUG FIX] eITS# 120304686 , SPR: 120803145

Symptom:

The "Ignore "Don't Fragment" setting in IP header" not work.(packets size can't over 1419)

Condition:

The "Ignore "Don't Fragment" setting in IP header" not work.(packets size can't over 1419)

100. [BUG FIX] eITS# 120500365 , SPR: 120803148

Symptom:

Establishing the L2TP tunnel will fail if the customer deletes the "default" certificate.

Condition:

Establishing the L2TP tunnel will fail if the customer deletes the "default" certificate.

101. [BUG FIX] eITS# 120301945 , SPR: 120803154

Symptom:

The Auto MSS function can't work fine.

Condition:

The Auto MSS function can't work fine.

102. [BUG FIX] eITS# 120401415 , SPR: 120803156

Symptom:

After upgrade the firmware to 3.00, the device will reboot.(the configuration will be modified)

Condition:

After upgrade the 3.00 firmware, the device will reboot.(the configuration will be modified)

103. [BUG FIX] eITS# 120403246 , SPR: 120803160

Symptom:

The release time and re-authentication time will caused device crash.( after established the L2TP, and times up. the device will crash)

Condition:

The release time and re-authentication time will caused device crash.( after established the L2TP, and times up. the device will crash)

104. [BUG FIX] eITS# 120402918 , SPR: 120803161

Symptom:

The user that authenticates with external server, the user name using for spaces will cause the authentication fail.

Condition:

The user that authenticates with external server, the user name using for spaces will cause the authentication fail.

105. [BUG FIX] eITS# 120403270 , SPR: 120803163

Symptom:

The device will selected wrong VPN gateway when there are many rules.

Condition:

The device will selected wrong VPN gateway when there are many rules.

106. [BUG FIX] eITS# 120403778 , SPR: 120803168

Symptom:

Connect with Android 4.X, IOS 5.1 or Windows 7.It will cause Payload Issue.

Condition:

Easy Reproduce, just need a USG with two policies created, one L2TP Default just enable and one Dynamic Connection to IP Sec Client. In Phase 1 set: AES256, SHA1, DH1Then connect with Android 4.X, IOS 5.1 or Windows 7.It will cause Payload Issue.

107. [BUG FIX] eITS# 120502182 , SPR: 120803170

Symptom:

If created the Log DDNS name in the DDNS setting, the GUI will showing strange name.

Condition:

If created the Log DDNS name in the DDNS setting, the GUI will showing strange name.

108. [BUG FIX] eITS# 120500936 , SPR: 120803171

Symptom:

The NAT-T function will be enabled after reboot the device.(it's not write to configuration file)

Condition:

The NAT-T function will be enabled after reboot the device.(it's not write to configuration file)

109. [BUG FIX] eITS# 120502982 , SPR: 120803173

Symptom:

When establishing the site to site VPN, the device will tried to establishing the tunnel that is already inactivated L2TP rule.



Condition:

When establishing the site to site VPN, the device will tried to establishing the tunnel that is already inactivated L2TP rule.

110. [BUG FIX] eITS# 120504065 , SPR: 120803174

Symptom:

Service object can't be deleted successfully.

Condition:

1. Create many service objects.
2. Create group A, and include #1 service object.
3. Create group B, and include group A and the other service object.
4. Delete all of the objects that in #1
5. Cannot delete group A

111. [BUG FIX] eITS# 120503134 , SPR: 120803177

Symptom:

If the LDAP server using for the other port(not 389). When the L2TP client establishing the tunnel, the device still using for 389 port to authentication with LDAP server.

Condition:

If the LDAP server using for the other port(not 389). When the L2TP client establishing the tunnel, the device still using for 389 port to authentication with LDAP server.

112. [BUG FIX] eITS# 120600344 , SPR: 120803179

Symptom:

If using for L2TP tunnel as BWM rule, it will unable been saved.

Condition:

If using for L2TP tunnel as BWM rule, it will unable been saved.

113. [BUG FIX] eITS# 120706110 , SPR: 120806222

Symptom:

USG50 build VPN connection to USG2000, VPN connection auto disconnected

Condition:

We solved this problem with firmware 300BDS0ITS-r34073.bin.

114. [BUG FIX] eITS# 120805401 , SPR: 120903003

Symptom:

It fixed CPU high by ctipd.bin.

Condition:

It fixed CPU high by ctipd.bin with firmware 300BDR4ITS-r34440

115. [BUG FIX] eITS# 120801599 , SPR: 120910536

Symptom:

In the customer's network environment, the device can't get the IP from DHCP server.

Condition:

In the customer's network environment, the device can't get the IP from DHCP server.

116. [BUG FIX] eITS# 72417 , SPR: 121015926

Symptom:

System cannot detect unacceptable character in pre-share key string then device reload lastgood.conf after rebooting. For example: (space) and ?

Condition:

System cannot detect unacceptable character in pre-share key string then device reload lastgood.conf after rebooting. For example: (space) and ?

117. [BUG FIX] eITS# 72331 , SPR: 121015928

Symptom:

Customer can't use QNAP for SSL file sharing server.

Condition:

Ask for a fix with let user typing accept account/password to login NAS.

118. [BUG FIX] eITS# 120602006 , SPR: 1211131099

Symptom:

When enabling SIP ALG, the SIP traffic can work fine, but the fax can't work. When disabling SIP ALG, the SIP can't work anymore, but fax work fine.

Condition:

When enabling SIP ALG, the SIP traffic can work fine, but the fax can't work. When disabling SIP ALG, the SIP can't work anymore, but fax work fine.

119. [BUG FIX] eITS# 72297, SPR: 120323955

Symptom:

It is not possible to use the ip 192.168.200.1 on the lan1 interface. After the reboot the ip on the interface is 0.0.0.0

Condition:

It is not possible to use the ip 192.168.200.1 on the lan1 interface. After the reboot the ip on the interface is 0.0.0.0

## 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, “300AQU0C0.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) Memery 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: V1.21 | 2009-11-18 08:49:30
DRAM: Size = 2039 Mbytes

Kernel Version: V2.6.25.4 | 2013-09-06 11:01:29
ZLD Version: V3.30(AQW.0) | 2013-09-09 11:08:24

Press any key to enter debug mode within 1 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: V1.21 | 2009-11-18 08:49:30
DRAM: Size = 2039 Mbytes

Kernel Version: V2.6.25.4 | 2013-09-06 11:01:29
ZLD Version: V3.30(AQW.0) | 2013-09-09 11:08:24

Press any key to enter debug mode within 1 seconds.
.....
Enter Debug Mode

usg2000> █

```

- 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 .....
.....
.....
.....
.....
.....
.....
OK
> █
```

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

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

- If “Connect a computer to port 1 and FTP to 192.168.1.1 to upload the new file” displays on the screen, you need to recover the firmware by the following procedure.

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

- You will use FTP to upload the firmware package. Keep the console session open in order to see when the firmware recovery finishes.
- Set your computer to use a static IP address from 192.168.1.2 ~ 192.168.1.254. No matter how you have configured the ZyWALL's IP addresses, your computer must use a static IP address in this range to recover the firmware.
- Connect your computer to the ZyWALL's port 1 (the only port that you can use for recovering the firmware).
- Use an FTP client on your computer to connect to the ZyWALL. This example uses the ftp command in the Windows command prompt. The ZyWALL's FTP server IP address for firmware recovery is 192.168.1.1
- Log in without user name (just press enter).
- Set the transfer mode to binary. Use "bin" (or just "bi" in the Windows command prompt).
- Transfer the firmware file from your computer to the ZyWALL (the command is "put 310AAAC0C0.bin" in the Windows command prompt).

```
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 00:00 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 C:\ZLD FW\310AAAC0C0.bin
```

- Wait for the file transfer to complete.

```
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 1.06Seconds 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!!