ZyXEL

Firmware Release Note

USG60W

Release V4.20(AAKZ.2)C0

Date: Nov 25, 2016
Author: Rain Lee
Project Leader: Rain Lee

Contents

ZyXEL USG60W

Release V4.20(AAKZ.2)C0

Release Note

Date: Nov 25, 2016

Supported Platforms:

ZyXEL USG60W

Versions:

ZLD Version: V4.20(AAKZ.2) | 2016-11-22 20:48:09
Boot Module Version: V1.02 | Jul 10 2014 14:05:59

Files lists contains in the Release ZIP file

File name:420AAKZ2C0.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 the configuration, the longer the update time. Do not turn off or reset the ZyWALL/USG 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: 420AAKZ2C0.conf
Purpose: This ASCII file contains default system configuration commands.

File name: 420AAKZ2C0.pdf
Purpose: This release file.

File name: 420AAKZ2C0.ri
Purpose: This binary firmware recovery image file is for emergent system firmware damage recovery only.
Note: The ZyWALL/USG firmware could be damaged, for example by the power going off or pressing Reset button during a firmware update.

File name: 420AAKZ2C0-MIB.zip

Purpose: The MIBs are to collect information on device. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

The zip file includes several files: 420AAKZ2C0-enterprise.mib,420AAKZ2C0-private.mib, ZYXEL-ES-SMI.MIB, ZYXEL-ES-CAPWAP.MIB, ZYXEL-ES-COMMON.MIB and ZYXEL-ES-ProWLAN.MIB. Please import ZYXEL-ES-SMI.MIB first.

File name: 420AAKZ2C0-opensource-list.xls

Purpose: This file lists the open source packages.

File name: 3G dongle compatibility table v106.xlsx, 3G patch file v106.wwan

Purpose: Mobile broadband dongle support list.

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 ge3, which are P3 port on the front 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 ge1, and the secondary WAN interface is ge2. These two interfaces will automatically get IP address using DHCP by default.
2. Recommended upgrade to ZLD4.13 patch2 C0 or later version first before upgrade to ZLD4.20.
3. It is recommended that user backs up “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.
4. If user upgrades from previous released firmware to this version, there is no need to restore to system default configuration.
5. When getting troubles in configuring via GUI (popup java script error, etc), it is recommended to clear browser’s cache first and try to configure again.
6. To reset device to system default, user could press RESET button for 5 seconds and the device would reset itself to system default configuration and then reboot.
   - Note: After resetting, the original configuration would be removed. It is recommended to backup the configuration before this operation.
7. If ZyWALL/USG can’t reboot successfully after firmware upgrade, please refer to Appendix 3: Firmware Recovery.

Design Limitations:

Note: Design Limitations described the system behavior or limitations in current version. They will be created into knowledge base.

APP Patrol

1. [SPR: 140425359, 140425375]

   [Symptom]

   If a profile is to block browser only (ex. Chrome, IE), it may not take effect because "user access website" have higher priority for matching.

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 50001/10443/10444/1723/2601-2604/2158/953. Users should avoid using these internal ports for built-in services.

   [Workaround]

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

DNS

1. [SPR: 140425458]

   [Symptom]

   DUT does not support *.com A-record PTR.

2. [SPR: 150122977]

   [Symptom]

   DNS security option will deny device local out DNS query

   [Condition]

   1. Edit the customize rule of DNS security option, and set the query recursion as deny.
   2. If device's WAN IP address is in the customize address range, device local-out DNS query will be deny.

GUI

1. Following are the table list for supporting GUI browser:

Operating System	For Administrator Login	For User Login
Windows 7 (X64) (SP1) Java 7 up-to-date	Internet Explorer 10.x, 11.x Chrome latest version Firefox latest version	Internet Explorer 10.x, 11.x Chrome latest version Firefox latest version

	Safari latest version	Safari latest version
Windows 7 (X32) (SP1) Java 7 up-to-date	Internet Explorer 10.x, 11.x Chrome latest version Firefox latest version Safari latest version	Internet Explorer 10.x, 11.x Chrome latest version Firefox latest version Safari latest version
Windows 8.0, 8.1 (X64) Java 7 up-to-date	Internet Explorer 10.x, 11.x Chrome latest version Firefox latest version Safari latest version	Internet Explorer 10.x, 11.x Chrome latest version Firefox latest version Safari latest version
Windows 8.0, 8.1 (X32) Java 7 up-to-date	Internet Explorer 10.x, 11.x Chrome latest version Firefox latest version Safari latest version	Internet Explorer 10.x, 11.x Chrome latest version Firefox latest version Safari latest version
Windows 10 (X64) Java 7 up-to-date	Internet Explorer 11.x Chrome latest version Firefox latest version Safari latest version edge latest version	Internet Explorer 11.x Chrome latest version Firefox latest version Safari latest version edge latest version
Linux OS(Ubuntu13.10x86)	Firefox latest version	Firefox latest version
Apple MAC OS X	Safari latest version Firefox latest version	Safari latest version Firefox latest version
iOS	8 latest version 9 latest version	8 latest version 9 latest version
Android	latest version	latest version

* Not support Opera browser

2. [SPR: 100415854]

   [Symptom]

   The GUI's initial help page's behavior was wrong.

   [Condition]

   1. In the GUI Interface page press the Site Map page, it will pop-up the window.
   2. Press the question mark (?), GUI will open the Site Map's help page.
   3. Close the help and Site Map window, press the Interface page's Help link.
   4. It still opens the Site Map's help page.

3. [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

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 cause 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: 070814168]

   [Symptom]

   VPN tunnel could not be established when:

   1. a non ZyWALL/USG peer gateway reboot and
   2. ZyWALL/USG has a previous established Phase 1 with peer gateway, and the Phase 1 has not expired yet. Under those conditions, ZyWALL/USG 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/USG or turn on DPD function to resolve problem.

2. [SPR: 100429119]

   [Symptom]

   VPN tunnel might be established with incorrect VPN Gateway

   [Condition]

   1. Prepare 2 ZyWALL/USG and reset to factory default configuration on both ZyWALL/USGs
   2. On ZyWALL/USG-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/USG-B
      1. Create one WAN interface
      2. Create one VPN Gateway. The Primary Peer Gateway Address is configured as WAN1 IP address of ZyWALL/USG-A and the Secondary Peer Gateway Address is configured as WAN2 IP address of ZyWALL/USG-A

4. Connect the VPN tunnel from ZyWALL/USG-B to ZyWALL/USG-A and we can see VPN-A is connected on ZyWALL/USG-A
5. Unplug WAN1 cable on ZyWALL/USG-A
6. After DPD triggered on ZyWALL/USG-B, the VPN Connection will be established again
7. On ZyWALL/USG-A, VPN-A is connected. But actually ZyWALL/USG-B should connect to VPN-B after step 5.

[Workaround]

Change the WAN1 setting of ZyWALL/USG-A to Static IP

3. [SPR: 140304057]

[Symptom]

After inactivating GRE over IPSec, old connection may remain if the traffic flows continuously. This may cause traffic bounded with old connection.

[Workaround]

Stop traffic for 180 seconds and the internal connection record will time out.

4. [SPR: 140416738]

[Symptom]

Ignore don't fragment setting cannot take effect immediately if there already existed the same connection.

[Workaround]

Stop traffic for 180 seconds and the internal connection record will time out.

5. The following VPN Gateway rules configured on the ZyWALL/USG cannot be provisioned to the IPSec VPN Client:
   1. IPv4 rules with IKEv2 version
   2. IPv4 rules with User-based PSK authentication
   3. IPv6 rules

SSL VPN

1. Following are the table list for SSL VPN supporting applications and operating systems:

Applications Operating System	Full Tunnel Mode	Reverse Proxy Mode File Sharing(Web-based Application)	RDP	VNC
Windows 7 (X64) (SP1) Java 7u45 or later	Internet Explorer 10.x, 11.x Chrome 45.x, 49.x, 50.x to latest version Firefox latest version Safari latest version	Internet Explorer 10.x, 11.x Chrome 45.x, 49.x, 50.x to latest version Firefox latest version Safari latest version	Internet Explorer 10.x, 11.x	Internet Explorer 10.x, 11.x Chrome 45.x, 49.x, 50.x to latest version Firefox latest version Safari latest version
Windows 7 (X32)	Internet Explorer 10.x, 11.x	Internet Explorer 10.x, 11.x	Internet Explorer	Internet Explorer

(SP1) Java 7u45 or later	Chrome 45.x, 49.x, 50.x to latest version Firefox latest version Safari latest version	Chrome 45.x, 49.x, 50.x to latest version Firefox latest version Safari latest version	10.x, 11.x	10.x, 11.x Chrome 45.x, 49.x, 50.x to latest version Firefox latest version Safari latest version
Windows 8, 8.1 (X64) Java 7u45 or later	Internet Explorer 10.x, 11.x Chrome 44.x or previous version Firefox latest version Safari latest version	Internet Explorer 10.x, 11.x Chrome 44.x or previous version Firefox latest version Safari latest version	Internet Explorer 10.x, 11.x	Internet Explorer 10.x, 11.x Chrome 44.x or previous version Firefox latest version Safari latest version
Windows 8, 8.1 (X32) Java 7u45 or later	Internet Explorer 10.x, 11.x Chrome 45.x, 49.x, 50.x to latest version Firefox latest version Safari latest version	Internet Explorer 10.x, 11.x Chrome 45.x, 49.x, 50.x to latest version Firefox latest version Safari latest version	Internet Explorer 10.x, 11.x	Internet Explorer 10.x, 11.x Chrome 45.x, 49.x, 50.x to latest version Firefox latest version Safari latest version
Windows 10 (X64) Java 7u45 or later	Internet Explorer 11.x Chrome 45.x, 49.x, 50.x to latest version Firefox latest version edge latest version	Internet Explorer 11.x Chrome 45.x, 49.x, 50.x to latest version Firefox latest version edge latest version	Internet Explorer 11.x	Internet Explorer 11.x Chrome 45.x, 49.x, 50.x to latest version Firefox latest version
MAC OSX (10.9) Java 7	Safari latest version Chrome latest version Firefox latest version	Safari latest version Chrome latest version	Not support	Firefox 45.0.x

2. [SPR: 100419034]

[Symptom]

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

L2TP VPN

1. Following are the table list for L2TP VPN supporting L2TP client and operating systems:

L2TP Client	OS type
Windows L2TP client	Windows 7 32/64 Windows 8 32/64 Windows 10 32/64
iPhone/iPAD L2TP client	iOS 8 latest Version iOS 9.latest Version
Android L2TP client	Google Phone
Mac L2TP client	X10.8.3

2. [SPR: N/A]

[Symptom]

L2TP connection will break sometimes with Android device. This issue comes from the L2TP Hollow packet will not by 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.

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)

MAC Authentication

1. [SPR: 150127103]

   [Symptom]

   Client use Internal MAC-Auth. connection Auth. Server can’t get IP successful.

   [Workaround]

   Set short ARP timeout value on monitored interface's switch and gateway side.

Wireless

1. [SPR: 150127103]
   [Symptom]
   MAC authentication use internal and auth. method set USG, wireless client can't get IP successful.

SecuExtender

1. Windows 7 users have not done Windows update before may have SecuExtender virtual Network interface card detection issue.
   [Workaround]
   Recommend installing all windows security patches before installing SecuExtender.
   One of reference: https://support.microsoft.com/en-us/kb/3033929

Known Issues:

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

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 successfully
2. [SPR: 140317624]
   [Symptom]
   DUT fails to fall back using primary WAN port when all DUT WAN's IP address were same subnet.
3. [SPR: 140818615]
   [Symptom]
   After Enable and Disable NAT rule, IPSec VPN traffic cannot forward to LAN subnet immediately.
   [Condition]
   1. Topology:
      PC1 ---LAN1 USG60W WAN1 ---- WAN1 USG60 LAN1 --- PC2 & PC3
   2. USG60W
      WAN1: 10.1.4.45/24
      WAN2: 192.168.9.x/24 (Can reach to 172.23.x.x network through NAT router.)
      LAN1: 192.168.181.x/24
      PC1: 192.168.181.33
   3. USG60
      WAN1: 10.1.6.79/24
      LAN1: 192.168.1.1/24
      PC2: 192.168.1.33
      PC3: 192.168.1.34
   4. USG60 sets a policy route, src=192.168.1.0/24, dst=172.0.0.0/8, next-hop=VPN tunnel
      USG60W sets
      1. policy route, src= 172.0.0.0/8, dst=192.168.1.0/24, next-hop=VPN tunnel
      2. policy route, src=192.168.1.0/24, dst=172.0.0.0/8, next-hop=WAN2
   5. PC2 ping 172.23.x.x is OK
   6. Add a 1:1NAT rule which is from WAN1 10.1.6.79 mapping to 192.168.1.34 (PC3) on USG60.

7. PC2 ping 172.23.x.x will fail now.
8. Disable 1:1 NAT rule.
9. PC2 still cannot ping to 172.23.x.x.
   *Need to reboot device or wait several minutes, it works.

4. [SPR: 141209575]
   [Symptom]
   IPSec VPN tunnel sometimes can be built up while initiator and responder devices use CA with the same subject name in IKE authentication. This tunnel should not be allowed to build.
5. [SPR: 160106369]
   [Symptom]
   To set up Local ID type in "DNS" mode at Advance setting under IPSec > VPN Gateway > Edit or Add page to make sure the Certificate works normally.
   [Workaround]
   If you are using certificate under the other modes, please go through VPN wizard then login again to VPN Gateway GUI page to modify the setting.

IPv6

1. [SPR: 131226738]
   [Symptom]
   Only one prefix delegation can be added in IPv6 address assignment.

App Patrol

1. [SPR: 140605136]
   [Symptom]
   [App Patrol]Cannot block Skype off-line message
2. [SPR: 160322066]
   [Symptom]
   Ultrasurf can't be blocked by App Patrol.

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: 121203072]

[Symptom]

Ext-group name and any password can login SSL VPN

3. [SPR: 160307230]

[Symptom]

If you use SecuExtender or Web GUI (SSL VPN) to login at same PC/Laptop, the pervious one will disconnect, i.e. SecuExtender will disconnect after Web GUI (SSLVPN) account login, vice versa.

4. [SPR: 160309776]

[Symptom]

GUI login can't auto connect/disconnect new SecuExtender tool in windows.

5. [SPR: 160324728]

[Symptom]

OWA (Outlook Web Access) will display incorrectly by using IE10.

System

1. [SPR: 130207529]

[Symptom]

When change SSH, Telnet and FTP Service default port, the connect session still exist.

2. [SPR: 150529308]

[Symptom]

Console sometimes display "XXX daemon dead" message during reboot.

3. [SPR: 160420343]

[Symptom]

USG310/1100/1900 and ZyWALL 310/1100 Interface up time counter will not reset after link down. For example, the ge1 port uptime shows 41 second and inactive ge1 port (link down). The next link up time should re-count from 00:00:00, but after link up, the uptime continues count from 41 second.

Anti-Virus

1. [SPR: 150522817]

[Symptom]

Upload Virus file by HTTP or Emails, the virus can be corrected detected and destroyed but the file name may be truncated in system log if the file name contains SPACE:' ', SEMICOLON: ';' or DOUBLE-QUOTE: '"'.

2. [SPR: 150603299]

[Symptom]

Virus-infected mail sent via IMAP protocol cannot be detected effectively.

3. [SPR: 160329211]

[Symptom]
Upload file with virus to Dropbox or Google Drive cannot be detected.

IDP

1. [SPR: 160329256]
   [Symptom]
   In custom UTM Profile > IDP > Custom Signatures > Payload option, if content have“[” word, GUI will show incorrect.

SSL Inspection

1. [SPR: 160620353]
   [Symptom]
   LAN PC cannot use management IP to access Device HA Pro backup device GUI when match SSL Inspection policy.
   [Workaround]
   Set up another security policy to bypass.

Wireless

1. [SPR: 150701137]
   [Symptom]
   Try to manage too many external APs over service/license count may cause capwap_srv daemon dead.
2. [SPR: 151119567]
   [Symptom]
   When AP firmware fails to synchronize with cloud server, alert log will display frequently
3. [SPR: 151208470]
   [Symptom]
   When AP firmware download failed from cloud server, exist AP firmware will be deleted and GUI show “to be downloaded” message at Configuration > Wireless >AP Management >Firmware page.
4. [SPR: 151203302]
   [Symptom]
   It takes 30 seconds or above to update the AP controller information when using ZyXEL Wireless Optimizer (ZWO) tool to monitor the status.

Web Auth

1. [SPR: 151125943]
   [Symptom]

After changing source address object name, LAN PC will not redirect to correct web portal.

AP

1. [SPR: 160603272]

   [Symptom]

   AP traffic Tx/Rx value show incorrectly in Email Daily Report.

Printer

1. [SPR: 160113511]

   [Symptom]

   If Printer is a DHCP Client and IP changed may cause Printer sync fail.

   [Workaround]

   Do “Printer Discover” again and to reserve IP

Easy Mode

1. [SPR: 160621418]

   [Symptom]

   Easy Mode user setup port forwarding to client HTTPS service list that will get message which shows “the HTTPS server port will change to 8443 on the USG” device; However, the HTTPS port will not change back from 8443 to 443 after delete the port forwarding rule.

GUI

1. [SPR: 151127016]

   [Symptom]

   The check box is overlapping with content text at Initial Wizard > Wireless setting page when using IE browser.

   [Workaround]

   Change another browser and restart Initial Wizard to set up wireless.

2. [SPR: 151208533]

   [Symptom]

   “Object Reference” cannot work at Configuration >Network> Interface > Ethernet > Edit IPv6 Configuration page.

3. [SPR: 151208561]

   [Symptom]

   GUI will not redirect to login page automatically after firmware upgrade by using Chrome browser.

4. [SPR: 151214778]

[Symptom]
After the IPv4 address object created by “Create New Object” there’s no updated IPv4 address object in IP address Pool list in Configuration > VPN >IPSec VPN >VPN connection >IPv4 Configuration > Add page.
[Workaround]
Close the “Add VPN Configuration” window and re-open again.

5. [SPR: 151217001]
[Symptom]
GUI always show “Loading…” message after apply below steps:
1. Apply system default configuration.
2. In[Configuration＞VPN＞IPSec VPN＞VPN Gateway]page, add one rule Enable, Name: ike1, interface: wan1 , static address: 10.1.4.x , pre-shared key:12345678
3. In[Configuration＞VPN＞IPSec VPN＞VPN Connection]page, add one rule
4. Enable, Name: ipsec1, site-to-site , VPN gateway : ike1, local policy: LAN1_subnet , remote policy: remote_subnet(use create new object-＞ IPv4 address, Name: remote_subnet, address type: subnet, network: 192.168.11.0 , netmask: 255.255.255.0)
5. In[Configuration＞VPN＞IPSec VPN＞VPN Gateway]page, edit ike1 rule
6. GUI always show “Loading…”.

[Workaround]
Refresh GUI

6. [SPR: 151223305]
[Symptom]
The changes of “E-mail Server 2”column will not applied after reboot device at Configuration > Log & Report > Log settings > System Log > Active Log and Alert (AP) page.

7. [SPR: 160411770]
[Symptom]
Go to Configuration > UTM Profile ＞ IDP ＞ Profile page, add a profile (e.g. name:2016USG) then back to the profile list select this rule and click “clone” you will find the background GUI profile name become the same as Clone Profile name before you apply.

8. [SPR: 160503266]
[Symptom]
It doesn't show logout IP after upgrade firmware to ZLD4.20.

Device-HA

1. [SPR: N/A]
[Symptom]

Device-HA can't sync. AP firmware to backup device.

[Workaround]

Go to Configuration > Wireless > AP Management > Firmware page, click "Check" and " Apply" button to manually download AP firmware for backup device.

Device-HA Pro

1. [SPR: 160226958]

   [Symptom]

   When the physical interface link down, the HTTP file downloading will terminate after failover to passive device.

2. [SPR: 160623509]

   [Symptom]

   Upgrade firmware from Active device and the upgrade process is to upgrade Passive device first. After Passive device finished firmware upgrade it will show device sync fail because of Active device is doing firmware upgrade and reboot.

3. [eITS: 160900786]

   [Symptom]

   When modify remote syslog setting by following steps the Device HA and Device HA Pro full configuration sync. will fail.

   Step 1: modify 2nd remote syslog setting

   Step 2: modify 1st remote syslog setting

IGMP

1. [SPR: 160802076]

   [Symptom]

   It should have system log when a client join or leave the IGMP member.

2. [SPR: 160804187]

   [Symptom]

   When playing IGMP streaming video, on the GUI > Monitor > System Status > Interface Status > Interface Statistics > "Tx B/s"/"Rx B/s" didn't show the IGMP traffic Tx/Rx B/s.

Features: V4.20(AAKZ.2)C0

Modifications in V4.20(AAKZ.2)C0 - 2016/11/25

1. [ENHANCEMENT] Add enhancement against ICMP type3 code3 DoS attack.

Features: V4.20(AAKZ.1)C0

Modifications in V4.20(AAKZ.1)C0 - 2016/09/29

1. [BUG FIX] eITS#160800705
   Guest wizard in easy mode gets wrong.
   1. enable the Guest network via wizard
   2. No IP address and DHCP server but port role is correct.
2. [BUG FIX] eITS#160800624
   The GeoIP can't update successfully, and shows 124014 error.
3. [BUG FIX] eITS#160800733
   When collecting diag-info by GUI and also in console, the device will reboot.
4. [BUG FIX] eITS#160800621
   USG will keep send out “R_U_THERE” even though the DPD is not checked.
5. [BUG FIX] eITS#160800900
   Unable to create a new VLAN.
   [Condition]
   When clicking the add button, loading screen hangs.
6. [BUG FIX] eITS#160800995, 160800977
   Upload firmware with a long filename, it will fail.
   [Condition]
   1. Go to file manager>firmware management
   2. Update a firmware with a filename more than length 31
   3. Update will fail.
7. [BUG FIX] eITS#160401060
   After few days, the mail sessions reach the maximum threshold and Anti-Spam stop working.
   [Condition]
   User select drop action of spam SMTP mail in Anti-Spam profile setting.
8. [BUG FIX] eITS#160800622
   IDP signature Link has wrong destination.
   [Condition]
   On the dashboard, you can click the signature ID on the GUI. The URL is wrong.
   Click GUI will pop-out
   https://onesecurity.com/pages/threat_info.php?virusid=1051723&type=policy
   But should be:
   https://onesecurity.zyxel.com/pages/threat_info.php?virusid=1051723&type=policy
9. [BUG FIX] eITS#160900521
   Firmware 4.20 - Every logged user is able to download "startup-config.conf"

10. [BUG FIX] eITS#160900525
    USG110 with CF and Safesearch random reboots
11. [BUG FIX] eITS#160900582
    When edit Anti-Virus rule, configuration change not writes correctly.
12. [BUG FIX] eITS#160900560
    When edit exist BWM rule, and disable “Maximize Bandwidth Usage” function. It not writes into configuration.
13. [BUG FIX] SPR#160801023
    Click “Configuration walk through” and “Troubleshooting” at NAT page, the link will display “Policy Route” information..

Features: V4.20(AAKZ.0)C0

Modifications in V4.20(AAKZ.1)C0 - 2016/07/20

1. [ENHANCEMENT]
   Easy Mode Support:
   (1) Only for USG40/40W/60/60W, USG20-VPN/20W-VPN

Supported Models
USG20-VPN, USG20W-VPN
USG40, USG40W
USG60, USG60W

   (2) Initial wizard pop-up when user first login in device under Easy Mode
   * Please be aware that Easy Mode is another user interface for different user market, it is not light version of Expert Mode. The changes made in Expert Mode may not be visualized correctly in Easy Mode.
   If you made changes in Expert Mode, we suggest staying in Expert Mode to ensure reliable configuration.
2. [ENHANCEMENT]
   Content Filter 2.0Support, more features add-on with the current Content Filter license.
   (1) HTTPS Domain Filter
   To block HTTPs web sites without deep inspection. Support on all models.
   (2) SafeSearch Enforcement
   To enforce safe search for the following search provides: Google, Bing, Yahoo, Yandex
   *Support on models with SSL inspection, USG110/ZyWALL110 or above.
   (3) Geo IP blocking
   Support IPv4/IPv6 geography type address object as the source or destination address of security policy.
   (4) Content Filter log enhancement; log all web access action with category information.
3. [ENHANCEMENT]
   Cloud Helper Support:
   (1) Auto check and show up the firmware download icon on dashboard and the release note information on firmware management page, if a new version is available.
   (2) Support pause/resume/stop action while running the online firmware download from cloud
   * Please note that you have to go to myZyXEL.com to register your device and activate firmware upgrade license and then to proceed the cloud firmware upgrade.
4. [ENHANCEMENT]
   IPSec VPN enhancement:
   (1) Route-based IPSec VPN - Static virtual tunnel interface for IPSec site-to-site VPN
   (2) Mode-config to assign IP address/DNS server/WINS server settings for IPSec client
   (3) IKEv2 VPN wizard

(4) IKEv2 configuration provisioning to ZyXEL IPSec Client

(5) IKEv2 support for Windows10

5. [ENHANCEMENT]

SSL VPN enhancement:

(1) Standalone SecuExtender client software for Windows

Please download the new SecuExtender client software from http://vpnclient.zyxel.com

(2) SSL VPN login page URL, https://<ip address>/ssl

(3) SSL VPN user portal behavior change,

- After login SSL VPN user portal, will not force logout even browser doesn't install Java Runtime
- After login SSL VPN user portal, will not auto download and install the SecuExtender client from device.

  Please download the new SecuExtender client software from http://vpnclient.zyxel.com
- After login SSL VPN user portal, will not bring up the SecuExtender. Please install and launch the new SecuExtender client on desktop.

6. [ENHANCEMENT]

Captive Portal authentication enhancement:

(1) Support Multiple Portal (max. 4 portals)

(2) Friendly captive portal page for mobile devices

(3) User agreement type authentication

(4) Support upload user customized captive portal page to USG/ZyWALL

- Max. 4 customized portal package (.zip) file can be upload
- Max. portal package (.zip) file size is 2MB (max. 5MB after unzip)

7. [ENHANCEMENT]

Hotspot enhancement:

(1) Hotspot license for USG/ZyWALL advance/extreme series

Support Hotspot Management Models
ZyWALL 310/1100
USG310/1100/1900

(2) Features support with Hotspot license

- Dynamic guest account
- Billing profiles (Time usage, Traffic usage, Bandwidth limitation)
- SP350E printer ticketing
- SMS ticketing with ViaNett
- Online tickets payment via PayPal
- Walled Garden
- IPnP

*Not support SP350E printer to connect on network of wan side.

*After add SP350E into the management list. The dynamic IP address of printer will auto

add into the DHCP reserve IP table.

8. [ENHANCEMENT]

Device HA Pro:

(1) Licensed feature

(2) Only support on ZW110/310/1100, USG110/210/310/1100/1900

Support Device HA Pro Models
ZyWALL 110/310/1100
USG110/210/310/1100/1900

(3) Dedicated port for heartbeat/synchronization between active and passive device

*The latest copper Ethernet port is the heartbeat port, if enable Device HA pro function

(4) Auto negotiation the device role (active or passive)

(5) Synchronization information

- Configuration
- License status
- AV/IDP/App signatures, GeoIP database
- Certificates
- Customized Captive portal pages
- zysh script files
- Login users information
- IPv4/IPv6 TCP sessions
- Static site-to-site IPSec SAs

*To avoid configuration conflicts, always make configuration changes on the active device

(6)Support firmware auto upgrade to passive device via GUI, FTP, Cloud Helper

* To avoid firmware inconsistent, always upgrade firmware from the active device

Limitation:

- Not support with IP/MAC binding feature
  If enable MAC Binding interface. After device failover, all the traffic of DHCP clients will be blocked by the active device until renew DHCP IP address.
- To change from HA Pro mode back to HA mode. Both devices need to reconfigure the HA settings.

9. [ENHANCEMENT]

Link Aggregation Group (LAG) interface

(1) Only support on the following models

Support Link Aggregation Group interface Models
ZyWALL 310/1100
USG310/1100/1900

(2) Max. LAG interface: 4; Max. ports in one LAG interface: 4

(3) Link Aggregation Mode support

- Active-Backup

- LACP 802.3ad (hash policy support: layer 2, layer 2+3)
- Balance-ALB (active-active path)

10. [ENHANCEMENT]
    Web GUI and SSL VPN login support TLS1.2
11. [ENHANCEMENT]

SSL Inspection enhancement :(*Support models USG110/ZyWALL110 or above)

(1) Support inspect TLS-1.1/TLS-1.2 connection with the following cipher

- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

(2)Support server downgrade TLS version while negotiation and implementation

12. [ENHANCEMENT]
    ADP enhancement:
    (1) Teardrop Attack detection and block
    (2) TCP Fragment detection and block
    (3) ICMP Fragment detection and block
    (4) IP Address Spoof detection and block
13. [ENHANCEMENT]
    Auto sync Time-Zone and Daylight-Saving from ZyXEL cloud server
14. [ENHANCEMENT]
    Support L2TP WAN connection type
15. [ENHANCEMENT]
    Support send RADIUS accounting data to external server
16. [ENHANCEMENT]
    Service redirect for HTTP and SMTP traffic
17. [ENHANCEMENT]
    DHCP clients table add leasing expiration time information
18. [ENHANCEMENT]
    Add DHCP clients table in daily report
19. [ENHANCEMENT]
    ZON utility support update location and system name
20. [ENHANCEMENT]
    Extend max. Concurrent SIP calls number

Model	Value
USG20-VPN/20W-VPN USG40/40W USG60/60W	50
USG110 /ZyWALL 110	100

USG210 USG310 / ZyWALL 310	
USG1100/ZyWALL 1100 USG1900	200

21. [ENHANCEMENT] Extend the Max. number of user create PPPoE interface

Model	Value
USG210	4 → 8
USG310 / ZyWALL 310	8 →16
USG1100/ USG1900 / ZyWALL 1100	16 → 32

22. [ENHANCEMENT]

New license: "Concurrent Device Upgrade" for extending the concurrent login devices.

Model	Value
USG110/210/ZyWALL 110	200→300 (extend by license)
USG310/ZyWALL 310	500→800 (extend by license)
USG1100/ZyWALL 1100	800→1500 (extend by license)
USG1900	1500→2000 (extend by license)

23. [ENHANCEMENT]

Feature behavior change:1:1 NAT port settings is hided on GUI

24. [ENHANCEMENT]"Use Static-Dynamic Route to Control 1-1 NAT Route" is enabled on system default setting.

25. [ENHANCEMENT]BEAST vulnerability mitigation

Support new CLI to disable TLS 1.0,

Router(config)# no ip http secure-server tlsv10

Router(config)# write

26. [BUG FIX] eITS#150700745

The customer is configured the Email Daily Report to send reports on a mail server that is located behind the IPSec-tunnel. Ping from the device to the mail server 192.168.5.15 successfully, but reports are not sent.

27. [BUG FIX] eITS#150801051

Top 5 viruses cannot be queried.

[Condition]

1. If clicking the Top 5 virus via dashboard, the URL cannot be downloaded successfully. It is because the URL is HTTPs. If changing it to HTTP, the explanation will show up.

28. [BUG FIX] eITS#150300296, 150900099

For eITS#150300296 and 150900099, enlarge the maximum number of the time period of connectivity check.

Was: The maximum number of the time period of connectivity check is 600 seconds

Is: The maximum number of the time period of connectivity check is 3600 seconds

29. [BUG FIX] eITS#150701032

Unable to build L2TP VPN. Connect hangs on checking account and is broken.

30. [BUG FIX] eITS#150900420

Edit the actions of some IDP rules from none to reject-both and save it, the actions become no instead of reject-both.

[Condition]

The issue can be easily reproduced with the following steps.

1. Create new IDP profile. Ex: Use wan base profile
2. Change the actions of some rules from none to reject-both and save it. Check these modified rules and user will find the actions are no instead of reject-both.
3. User needs to change the actions from no to reject-both again and save it.

31. [BUG FIX] eITS#150900398

After editing BWM rule, the error message pops up. Error Number: -37004 Error Message: 'System internal error. Internal application error.'

32. [BUG FIX] eITS#150600517

The Web GUI will be slow if edit VPN rule when device has configured 300 VPN connection rules.

[Condition]

There are 300 VPN tunnels. If Enable/Disable with 10 rules in the same time, the web GUI with hang.(VPN tunnel is not established yet)

33. [BUG FIX] eITS#150800872

ZySH daemon will dead when collect the diag-info file.

[Condition]

When issue happen GUI and console will not feasible to access and customer can only do power cycle to regain.

34. [BUG FIX] eITS#150901026

USG110 / L2TP fails user login

[Condition]

For the old accounts which were created before upgrading to WK37 firmware, L2TP tunnel can be established successfully; however, created some accounts after upgrading, L2TP will be failed due to incorrect username or password.

35. [BUG FIX] eITS#150600519

Solved “tunnel leak” issue when using a DDNS address in peer address.

36. [BUG FIX] eITS#150900987

USG1900 doesn't detect LTE dongle WLTUBA-107

37. [BUG FIX] eITS#150800739, 160400735

USG60W CPU random issue

[Condition]

The customer reported the CPU rate will be high, and the only recovery way is rebooting the USG. When the issue occurs, LAN users cannot access internet; however, the LAN users can communicate with each other.

38. [BUG FIX] eITS#151001056

    Moscow, Kazan, Volgograd is using GMT+3 (without daylight savings), but in settings of USG it is GMT+4.

39. [BUG FIX] eITS#150901015

    After rebooting the USG does not raise PPPoE automatically. The PPPoE could be connected if dial manually, but not automatically.

40. [BUG FIX] eITS#151000924

    The error message is wrong when adding wrong format URL in field.

    [Condition]

    Enter the complete URL of the site including "http://" on Trusted Web Site column in Content Filter. The pop out message shows "IPv6 subnet in CIDR format error". The URL seems not related to IPv6.

41. [BUG FIX] eITS#150701192

    ZyWALL series have IPSec VPN problem

    [Condition]

    Cannot establish VPN tunnel with Wlink device; however can connect successfully with downgrade firmware 3.2 on ZyWALL series.

42. [BUG FIX] eITS#150901170

    The L2TP tunnel will frequent disconnects.

43. [BUG FIX] eITS#151001230, 151100428

    Device reboot time to time

44. [BUG FIX] eITS#150800878

    Error IP format still saved into configuration by CLI command

45. [BUG FIX] eITS#150900889

    Solved IOP issue with Sophos UTM 9 Release 9.211-3.

46. [BUG FIX] eITS#151100824

    PPPoE Dial In issue with Nailed-Up

    [Condition]

    To enable nail-up in the PPPoE interface, and pressed disconnect button. Repeating the action around 8-20 times, nail-up will not work. The connection only can be established by press connect manually or reboot the device.

47. [BUG FIX] eITS#151101099

    Unable to access the console from web by using Java 8 update 51 or above (any browser). There is no problem with Java 8 update 45 and previous versions.

48. [BUG FIX] eITS#151200212

The DNS query will pass through by local NIC’s DNS address.(only happens on Win10)

49. [BUG FIX] eITS#151201300

USG210: Statefull Firewall does not work correctly for DNS over VPN

[Condition]

PC-------USG110========[VPN]========USG200

(1)PC's DNS IP is USG110's LAN1 interface.

(2)USG110 is establish VPN tunnel with USG200.

a. Add a domain zone forward: darkzone.local, IP: USG200's LAN1 interface

b.Disable default rule: From: IPSec VPN, To: ZyWALL, Action: allow. ->it means the traffic initiated from USG200 LAN site, the packets will hit default rule and drop.

(3)Add A record on USG200: ap.darkzone.local, IP: LAN subnet.

(4)Send DNS query for ap.darkzone.local from PC and cannot get IP for it.

50. [BUG FIX] eITS#151100310

Not possible delete VPN rules created by L2TP wizard

51. [BUG FIX] eITS#141001045

It shows incorrect expiration date of licenses on the GUI.

52. [BUG FIX] eITS#160100921

USG1100: SSL Inspection signs with SHA1

[Condition]

(1) Access https://www.google.ch without SSL Inspection activated and check the Google certificate == sha256 signed

(2) Activate SSL Inspection on USG1100 Firewall, use self-signed sha256 certificate on USG1100 for SSL Inspection configuration

(3) Access https://www.google.ch with SSL Inspection enabled ... no the Google certificate == sha1 signed

53. [BUG FIX] eITS#160100981

One wrong Russian translation

54. [BUG FIX] eITS#150800874

ZyWALL1100 DHCP relay offer is dropped.

[Condition]

The DHCP relay for unicast DHCP offer and ack (for apple's device) will be dropped.

55. [BUG FIX] eITS#151100489, 151000326, 151100898

USG Anti-Spam module Threshold flush not possible

[Condition]

Mails lost. (Mail session reached maximum 200/200 and never going down unless the device reboot)user has to modify the anti-spam behavior to let mail 'Forward' when mail scan reaches maximum in order to avoid mail lost.

56. [BUG FIX] eITS#160101287

The mail server can't receive mail from internet.

[Condition]

Device response "reached the maximum threshold of 200."

57. [BUG FIX] eITS#160200401, 160200399

SNMP port traffic does not work correctly

[Condition]

The customer use the network management software named PRTG (based on SNMP) and the port traffic doesn't work correctly.

The software will query SNMP to device every 60 seconds; however device will responds there is no traffic but will show the correct value after 5 minutes.

58. [BUG FIX] eITS#160300528

Auto Discovery from Office 365 doesn't work

[Condition]

When creating a new account in outlook, the auto-discover will fail when any UTM service has enabled.

59. [BUG FIX] eITS#160200111

Route Policy entry in packet flow is wrong

[Condition]

When creating policy route and set the specific service port in rule. In packet flow will shows incorrect and it will affect the site to site VPN routing.

60. [BUG FIX] eITS#160400165

USG310: ZySH daemon no response

[Condition]

After upgrade to the firmware to 4.15 patch 2, the ZySH daemon no response after 12.24hr.

61. [BUG FIX] eITS#150800388, 150800459

Proxy Cap SSH connection through USG

[Condition]

SSH daemon TCP forwarding does not work.

62. [BUG FIX] eITS#160101023

Traffic drop during the Device-HA synchronization

[Condition]

The RDP and cloud AP will disconnect during the Device-HA synchronization.

63. [BUG FIX] eITS#160200257

Remove the "DONT FRAGMENT BIT" from IP header of IKE packet for the MTU issue.

64. [BUG FIX] eITS#160400549

Device-HA sync failed

65. [BUG FIX] eITS#160500683

    Enhance DPD timer in IPSec PM and fix DPD handshaking twice issue.

66. [BUG FIX] eITS#160601226

    Memory leakage

67. [BUG FIX] eITS#160200037

    iOS client logout when trigger rekey.

    [Condition]

    (1) Setup a ikev2 VPN rule.

    IKE: AES256, SHA256, DH14

    IPSec: AES256, SHA256

    (2) Use iOS 9.3 to connect to DUT.

    (3) After 480 seconds, iOS rekey and then user logout.

68. [BUG FIX] eITS#160300715

    When CF is active no http/https traffic possible

Features: V4.15(AAKZ.2)C0

Modifications in V4.15(AAKZ.2)C0 - 2016/03/17

1. [ENHANCEMENT]APC 1.97

Support new AP model
WAC6103D-I
NWA5123-AC

2. [BUG FIX] eITS#160101036

   The AP images update incomplete randomly

Features: V4.15(AAKZ.1)C0

Modifications in V4.15(AAKZ.1)C0 - 2016/02/24

1. [ENHANCEMENT]Patch for Vulnerability CVE-2015-7547.

Features: V4.15(AAKZ.0)C0

Modifications in V4.15(AAKZ.0)C0 - 2015/12/31

1. [ENHANCEMENT]AP Firmware Cloud Update
2. [ENHANCEMENT]Force users to change password
3. [ENHANCEMENT]APC 1.95

Support new AP model
WAC6502D-E
WAC6502D-S
WAC6503D-S
WAC6553D-E
NWA5301-NJ

4. [ENHANCEMENT]Support generating SHA2 Certificate
5. [ENHANCEMENT]One Security Icon
6. [ENHANCEMENT]IPSec VPN Rule Number Parameters Change

Model	IPSec VPN Rule Number
USG40/40W	20
USG60/60W	40

7. [ENHANCEMENT]Max number of control AP Change

Model	Max number of control AP
USG40/40W/60/60W	18
USG110/ZW110/USG210/ZW310/USG310	34
ZW1100/USG1100/USG1900	66

8. [BUG FIX] eITS#150701258

   The customer configured wan1_ppp. In Ethernet ＞ wan1, he configured static IP with 0.0.0.0. (The modem issues IP 192.168.1.0/24, so he configures static IP as 0.0.0.0.)However, it shows 192.168.4.1 on the dashboard.

9. [BUG FIX] eITS#150701098

   When added external group user(RADIUS), and using space in group identifier, it will caused RADIUS daemon dead per 3 mins,

10. [BUG FIX] eITS#150700521

    The customer found out that the PPPoE is not able to connect while there's specific combination of characters in username ($ and @)

11. [BUG FIX] eITS#150700453

    Incorrect sorting in MONITOR＞UTM Statistics＞IDP＞Occurrence.

12. [BUG FIX] eITS#150700327

    If the DNS server of LAN PC is pointed to USG, the URL cannot be resolved. Via the console, the named is not existed.

13. [BUG FIX] eITS#150601043, 150701260

    Device HA status will keep Active-Fault-Active-Fault.

[Condition]

After enabling Device-HA, the VLAN client cannot pint to USG, and the Device-HA status is not stable.

14. [BUG FIX] eITS#150600669, 150601080

    Internal server error after attempts to log in to device web GUI.

15. [BUG FIX] eITS#150600524

    When Device HA activated. The Backup device syncs with Master device, the backup device will establishing VPN tunnel with remote site by management IP address.

16. [BUG FIX] eITS#150600517

    There are over 300 VPN rule in configuration. When configuring rule, the device will hanging.

17. [BUG FIX] eITS#150600437

    Deactivate VLAN interface before activate Device HA function. Then enable Device HA function. the PC still get IP address from VLAN interface again.

18. [BUG FIX] eITS#150600368

    The daily-report can't send success to specific ISP. Our SMTP TLS by default will use STARTTLS but Swisscom does not support STARTTLS.

19. [BUG FIX] eITS#150600248

    USG100: DHCP Daemon crash. Configure virtual service IP address on wrong Incoming interface let dhcp dead. To check IP address are Incoming interface subnet.

20. [BUG FIX] eITS#150600243

    Enhance the speed when switching the page between Application object and Application group. (this has been enhanced with DF 411AAKZ2ITS-WK28-2015-08-04-150600243.rar)

21. [BUG FIX] eITS#150600067

    USG100 dhcp server size > 254When configure DHCP server, to check each Interface to alert overlap Error.

22. [BUG FIX] eITS#150501127

    USG110 interface status while using trunk is wrong even though the connection is down, the wan1_ppp interface still shows alive.

23. [BUG FIX] eITS#150500830, 150701013

    When user login/logout from GUI, device will deletes exist TCP session.

24. [BUG FIX] eITS#150500671

    The device work fine for few days, but when symptom happening the device can't access to internet any more.(needs reboot device to recover it)

25. [BUG FIX] eITS#150500646

    Enabled SSL inspection function on the device, and work perfect with few days. When symptom happening, the HTTPs page will became very slower until can’t open any more. The symptom needs boot to resolve this situation.

26. [BUG FIX] eITS#150300227
    When authentication with WPA2-Enterprice to authentication with802.1X, the client can't authentication success.
27. [BUG FIX] eITS#150200529
    DHCPv6 DIUD length is too short compare to RFC definition.
28. [BUG FIX] eITS#150200167
    Ping virtual interface successfully even if the virtual interface is deleted.
29. [BUG FIX] eITS#150200142
    USG110 WPA2-enterprise for controlled ap not working when using ad as aaa-server.
30. [BUG FIX] eITS#150100917
    SNMP MIBs ifOperStatus and ifSpeed incorrect for port-grouping interface.
31. [BUG FIX] eITS#140900194
    When enable Anti-spam, client can’t receive the mail.
    [Condition]
    Disable zypktorder duplicated ACK send when AS mail inspection stage.
    (USG60 - Cannot get mails from external Mail server through USG)

Features: V4.13(AAKZ.1)C0

Modifications in V4.13(AAKZ.1)C0 - 2015/08/30

1. [BUGFIX]

   Some objects cannot be correctly added or removed by CloudCNM.

Features: V4.13(AAKZ.0)C0

Modifications in V4.13(AAKZ.0)C0 - 2015/08/15

1. [ENHANCEMENT]

   Management Feature Enhancement:

   1. Support CloudCNM, a cloud-based network management system. 4.13 CloudCNM feature support includes:
      - Batch import of managed devices at one time using one CSV file
      - See an overview of all managed devices and system information in one place
      - Monitor and manage devices
      - Install firmware to multiple devices of the same model at one time
      - Backup and restore device configuration
      - View the location of managed devices on a map
      - Receive notification for events and alarms, such as when a device goes down
      - Graphically monitor individual devices and see related statistics
      - Directly access a device for remote configuration
      - Create four types of administrators with different privileges
      - Perform Site-to-Site, Hub & Spoke, Fully-meshed and Remote Access VPN provisioning.
   2. Support Russian Language
   3. VPN MIB Support:eITS#150317956

      SNMP VPN status MIBs.

      The VPN status MIB is a MIB table containing the following information:
      - Connection name
      - VPN gateway
      - IP version
      - Active status
      - Connected status.

      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 counter MIBs.

The VPN connection counter MIB is a MIB group containing:

- Total VPN connection configured
- Number of activated connection
- Number of connected connection
- Number of disconnected connection

Followings are the example of snmpwalk for the added MIBs;

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

MIB table for VPN SA monitor

The new OID is 1.3.6.1.4.1.890.1.6.22.2.6.

The MIB table contains the following columns:

- 1.3.6.1.4.1.890.1.6.22.2.6.1.1 --> VPN connection index
- 1.3.6.1.4.1.890.1.6.22.2.6.1.2 --> VPN connection name
- 1.3.6.1.4.1.890.1.6.22.2.6.1.3 --> VPN connection policy
- 1.3.6.1.4.1.890.1.6.22.2.6.1.4 --> VPN connection uptime
- 1.3.6.1.4.1.890.1.6.22.2.6.1.5 --> VPN connection timeout
- 1.3.6.1.4.1.890.1.6.22.2.6.1.6 --> Number of in-bound packets for the connection
- 1.3.6.1.4.1.890.1.6.22.2.6.1.7 --> Number of in-bound octets for the connection
- 1.3.6.1.4.1.890.1.6.22.2.6.1.8 --> Number of out-bound packets for the connection
- 1.3.6.1.4.1.890.1.6.22.2.6.1.9 --> Number of out-bound octets for the

connection

4. Support license refresh immediately while device-ha backup device become active.
5. Add pre-defined configuration (or pre-defined UTM profile) by default.
6. Offering DHCP option 138 has been disabled by default.

2. [ENHANCEMENT]

   Connectivity Feature Enhancement:

   1. Support RPS(Receive Packet Steering) to ensure that packets for the same stream of data are sent to the same CPU, which could help to increase performance in a congest(low bandwidth or high latency) network environment, eITS#150200442, 150200636.
   2. We enlarge static DHCP host pool from 512 to 1024 for ZyWALL 1100, USG1100, and USG1900, eITS#150100773
   3. Adjust Spec for SSLVPN Connections

Model	Default SSLVPN Connections	Maximum SSLVPN Connections
USG40/40W	5	15
USG60/60W	5	20
USG110	25	150
USG210	35	150
USG310	50	150
USG1100	250	500
USG1900	250	750
ZyWALL 110	25	150
ZyWALL 310	50	150
ZyWALL 1100	250	500

3. [ENHANCEMENT]

   Security Feature Enhancement:

   1. ADP engine and IDP engine upgrade to support more social networking application behavior, such as FACEBOOK like, FACEBOOK share…etc.

4. [ENHANCEMENT] eITS#150200756

   UDP session timeout value can be configured up to 28800 seconds.

5. [ENHANCEMENT]

   Patches for CVE-2015-0204, FREAK: OpenSSL vulnerability.

6. [ENHANCEMENT]

   Patches for CVE-2015-4000, Logjam: TLS vulnerabilities (CVE-2015-4000).

7. [ENHANCEMENT]

   Patches for vulnerability of HTTP authentication module which may cause USG behave as an open proxy to proxy HTTP request from external clients to internal servers.

8. [ENHANCEMENT]

   Add CLI “no ip icmp-redirects” command to disable ICMP redirects manually.

9. [BUG FIX] eITS#150317956

[OID]OID formats are different between USG40W and USG1900.

[Condition]

MIBs...1.3.6.1.4.1.890.1.15.3.1.6.0.....

USG40W: V4.11(AALB.0)/1.01 | Aug 28 2013 14:19:07/2015-03-13 06:53:46

USG1900: V4.11(AAPL.0)/1.10/2015-03-13 01:27:44

10. [BUG FIX] eITS#150301008, 150701094

DNS Security configuration can't change.

[Condition]

1. Go to Configuration > System > DNS > Click Show Advanced Settings > Security Option Control > Edit default profile e.g. Query Recursion deny > Click OK button
2. You will find the OK button no function.

11. [BUG FIX] eITS#150300062

If adding radius server into auth. method, L2TP cannot be established successfully.

[Condition]

1. Go to Configuration > Object > AAA Server > RADIUS.
2. Set Server address: R1.domain.tw
3. Set Backup Server address: R2.domain.tw (PS. R1.domain.tw and R2.domain.tw need result same ip address)
4. Radiusd daemon couldn't bring on fail.

12. [BUG FIX] eITS#150300789

Combo-box show field is in wrong location.

[Condition]

1. In the settings of WLAN-interface, the input fields "802.11 band" and "Channel" are incorrectly positioned.
2. The problem occurs only in the browser IE 11

13. [BUG FIX] eITS#150300851

Limited admin user fails to view click diagnostic page

[Condition]

1. Add a limited admin account
2. Login by limited admin
3. Go to Maintenance > Diagnostic
4. You will find USG GUI no response

14. [BUG FIX] eITS#150300910, 150400430

DHCP Relay may not work in Device HA environment.

[Condition]

When master device change status from fault state to active state, the DHCP relay function may not work.

15. [BUG FIX] eITS#150400012, 150200484, 150500302, 150600123, 150301005, 150501020, 150301061

    In some cases, apply configuration will fail and cause zyshd dead. This may occur during the firmware upgrade progress or manually apply configuration.

16. [BUG FIX] eITS#150400115

    [SSO][Authentication]Without SSO enabled, user can be correctly authenticated and associated with the AD-group "Internet Users". However, with SSO enabled, the user from the AD-group "Internet Users" always appears only in the group of "ext-user (ad-users)".

17. [BUG FIX] eITS#150301062

    VLAN Packets can still be sent out even the base interface is disabled.

18. [BUG FIX] eITS#150300850

    Configure many static DHCP address up to maximum, the CLI command may not correctly be configured and cause “incomplete entry” error each time DUT reboot.

19. [BUG FIX] eITS#150401185

    In USG310, 1100, 1900, ZyWALL 310, 1100, it will show error message when configuring the port negotiation type on port 8.

20. [BUG FIX] eITS#150400882

    When trying to sort the table (Hits) of "Top 5 Viruses" and "Top 5 Intrusions" in Dashboard by descending/ascending, sorting is only by the first digit.

21. [BUG FIX] eITS#150500769

    Unable to edit application object page if it contains “,” character.

22. [BUG FIX] eITS#150300799, 150400336, 150401001, 150401067, 150401143, 150200666

    SSO does not work correctly sometimes.

23. [BUG FIX] eITS#150300240

    Unable to open IDP signature name to see the description in MONITOR > UTM Statistics > IDP

24. [BUG FIX] eITS#150200331

    Fix unexpected reboot related to packet processing.

25. [BUG FIX] eITS#140900194, 150600194, 150600840

    In some cases, user cannot get mails from external mail server through USG.

26. [BUG FIX] eITS#150200355

    When we set speed on port1, the traffic doesn't work and show some abnormal message.

27. [BUG FIX] eITS#150600082

    The CF report in monitoring page and report server record not match.

28. [BUG FIX] eITS#150600688

    In some cases, DUT will crash when trying to establish L2TP.

29. [BUG FIX] eITS#150501015

In some cases, enable connectivity check in policy route rules may cause zyshd daemon dead.

30. [BUG FIX] eITS#150600137
    In some cases, AV signature cannot be successfully updated.
31. [BUG FIX] eITS#150700094
    Self-Signed DSA certificate can be created but cannot show on the GUI.
32. [BUG FIX] eITS#150300324
    In USG110, USG210 and ZyWALL 110, DUT will become pure switch in a short period during booting process. When external AP and USG reboot at the same time, there might have possibility that AP will acquire IP address from outer DHCP server instead of DUT LAN DHCP server.
33. [BUG FIX] eITS#150600585
    Wrong German translation, “Intra-BSS-Verkehr aktivieren” should be corrected to “Intra-BSS-Verkehr blockieren”
34. [BUG FIX] eITS#150200663, 150500327
    Some mails with attached files transferred from WAN to LAN cannot be received while Anti-Spam enabled.
35. [BUG FIX] eITS#150100252, 150200029, 150200072, 150300445
    TFTP over IPSec cannot work well in the following topology.
    TFTP Server---------USG40/60=======VPNtunnel========USG20------TFTP Client
36. [BUG FIX] eITS#150100898
    After Device HA fallback to Master, IP on VLAN interface become 0.0.0.0.
37. [BUG FIX] eITS#150500371
    3G dongle E372 cannot work well in ZLD 4.11 Firmware.
38. [BUG FIX] eITS#150200205
    Some session will hit wrong BWM rules with application service type and application object is not any.
39. [BUG FIX] eITS#150200080
    ZyXEL VPN Client cannot establish VPN tunnel when using DUT default certificate to do IKE authentication.
40. [BUG FIX] eITS#141200576
    Fix the issue that 'Disconnect Connections Before Falling Back' cannot work.
41. [BUG FIX] eITS#140800138
    When setting Email Daily Report, strange log “msg="/USR/SBIN/CRON: (root) MAIL (mailed 369 bytes of output but got status 0x0001)” will dump in system log.

Features: V4.11(AAKZ.2)C0

Modifications in V4.11(AAKZ.2)C0 - 2015/04/28

1. [BUG FIX] eITS#150400012

   Apply configuration which has SSID "VLAN Support" may causes zyshd daemon dead and device cannot be managed any more. User must reset device to default for recovery.

Features: V4.11(AAKZ.1)C0

Modifications in V4.11(AAKZ.1)C0 - 2015/04/21

1. [BUG FIX] eITS#150301160
   Content Filter doesn't work at all after 4.11 upgrade.
2. [BUG FIX] eITS#150200801
   Radius daemon will fail to launch if the radius server (in AAA server) is configured with domain name and DNS is not ready during device boot-up.
3. [BUG FIX] eITS#150301005
   When SSID "VLAN Support" has been enabled, device will fail to load start-up config after reboot. User must reset device to default for recovery.

Features: V4.11(AAKZ.0)C0

Modifications in V4.11(AAKZ.0)C0 - 2015/03/12

1. [ENHANCEMENT]
   Management feature enhancement:
   1. ZON Utility Support (Device Discovery, Change Admin Password, Firmware Upgrade, Reboot Device, Web GUI Link)
   2. Smart Connect Support (Device Discovery, Web GUI Link)
2. [ENHANCEMENT]
   Connectivity feature enhancement:
   1. AP Controller Technology 1.9
   2. LTE dongle support
   3. VLAN 802.1P marking support
3. [ENHANCEMENT]
   Security feature enhancement:
   1. Antivirus white/black list
   2. Support ADP scan IPv6 traffic
   3. ADP block time period
   4. DNS security option control
   5. SNMPv3
   6. Add Reject Option in Security Policy
   7. Add AV EICAR Detect Option
   8. Add Action for untrusted cert chain of SSL Inspection
   9. SSL Inspection certificate support cloud update.
   10. UTM Performance Tuning #eITS141100375, 150100136, 150100251, 150200495
4. [ENHANCEMENT]
   Usability enhancement
   1. Wireless Initial Installation Wizard
   2. Network Diagnostic tools on GUI
   3. Security Policy Rules Filter & Clone
   4. UTM Profile Viewer
   5. Policy Route Rule Filter
   6. NAT rule support service group
   7. Dual image enhancement
   8. Multi-Lingual GUI
5. [ENHANCEMENT]
   VPN Feature Enhancement:
   1. L2TP/IPsec behind NAT.

6. [ENHANCEMENT] eITS#141100032
   Certificate support space character in the following field: Organizational Unit, Organization, Town, State (Province), Country.
7. [ENHANCEMENT] eITS#141000153
   Support GUI check box “Use Static-Dynamic Route to Control 1-1 NAT Route” to change routing order. Static-Dynamic Route has higher priority to 1-1 NAT Route when it is enabled.
8. [ENHANCEMENT]
   Patches for CVE-2015-0235, GHOST Vulnerability of glibc.
9. [FEATURE CHANGE]SPR#141007503
   AP Controller default configuration changed from “Always Accept” to “Manual” setting.
10. [FEATURE CHANGE]
    WAS:
    AV, CF, AS black and white list and IDP custom signature **DO NOT** work without license.
    IS:
    AV, CF, AS black and white list and IDP custom signature **DO** work even without license.
11. [FEATURE CHANGE]
    Enlarge Log Entry Size by each model
    WAS:
    For USG110/210/310/ and ZyWALL110/310: 512
    For USG1100/1900 and ZyWALL 1100: 512
    IS:
    For USG110/210/310/ and ZyWALL110/310: 1024
    For USG1100/1900 and ZyWALL 1100: 2048
    USG40/40W/60/60W keep log entry size as 512.
12. [BUG FIX]eITS#150200052
    Dynu DDNS cannot work
13. [BUG FIX] eITS#150100468, 140900136
    Not connected to zyshd daemon due to deadlock by sshipsecpm connectivity check.
14. [BUG FIX] eITS#141200823
    DUT cannot connect to SSO agent and output CLI command as below:
    Router# show sso agent status
    % connect failed
    % SSO: domain socket fial!
    ZySSO Primary Agent: offline
    ZySSO Secondary Agent: offline

15. [BUG FIX] eITS#150100588

    Apply configuration failed in the following steps:

    1. reset the device back to default
    2. Modify the WWW HTTPs port from 443 to 447, and some NAT and policy route rules.
    3. Download the startup.conf which with HTTPs port as 447.
    4. Change the startup.conf name as test_www and upload it.
    5. Apply test_www config.
    6. After device boot up, the device will fall back to default.

16. [BUG FIX] eITS#141100503

    Strange behavior when ZyWALL is in DNS proxy role.

    [Condition]

    1. Add zone forwarder 8.8.8.8 for zone * via WAN interface
    2. Add A-record for domain ftp.zanolari.net, IP 192.168.200.3
    3. On PC, ping www.zanolari.net
    4. Run CLI 'show ip dns server cache' and check www.zanolari.net is in DNS cache
    5. Capture packets on device for WAN interface and port 53 (DNS)
    6. On PC, run command 'ipconfig /flushdns' to flush DNS cache on PC, and then ping www.zanolari.net again
    7. From captured packets you will find device sends DNS query for www.zanolari.net even if it is found in device's DNS cache.

17. [BUG FIX] eITS#141200186, 150100084

    After enabling AS, the throughput is low.

18. [BUG FIX] eITS#141200341, 141200033

    Move the log “App ID has been changed from 83886594 to 83886855” to debug log.

19. [BUG FIX] eITS#141001029

    User cannot be configured in security policy rule with zone to zone rule from WAN to ZyWALL.

20. [BUG FIX] eITS#141100574

    After rebooting, WAN gateway will disappear.

21. [BUG FIX] eITS#141100745

    Device’s management IP cannot be reachable while Device HA status changed.

22. [BUG FIX] eITS#141000415

    The tunnel shows to be up in VPN Connections in both sides. However, no traffic can pass the tunnel and the log shows IPSec error with "no rule found, Dropping ESP packet".

23. [BUG FIX] eITS#141100945

    Device HA failed to synchronize backup device with master device.

24. [BUG FIX] eITS#141200132

The IP pool size cannot be varied with the changing of IP pool start address on GUI.
[Condition]

1. Default "IP Address" is 192.168.1.1 and "IP Pool Start Address" is 192.168.1.33. The maximum pool size value is 223.
2. Change the "IP Pool Start Address" to 192.168.1.60, the pool size should be 196 but it is still 223.

25. [BUG FIX] eITS#141100753
    Signature release date didn't display based on different time zone.
26. [BUG FIX] eITS#141100849
    Changing the firewall rule to deny traffic to ZyWALL but not take effect immediately.
27. [BUG FIX] eITS#141100177
    Building IPSec VPN tunnel with FortiGate, VPN tunnel cannot build after rekeying.
28. [BUG FIX] eITS#140800319
    Download files may get stuck when UTM is activated.
29. [BUG FIX] eITS#141100097
    Validation result of my certificate is failed.
30. [BUG FIX] eITS#141100402
    Packets are sending out in the wrong interface.
31. [BUG FIX] eITS#141001052
    Device has wrong or missing DNS cache record.
32. [BUG FIX] eITS#141000951
    When using for SHA256 as intermediate certificate, the certificate path will shows "incomplete path".
33. [BUG FIX] eITS#141000870, 141100240
    Rename a zone which has been used in Policy Control Rules will cause the zone field of these policy control rules cannot be changed or modified to other zones.
34. [BUG FIX] eITS#140900955
    [RIP]When setting RIP redistribute OSPF as metric=3, reboot DUT will show error message and cause applying startup configuration failed.
35. [BUG FIX] eITS#140926122
    [DHCPv6] When LAN interface set DHCPv6 client, it cannot send NS Packet.
36. [BUG FIX] eITS#140900251, SPR#140922847
    [File Manager]Rename configuration file to 64 characters will fail with wrong CLI command.
37. [BUG FIX] eITS#141000516
    [File Manager]Trying to download a file from download.microsoft.com or using the windows update service, in USG logs, IDP blocks the access
38. [BUG FIX] eITS#140900051

Route packets from a bridge interface according to the NAT result.

39. [BUG FIX] eITS#140900272

    Ge3 is configured as IP/MAC binding enabled. Disable interface any one of ge4 ~ ge8. The DHCP client of ge3 is unable to ping the default gateway anymore.

40. [BUG FIX] eITS#141100569

    [Interface]Routing didn't change even connective check failed.

41. [BUG FIX] eITS#150100603

    IPSec VPN daemon causes high memory usage(99%).

Features: V4.10(AAKZ.2)C0

Modifications in V4.10(AAKZ.2)C0 - 2014/12/03

1. [ENHANCEMENT]eITS#140600094
   Update driver to fix IOP issue with Genexis FiberXport device.
2. [ENHANCEMENT]
   Add CLI to show the mapping for internal and external interface. CLI: “debug interface show mapping”
3. [ENHANCEMENT]eITS#141000162
   Change log format as following:
   Before:
   category=”ipsec” level=”error” src=”” dst=”” msg=”Failed to send packet, err=N”N: 1 or 2
   After:
   category=”ipsec” level=”debug” src=”<source and port of packet>” dst=”<destination and port of packet>” msg=”Packet(PROTOCOL) cannot be sent, reason: REASON”
   PROTOCOL: ESP/AH/TCP/UDP/Unknown(protocol number)
   REASON: System dropped/Network congestion/Traffic control dropped
4. [ENHANCEMENT]
   Update bash binary for shellshock bash vulnerability issue
5. [ENHANCEMENT] eITS#140900846
   Support Huawei E303 USB 3G dongle with version 22.318.27.00.00
6. [ENHANCEMENT]
   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"

7. [ENHANCEMENT] eITS#140800801, 141000157
   Improve SMB performance
8. [ENHANCEMENT] eITS#141000576
   PPTP ALG support server in LAN scenario
9. [ENHANCEMENT]
   Add an interface at GUI to setting SSL Inspection policy for untrusted certificate chain
10. [ENHANCEMENT]
    Single Sign-on support authentication failover to web authentication. Note: With SSO Agent 1.0.4 or above.

    [Condition]

    When enable both Single Sign-on and Force User Authentication in web authentication policy. Once the Single Sign-On authentication fail, user will be redirect to web authentication login page as second authentication method.
11. [FEATURE CHANGE]eITS#141000788
    Turn off SSLV3 support in build-in service(HTTPs) by default due to Poodle vulnerability issue
12. [FEATURE CHANGE]eITS#141000154
    WAS: The columns "IKE Name" and "Cookies" showed on VPN Monitor
    IS: The columns "IKE Name" and "Cookies" are hidden on VPN Monitor by default.
13. [FEATURE CHANGE]

WAS: WLAN bind with lan1 by default

IS: WLAN bind with lan2 by default

14. [FEATURE CHANGE]

WAS:

Log entry is 256

IS:

Log entry is 512

PS: For ZyWALL 310 and USG310 only

15. [FEATURE CHANGE]

WAS:

IKE packet can be sent from any interface by routing even the packet's source IP doesn't match to the outgoing interface.

IS:

The IKE packet can only be sent from the interface bound the same IP with the packet's source IP.The above feature may cause some scenario of VPN establishment not work.

Please refer to KB:

http://kb.zyxel.com/KB/searchArticle!viewDetail.action?articleOid=014363&lang=EN

16. [BUG FIX] eITS#140900194

User cannot get mail from external mail server through USG due to duplicate ACK packet.

17. [BUG FIX] eITS#140800834

USG with wrong CEF syslog format

18. [BUG FIX] eITS#140800642

Device HA status not changed when monitored interface IP changed

19. [BUG FIX] eITS#141000158

SSLVPN reverse proxy RDP cannot work

20. [BUG FIX] eITS#140900380

USG1100 / L2TP can't login user and with crazy log message

21. [BUG FIX] eITS#141000460, 141000461, 141000462

Static ARP entry will gone if enabling device HA

22. [BUG FIX] eITS#141000171

USG bootup makes switch function("Loop Guard") blocking port

23. [BUG FIX] eITS#141000157

False alarm in CAPWAP protocol in ADP engine

24. [BUG FIX] eITS#141000155

IKE packet sent at wrong interface and wrong IP

25. [BUG FIX] eITS#141000458

DHCP will clear static ARP entry after send DHCP ACK

26. [BUG FIX] eITS#141001108

USG110 cannot load Firmware if USB memory stick connected

27. [BUG FIX] eITS#140800642, SPR#140714684, 140804120, 141103007

    ZyWALL 1100 - VPN connect fail and hang

28. [BUG FIX] eITS#140700610, 141000163, SPR#140909287

    After device boot up, the log will show that the DHCP packets have been dropped by default firewall rule. However, WAN interface still gets the IP address from DHCP server.

Features: V4.10(AAKZ.1)C0

Modifications in V4.10(AAKZ.1)C0 - 2014/10/01

Release for manufacturing

Features: V4.10(AAKZ.0)C0

Modifications in V4.10(AAKZ.0)C0 - 2014/08/22

First release

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/USG 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 in a file that (usually) uses the system model name with a .bin extension, for example, "420AAKZ2C0.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/USG 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/USG.
   - Router>**enable**
   - Router#**configure terminal**
   - Router(config)#**setenv-startup stop-on-error off**
   - Router(config)#**write**
   - Load the older firmware to ZyWALL/USG using standard firmware upload procedure.
   - After system uploads and boot-up successfully, login into ZyWALL/USG 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:
   - Use Console/Telnet/SSH to login into ZyWALL/USG.
   - Router>**enable**
   - Router#**configure terminal**
   - Router(config)#**setenv-startup stop-on-error off**
   - Router(config)#**write**
   - Load the older firmware to ZyWALL/USG using standard firmware upload procedure.
   - After system upload and boot-up successfully, login into ZyWALL/USG via Console/Telnet/SSH.
   - Router>**enable**
   - Router#**write**

Now the system is successfully downgraded to older version.

Note: ZyWALL/USG 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/USG platform status. If user wants to use this feature, you must prepare the following step:

1. Have ZyWALL/USG mib files(**420AAKZ2C0-enterprise.mib** and **420AAKZ2C0-private.mib**) and install to your MIBs application (like MIB-browser).You can see 410AAPJ2C0-private.mib (OLD is 1.3.6.1.4.1.890.1.6.22).
2. ZyWALL/USG SNMP is enabled.
3. Using your MIBs application connects to ZyWALL/USG.
4. SNMPv2 private MIBs support three kinds of status in ZyWALL/USG:
    1. CPU usage: Device CPU loading (%)
    2. Memory usage: Device RAM usage (%)
    3. VPN IPSec Total Throughput: The VPN total throughput (Bytes/s), Total means all packets(Tx + Rx) through VPN.

Appendix 3. Firmware Recovery

In some rare situation(symptom as following), ZyWALL/USG 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/USG.

1. Symptom:
   - Booting success but device show error message “can’t get kernel image” while device boot.

```
U-Boot 2011.03 (Development build, svnversion: u-boot:422M, exec:exported)
 (Build time: Feb 21 2013 - 10:15:57)


BootModule Version: V1.07 | 02/21/2013 10:45:46
DRAM: Size = 2048 Mbytes

Press any key to enter debug mode within 3 seconds.
.....................................................
Wrong Image Format for bootm command
ERROR: can’t get kernel image!
Start to check file system...
```

   - Device reboot infinitely.

```
U-Boot 2011.03 (Development build, svnversion: u-boot:422M, exec:exported)
 (Build time: Feb 21 2013 - 10:15:57)


BootModule Version: V1.07 | 02/21/2013 10:45:46
DRAM: Size = 2048 Mbytes

Press any key to enter debug mode within 3 seconds.
.....................................................
U-Boot 2011.03 (Development build, svnversion: u-boot:422M, exec:exported)
 (Build time: Feb 21 2013 - 10:15:57)


BootModule Version: V1.07 | 02/21/2013 10:45:46
DRAM: Size = 2048 Mbytes

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

   - Nothing displays after “Press any key to enter debug mode within 3 seconds.” for more than1 minute.

```
U-Boot 2011.03 (Development build, svnversion: u-boot:422M, exec:exported)
 (Build time: Feb 21 2013 - 10:15:57)


BootModule Version: V1.07 | 02/21/2013 10:45:46
DRAM: Size = 2048 Mbytes

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

   - Startup message displays “Invalid Recovery Image”.

```
U-Boot 2011.03 (Development build, svnversion: u-boot:422M, exec:exported)
 (Build time: Feb 21 2013 - 10:15:57)


BootModule Version: V1.07 | 02/21/2013 10:45:46
DRAM: Size = 2048 Mbytes

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




Invalid Recovery Image

ERROR

EnterDebug Mode

ZW1100>
```

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

```
Invalid Firmware!!!

ERROR
```

2. Recover steps
   - Press any key to enter debug mode

```
U-Boot 2011.03 (Development build, svnversion: u-boot:422M, exec:exported)
 (Build time: Feb 21 2013 - 10:15:57)


BootModule Version: V1.07 | 02/21/2013 10:45:46
DRAM: Size = 2048 Mbytes

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

EnterDebug Mode

ZW1100>
```

   - Enter atkz –f –l 192.168.1.1 to configure FTP server IP address

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

   - Enter atgof to bring up the FTP server on port 1

```
ZyWALL 1100> atgof

Booting...
```

   - The following information shows the FTP service is up and ready to receive FW

```
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 update 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/USG's IP addresses, your computer must use a static IP address in this range to recover the firmware.
- Connect your computer to the ZyWALL/USG'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/USG. This example uses the ftp command in the Windows command prompt. The ZyWALL/USG'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/USG (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 5001
226-944.6 Mbytes free disk space
226-File successfully transferred
226 5.540 seconds (measured here), 9.32 Mbytes per second
ftp: 54141580 bytes sent in 5.55Seconds 9760.52Kbytes/sec.
ftp>
```

- The console session displays "Firmware received" after the FTP file transfer is complete. Then you need to wait while the ZyWALL/USG 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/USG automatically restarts.

```
.....
.....
.....
.....
.....
.....
.....
       done

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

- The username prompt displays after the ZyWALL/USG starts up successfully. The firmware recovery process is now complete and the ZyWALL/USG is ready to use.

```
U-Boot 2011.03 (Development build, svnversion: u-boot:422M, exec:exported)
 (Build time: Feb 21 2013 - 10:15:57)


BootModule Version: V1.07 | 02/21/2013 10:45:46
DRAM: Size = 2048 Mbytes

Press any key to enter debug mode within 3 seconds.
.....
Start to check file system...
/dev/sda3: 33/20480 files (0.0% non-contiguous), 57481/81920 blocks
/dev/sda4: 97/23040 files (1.0% non-contiguous), 7623/92160 blocks
Done

INIT: version 2.86 booting
Initializing Debug Account Authentication Seed (DAAS)... done.
Setting the System Clock using the Hardware Clock as reference...System Cl
ock set. Local time: Tue May 28 08:54:07 GMT 2013

INIT: Entering runlevel: 3
Starting zylog daemon: zylogd zylog starts.
Starting syslog-ng.
Starting ZLD Wrapper Daemon....
Starting uam daemon.
Starting periodic command scheduler: cron.
Start ZyWALL system daemon....
.....
Got LINK_CHANGE
.....
Got LINK_CHANGE
Port [1] Copper is up --> Group [1] is up
.....Applying system configuration file, please
 wait...
no startup-config.conf file, Applying system-default.conf
Use system default configuration file (system-default.conf)
ZyWALL system is configured successfully with system-default.conf

Welcome to ZyWALL 1100

Username:
```

- 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/USG for further analysis.
  - 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 configuration file, system configuration stop!!