ZYXEL

Firmware Release Note

USG60W

Release V4.63(AAKZ.0)C0

Date: Jun 15 2021
Author: Bert Li
Project Leader: Jacky Lin

Contents

ZYXEL USG60W

Release V4.63(AAKZ.0)C0

Release Note

Date: Jun 15 2021

Supported Platforms:

ZYXEL USG60W

Versions:

ZLD Version: V4.63(AAKZ.0) | 2021-06-10 13:36:28

Files lists contains in the Release ZIP file

File name: 463AAKZ0C0.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: 463AAKZ0C0.conf
Purpose: This ASCII file contains default system configuration commands.

File name: 463AAKZ0C0.pdf
Purpose: This release file.

File name: 463AAKZ0C0.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: 463AAKZ0C0-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: ZYXEL-ZW-SMI.MIB, ZYXEL-ZW-COMMON.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: 463AAKZ0C0-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.
   - For new model, requires connecting to myZyxel to complete device registration and Security Service activation.
2. **FIRMWARE UPGRADE NOTICE:**
   Before doing firmware upgrade, please check your Firmware version and Configuration if met following condition.
   You may encounter device freeze, after upgrading firmware to any newer version.
   Cold start (power off/on the device) **is a MUST** to complete the firmware upgrade.

[Condition] Configured FQDN Address Object before and with following Firmware version:

ZLD4.39, ZLD4.39 week32

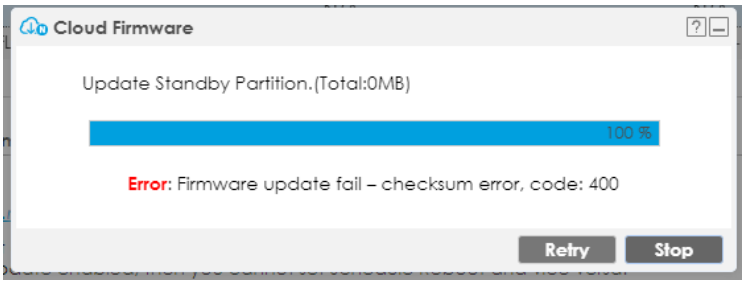
ZLD4.38 week26, ZLD4.38 week30

[Symptom]

The firmware listed above is subject to a bug. When FQDN address object is created and used in the system configuration, the device will hang after upgrading firmware to any newer version. However, if the device is running firmware version that is not listed above, then your device is immune from this symptom. **Lastly, if you didn't configure FQDN address object**, then your **device is immune** from this symptom, regardless of the running firmware version.

[Caution]

1. Please do **backup** your device **configuration** before upgrading firmware.
2. Please be reminded that **Cold start** (power off/on the device) **is a MUST** to complete the firmware upgrade.
3. Checksum error can be ignored while pressing "Upgrade Now" button.



3. Recommended upgrade to ZLD4.38 Patch0 or later version first before upgrading to ZLD4.62.
4. 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.
5. Downgrading to previous firmware versions results in configuration loss and apply configure failure.
   Before downgrading please:
   (1) Back up current "startup-config.conf" file
   (2) Perform the downgrading
   (3) Reset to default
   (4) Upload and apply the previous firmware versions backup configuration.
6. If user upgrades from previous released firmware to this version, there is no need to restore to system default configuration.

7. 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.
8. Firefox will start with the last position that user leaves the page of Terms of Use last time. It is its user-friendly behavior.
9. When changing the language combo box of Terms of Use to get new PDF, sometimes the PDF could be refreshed fail with browser Firefox. Suggest that clear browser's cache when the case occurs.
10. 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.
11. If ZyWALL/USG can't reboot successfully after firmware upgrade, please refer to Appendix 3: Firmware Recovery.
12. If you use a WK-Version, please contact local Support Team for Upgrade Information.
13. [APC] AP image list

APC version	ZLD version	NXC version	Cloud External AP	Support AP (Managed AP)	Forward Compatible AP
APC3.60	ZLD4.63	NXC 6.10 Patch2	6.20P0C0 6.10P10C0 5.10P3C0 5.10P10C0 5.02P3C0	NWA3160-N(5.10P3C0) NWA3550-N(5.10P3C0) NWA3560-N(5.10P3C0) NWA5160N(5.10P3C0) NWA5550-N(5.10P3C0) NWA5560-N(5.10P3C0) NWA5121-NI(5.10P10C0) NWA5123-NI(5.10P10C0) NWA5121-N(5.10P10C0) NWA5301-NJ(5.10P10C0) WAC6502D-E(6.20P0C0) WAC6502D-S(6.20P0C0) WAC6503D-S(6.20P0C0) WAC6553D-E(6.20P0C0) WAC6552D-S(6.20P0C0) WAC6103D-I(6.20P0C0) NWA5123-AC(6.10P10C0) NWA5123-AC-HD(6.20P0C0) WAC5302D-S(6.10P10C0) WAC6303D-S(6.20P0C0) WAX650S(6.20P0C0) WAX510D(6.20P0C00) WAX610D(6.20P0C0) WAC500(6.20P0C0)	WNA4320v2(5.02P3C0) WNA4320v3(5.02P3C0) WNA4320(5.02P3C0)

				WAC500H(6.20P0C0) WAC5302D-Sv2(6.20P0C0)	

Design Limitations:

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

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 50001/10443/10444/1723/2601-2604/2158/53/179. Users should avoid using these internal ports for built-in services.
   [Workaround]
   Users should avoid using these internal ports for built-in services.

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.

DNS

1. [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 denying.

GUI

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

Operating System	For Administrator Login Browsers	For User Login Browsers
Windows 7 (X64) (SP1)	Internet Explorer 10.x, 11.0.9600.17843	Internet Explorer 10.x, 11.0.9600.17843

	Chrome 59.0.3071.115	Chrome 59.0.3071.115
	Firefox 54.0.1	Firefox 54.0.1
	Opera 46.0.2597.46	Opera 46.0.2597.46
	Safari 5.1.7(7534.57.2)	Safari 5.1.7(7534.57.2)
Windows 8.1 (X64)	Internet Explorer 10.x, 11.0.9600.16384	Internet Explorer 10.x, 11.0.9600.16384
	Chrome 59.0.3071.115	Chrome 59.0.3071.115
	Firefox 54.0.1	Firefox 54.0.1
	Opera 46.0.2597.46	Opera 46.0.2597.46
	Safari 5.1.7(7534.57.2)	Safari 5.1.7(7534.57.2)
Windows 8.1 (X32)	Internet Explorer 10.x, 11.0.9600.16384	Internet Explorer 10.x, 11.0.9600.16384
	Chrome 59.0.3071.115	Chrome 59.0.3071.115
	Firefox 54.0.1	Firefox 54.0.1
	Opera 46.0.2597.46	Opera 46.0.2597.46
	Safari 5.1.7(7534.57.2)	Safari 5.1.7(7534.57.2)
Windows 10 (X64)	Internet Explorer 11.0.10240.16683	Internet Explorer 11.0.10240.16683
	Chrome 59.0.3071.115	Chrome 59.0.3071.115
	Firefox 54.0.1	Firefox 54.0.1
	Opera 46.0.2597.46	Opera 46.0.2597.46
	Safari 5.1.7(7534.57.2)	Safari 5.1.7(7534.57.2)
	Edge 20.10240.16384.0	Edge 20.10240.16384.0
Linux OS (Ubuntu)	Firefox 50.0.2	Firefox 50.0.2
	Opera 47.0.2631.55	Opera 47.0.2631.55
Apple MAC OS X	Chrome latest version 60.0.3112.101	Chrome latest version 60.0.3112.101
	Safari latest version 10.1.2(12603.3.8)	Safari latest version 10.1.2(12603.3.8)
	Firefox latest version 50.0.2	Firefox latest version 50.0.2
Apple iOS (Tablet)	9 latest version 9.3.3 (Safari)	Safari 9 latest version 9.3.3
	10 latest version 10.3.2 (Safari)	Safari10 latest version 10.3.2
Android (Tablet)	latest version 5.0 (Chrome)	latest version 5.0 (Chrome)

* Not support Opera browser 10.6x
* Not support Mobile OS

2. [SPR: 171030438]
   [Symptom]
   IE browser will download the privacy statement when accessing the related page, instead of reading on browser.

Interface

1. [SPR: 170628894]
   [Symptom]
   [LAG] The active slave may always switch to each other between ge1

and ge2 with active-backup mode and link-monitoring method is ARP.

[Workaround]

Suggest using MII monitoring method.

IPSec VPN

1. [SPR: 070814168]

   [Symptom]

   VPN tunnel could not be established when:

   a. a non ZyWALL/USG peer gateway reboot and
   b. 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]

   a. Prepare 2 ZyWALL/USG and reset to factory default configuration on both ZyWALL/USGs
   b. On ZyWALL/USG-A:
      - Create 2 WAN interfaces and configure WAN1 as DHCP Client
      - Create 2 VPN Gateways. The "My Address" is configured as Interface type and select WAN1 and WAN2 respectively
      - Create 2 VPN Connections named VPN-A and VPN-B accordingly which bind on the VPN Gateways we just created
   c. On ZyWALL/USG-B
      - Create one WAN interface
      - 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
   d. Connect the VPN tunnel from ZyWALL/USG-B to ZyWALL/USG-A and we can see VPN-A is connected on ZyWALL/USG-A
   e. Unplug WAN1 cable on ZyWALL/USG-A

f. After DPD triggered on ZyWALL/USG-B, the VPN Connection will be established again
g. 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 by 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:
a. IPv4 rules with IKEv2 version
b. IPv4 rules with User-based PSK authentication

SSL VPN

1. Following are the list for SSL VPN supporting applications and operating systems:
- SecuExtender SSL VPN Client support : Windows 7/8/10 and Mac OS 10.12.2
- Chrome, Firefox, Opera Browsers are not support JAVA since Sept. 2017

Applications / Operating System	Reverse Proxy Mode: File Sharing(Web-based Application)	RDP	VNC
Windows 7 (X64) (SP1) Java 7u45/ 8u111 or later	Internet Explorer 10.x, 11.x	Internet Explorer 10.x, 11.x	Internet Explorer 10.x, 11.x
Windows 7 (X32) (SP1) Java 7u45/ 8u111 or later	Internet Explorer 10.x, 11.x	Internet Explorer 10.x, 11.x	Internet Explorer 10.x, 11.x

Windows 8, 8.1 (X64) Java 7u45/ 8u111 or later	Internet Explorer 10.x, 11.x	Internet Explorer 10.x, 11.x	Internet Explorer 10.x, 11.x
Windows 8, 8.1 (X32) Java 7u45/ 8u111 or later	Internet Explorer 10.x, 11.x	Internet Explorer 10.x, 11.x	Internet Explorer 10.x, 11.x
Windows 10 (X64) Java 7u45/ 8u111 or later	Internet Explorer 11.x	Internet Explorer 11.x	Internet Explorer 11.x
MAC OSX (10.12.2)	Safari latest version Chrome latest version	Not support	Not Support

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 14
Android L2TP client	Google Phone
MacOS L2TP client	MacOS 10.15.5

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 pops up a logout message. (HTTP redirect to HTTPS must enable)

Anti-Spam

1. Not support SMTPs , STARTTLS, POP3s, SMTP Extension command – BDAT

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.

SecuExtender SSL VPN Client

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: 140818615]
   [Symptom]
   After Enable and Disable NAT rule, IPSec VPN traffic cannot forward to LAN subnet immediately.
   [Condition]
   a. Topology:
      PC1 ---LAN1 USG60W WAN1 ---- WAN1 USG60 LAN1 --- PC2 & PC3
   b. 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
   c. USG60
      WAN1: 10.1.6.79/24
      LAN1: 192.168.1.1/24
      PC2: 192.168.1.33
      PC3: 192.168.1.34
   d. 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
   e. PC2 ping 172.23.x.x is OK
   f. Add a 1:1NAT rule which is from WAN1 10.1.6.79 mapping to 192.168.1.34 (PC3) on USG60.

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

3. [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.
4. [SPR: 190411087]
[Symptom]
It may take too much time to setup IPsec VPN tunnel with DH18 of key group
5. [eITS: 201100335][174827]
[Symptom]
ATP200 / IKE v2 Proposal mix not working (DH16, DH17, DH18).

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.
3. [SPR: 170317753]
[Symptom]
[App Patrol][LOG] Log of FTP App Patrol was different with previous signature version
4. [SPR: 180509277]
[Symptom]
Use Chrome can't reject/drop the social networks "Facebook" application.
5. [SPR: 180517532]

[Symptom]
Can't drop & reject "Yahoo mail" application and no logs.

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: 160309776]
   [Symptom]
   GUI login can't auto connect/disconnect new SecuExtender tool in windows.
3. [SPR: 160324728]
   [Symptom]
   OWA (Outlook Web Access) will display incorrectly by using IE10.
4. [SPR: 170830303]
   [Symptom]
   File sharing and reverse proxy mode with Google Chrome may not work.
   [Workaround]
   You can use other kinds of browsers.
5. [SPR: 170517424]
   [Symptom]
   SecuExtender after ZLD4.30 will not support Windows XP due to strong cipher suite activated by default. Please upgrade client OS or allow ZLD with unsecure cipher suite via CLI, "no ip http secure-server strong-cipher".

System

1. [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.
4. [SPR: 170210431]
   [Symptom]
   Use Thunderbird to be a mail client send virus mail (SMTP), UTM cannot detect virus, but virus can be detected when mail client exchange to MultiMail (SMTP).
5. [SPR: 161019640]
   [Symptom]
   Anti-virus cannot detect uuencode eicar virus

IDP

1. [SPR: 170919289]
   [Symptom]
   When adding an IDP Profile and click “Search” button will cause GUI hang or take a long time to display the result by IE browser.

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.
5. [SPR: 170830306]
   [Symptom]
   [Station info] When client from 2.4G Wi-Fi to 5G Wi-Fi, the station info will show client connect to 2.4G Wi-Fi
6. [Symptom]
   AP Firmware update will fail when using FTP
   [Solution]
   Please use CAPWAP to update AP firmware.

Web Auth

1. [SPR: 161215730]
   [Symptom]
   [Billing] Guest B (Custom Fix IP) using same IP with Guest A and can access internet.

AP

1. [SPR: 160603272]
   [Symptom]
   AP traffic Tx/Rx value show incorrectly in Email Daily Report.

GUI

1. [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.
2. [SPR: 160503266]
   [Symptom]

It doesn't show logout IP after upgrade firmware to ZLD4.20.

3. [SPR: 170328262]
   [Symptom]
   Network risk warning information show null on ZyWALL series device
4. [SPR: 171016187]
   [Symptom]
   Easy mode ＞ click Network Client list button may cause page always loading status
5. [eITS: 170300826]
   [Symptom]
   With feature “Link Aggregation Group”, it no longer provide the field “none” on link-monitoring, balanced-alb and active-backup due to useless.
6. [SPR: 190329412]
   [Symptom]
   [GUI] When PC login admin then login user，admin user have some page always was loading.
7. [SPR: 190329413]
   [Symptom]
   [GUI] After remove policy route rule, routing table still has this rule.
8. [SPR: 200921563]
   [Symptom]
   When the certificate with '<' symbol, the domain name column at SSL Inspection > Exclude List page will be empty.
9. [SPR: N/A]
   [Symptom]
   Sometimes GDPR dialog will be blocked by device dashboard loading mask. Please move the dialog to usable place for advanced operations or wait for the loading mask finished.
10. [SPR: N/A]
    [Symptom]
    GUI displays wrong firmware version, for example 4.35(VVVV.0)/4.35(WWWW.0)/4.35(ZZZZ.0)/4.35(YYYY.0), if uploaded ZLD4.35 or above firmware to standby partition without reboot.
    It’ll auto recover after reboot device.
11. [SPR: 201027300]
    [Symptom]

[MAC Address] Add MAC Address GUI pop-up CLI error message.
[Workaround]Please use CLI to add rules for example "mac-auth database mac aa-aa-aa-aa-aa-aa type int-mac-address mac-role mac-users".

3G Dongle

1. [SPR: 161215667]
   [Symptom]
   Budget set only download, action upload still has budget logs.

Remote Access VPN wizard

1. [Symptom]
   When IP address pool subnet is not /24 it will conflicts with VLAN interface and will not auto change IP pool subnet.
   [Workaround]
   Manually change the IP pool in the Remote Access VPN Wizard.

PCI

1. [eITS: 201001082]
   [Symptom]
   PCI Compliance failure by package issue.

2FA

1. [eITS: 201100207] [174411]
   [Symptom]
   Unable to enable Two-Factor Authentication when "Allowed_User" is empty.
2. [eITS: 201100916]
   [Symptom]
   Remote User cannot login with 2FA.

BWM

1. [eITS: 201101282]
   [Symptom]
   BWM rules not working after reboot on USG20-VPN/40(W)/60(W).

Features: V4.63(AAKZ.0)C0

Modifications in V4.63(AAKZ.0)C0 - 2021/06/15

1. [ENHANCEMENT] eITS#210300954
   a. Anti-Spam email header support character "=".
2. [ENHANCEMENT] Supported AP image upgrade to 6.20p0c0.
3. [ENHANCEMENT] Change AP Controller secret key design.
4. [ENHANCEMENT] Fine tune AP controller system log.
5. [Vulnerability Fix] [CVE-2020-1971]
   a. Fix: OpenSSL Vulnerability.
6. [Vulnerability Fix] [CVE-2016-2776]
   a. Fix: Assertion Failure in buffer.c While Building Responses to a Specifically Constructed Request.
7. [Vulnerability Fix] Add sanity check on CRLF to prevent cross-site scripting attack. (Acknowledgement Soter IT Security)
8. [BUG FIX] eITS#200801449
   a. Fix: Content Filter malfunctioning occasionally.
9. [BUG FIX] eITS#201001362
   a. Fix: Policy route malfunctioning in specific conditions.
10. [BUG FIX] eITS#201200879
    a. LAN Port provisioning issue with new AP models: WAC500H and WAC5302D-Sv2.
11. [BUG FIX] eITS#210100807
    a. Fix: When add new MAC address profile, the GUI will pop-up error.
12. [BUG FIX] eITS#210101017
    a. Fix: UTM Cloud Query function may lead to abnormal memory usage
13. [BUG FIX] eITS#210101673
    a. Fix: Cannot set the lifetime value to 1 year on the certificates.
14. [BUG FIX] eITS#210200733
    a. Fix: Email security functional issue.
15. [BUG FIX] eITS#210300997
    a. Enhancement: Renewed the DNS server database in the system.

Features: V4.62(AAKZ.0)C0

Modifications in V4.62(AAKZ.0)C0 - 2021/01/19

1. [Vulnerability Fix] Potential Remote Code Execution vulnerability.
2. [Vulnerability Fix] Buffer Overflow vulnerability

Features: V4.60(AAKZ.1)C0

Modifications in V4.60(AAKZ.1)C0 - 2020/12/02

1. [ENHANCEMENT] Enhanced HA Pro reliability.
2. [BUG FIX][CVE-2020-29583]
   a. Vulnerability fix for undocumented user account.
3. [BUG FIX] eITS#201000455
   a. Fixed Port Zone Assignment issue.
4. [BUG FIX] eITS#201100284, 201100639, 201100647
   a. Fixed GUI show up issue when editing interfaces.
5. [BUG FIX] eITS#201100338
   a. Mouseover popup information adjustment.
6. [BUG FIX] eITS#201100416, 201100564
   a. Stability improvement.
7. [BUG FIX] eITS#201100511, 201100661, 201100730, 201101210, 201101248
   a. Fixed the issue that DNS packets cannot passthrough VPN tunnel.

Features: V4.60(AAKZ.0)C0

Modifications in V4.60(AAKZ.0)C0 - 2020/10/21

1. [ENHANCEMENT] SSL Inspection enhancement
   a. Support TLS1.3
   b. Support ECDSA certificate generation
   c. Performance enhancement
2. [ENHANCEMENT] Support customized block page of Content Filtering and URL Threat Filter at Notification > Response Message.
3. [ENHANCEMENT] Move Content Filtering HTTPs Domain Filter port setting for Block/Warning page from System/WWW to Content Filtering/General settings.
4. [ENHANCEMENT] Support IDP and Application Patrol signature information query at OneSecurity Threat Intelligence web site.
5. [ENHANCEMENT] Cloud CNM SecuReporter new add Application Statistic category.
6. [ENHANCEMENT] [Secure Policy] CLI command support update firewall rule by rule name.
7. [ENHANCEMENT] System GUI HTTPs service security enhancement
   a. Support TLS 1.3
   b. TLS 1.0/1.1 disabled by default
   c. Weak chipper DES is deprecated
8. [ENHANCEMENT] System FTPs service security enhancement
   a. Weak cipher RC4/3DES disabled by default
   b. Support CLI to enable 3DES/RC4 cipher
9. [ENHANCEMENT] System SNMP service security enhancement
   a. SNMP service disable by default
   b. Remove default Get/Set Community string
   c. Support CLI to disable SNMPv1(eITS#190800258)
   Note:
   If you never change the default value of Get/Set Community string. After upgrade to 4.60, the value will be reset (as 4.60 default). You need to configure the Community string if you want to enable SNMP.
10. [ENHANCEMENT] Support Google Authenticator two-factor authentication for administrator access.
11. [ENHANCEMENT] Support send configuration by Email
12. [ENHANCEMENT] Support Scheduling Auto configuration backup and send via Email.

13. [ENHANCEMENT] Support Scheduling Reboot function.
14. [ENHANCEMENT] Support LAG feature for USG2200
15. [ENHANCEMENT] [USG60W / USG60 / USG40W / USG40 / USG20W-VPN / USG20-VPN] Support Fast Forwarding
16. [ENHANCEMENT] Support Remote Access VPN Wizard for easy VPN client configuration.
17. [ENHANCEMENT][IPsec VPN] Support Diffie-Hellman Groups 19/20/21.
18. [ENHANCEMENT] APC upgrade to V3.60 support new features and 11ax AP.
    a. WPA3 enhancement.
    b. AP Log message enhance for Kick station enhancement of sticky clients
    c. Diagnostic enhancement for technical support.
    d. WAX510D and WAX650S AP support.
    e. Support wireless interface packet at Packet Capture on AP.
    f. Fully compatible configuration support for compatible AP
    g. Enhance Top N Stations traffic statistics from 24hour to 7days.
    h. Support Load-Balancing in AP Management.
    i. 802.11ax support.
    j. Tunnel SSID can chose Internal Ethernet interface not only VLAN support.
    k. Support Unicode SSID.
19. [ENHANCEMENT] GUI enhancement
    a. Support GUI grid tip content of objects
    b. Align the terms of Networking traffic indication
20. [Feature Change] [SMS] End of ViaNett support.
21. [Feature Change] [SSH] The GUI modification remove SSH Version 1.
22. [Feature Change] [Web Authentication] Default uncheck SSO when add new Web Auth. Policy.
23. [Feature Change] [USG40W / USG60W / USG20W-VPN] Default disable built-in Wi-Fi for Security purpose.
24. [BUG FIX][CVE-2015-5477] System DNS service vulnerability fix.
25. [BUG FIX][CVE-2020-3702] Cryptographic issues in WiFi driver(Kr00k) on USG40W, USG60W
26. [BUG FIX] eITS#200100755
    Fix: HA syncing issue when using FTPs to sync up the settings.
27. [BUG FIX] eITS#200301052
    Fix: Site to site VPN routing issue.
28. [BUG FIX] eITS#200301256
    Add L2TP VPN user login information on SecuReporter.

29. [BUG FIX] eITS#200400280
    Fix: ATP800 / FQDN cache full issue.
30. [BUG FIX] eITS#200401028
    Debug log adjustment.
31. [BUG FIX] eITS#200401102
    Load-Balancing on VTI-Trunk enhancement.
32. [BUG FIX] eITS#200401499
    IP MAC binding malfunction issue.
33. [BUG FIX] eITS#200500114
    Fix: The syslog does not send out device HA role changed log.
34. [BUG FIX] eITS#200500789
    Enhancement: Disable TLS v1.0 for ddns service.
35. [BUG FIX] eITS#200525649
    SSL VPN connection issue.
36. [BUG FIX] eITS#200602927
    Fix: Direct router table isn't appearing at once in packet flow explore page.
37. [BUG FIX] eITS#200603050, 200603439
    Malfunction in user group when authenticating by 802.1x with external RADIUS server.
38. [BUG FIX] eITS#200603107
    Incorrect SSL VPN status information in dashboard.
39. [BUG FIX] eITS#200603276
    GUI time display issue.
40. [BUG FIX] eITS#200603297
    Object reference table display issue.
41. [BUG FIX] eITS#200603364
    Incorrect 3G/LTE dongle warning message
42. [BUG FIX] eITS#200603806
    MAC address table display issue
43. [BUG FIX] eITS#200603855
    Anti-Spam functional issue.
44. [BUG FIX] eITS#200700662
    Hyperlink redirect to incorrect page.
45. [BUG FIX] eITS#200603433
    Fix: Accounting packet issue for L2TP.
46. [BUG FIX] eITS#200700596
    Fix: Connectivity Check functional issue.

47. [BUG FIX] eITS#200700772
    Fix: Mail notification with invalid header error.
48. [BUG FIX] eITS#200701095
    Fix: Deactivated Interface IP address reply ICMP ping.
49. [BUG FIX] eITS#200701207
    Fix: L2TP User Group Issue.
50. [BUG FIX] eITS#200701291
    Device stability enhancement.
51. [BUG FIX] eITS#200800125
    Fix: OSPF routes will be reset after clicking "apply" on interfaces
52. [BUG FIX] eITS#201000593
    GUI wording fine-tuned

Features: V4.39(AAKZ.0)C0

Modifications in V4.39(AAKZ.0)C0 - 2020/07/30

1. [ENHANCEMENT] Adopt new Technology from Security Partner: McAfee for Content Filter, and Anti-Spam.
2. [BUGFIX] eITS#200300829, 200301264, 200301372
   Fix: 2FA functional issue
3. [BUGFIX] eITS#200603107
   Fix: Correct SSL VPN status information at Dashboard by update the SSL VPN Policy.
   (Update SSL VPN Policy, only allow remote user in "User" type to access the internal network.)
4. [BUGFIX] eITS#200603170, 200603855
   Fix: Anti-Spam function may damage the mails in some circumstance
5. [BUGFIX] eITS#200700662
   Fix: Hyperlink redirected pages correction

Features: V4.38(AAKZ.0)C0

Modifications in V4.38(AAKZ.0)C0 - 2020/04/13

1. [ENHANCEMENT] [Anti-Virus] Support Cloud Query
2. [ENHANCEMENT] [INTERFACE] Support LAG on USG2200
   a. LACP only (not support Active-backup and balance-alb)
3. [ENHANCEMENT] [MAINTENENCE] Performance tuning on Speedtest tool
4. [ENHANCEMENT] [BWM] Let TCP ack packets can be managed by BWM function. Add CLI command to enable/disable this enhancement. (eITS#180700033, 200200602)
5. [ENHANCEMENT] Enlarge SSL VPN Users number

Concurrent SSL VPN users		
	WAS (default/max.)	IS(default/max.)
USG40/40W	5 / 15	20 / 30
USG60/60W	5 / 20	20 / 60
USG110	25 / 150	50 / 150
USG210	35 / 150	50 / 150
ZyWALL 110	25 / 150	50 / 150

6. [BUGFIX] eITS#190200518
   Fix: Streamer Connection issue since v4.33 upgrade
7. [BUGFIX] eITS#190300697
   Fix: Proxy by controller directly not working.
8. [BUGFIX] eITS#190500795
   Fix: The USG log indicated that the mail was drop by DNSBL (server to server SMTP), but client outlook still can receive the mail.
9. [BUGFIX] eITS#190500997, 191100683
   Fix: After edited static DHCP in IP/MAC binding, the DNS service cannot works.
10. [BUGFIX] eITS#190700250
    Fix: The CPU usage growing even without huge traffic.
11. [BUGFIX] eITS#190700606
    Fix: Specific mail server unreachable when use POP3.
12. [BUGFIX] eITS#190900282
    Fix: When add a new VLAN interface, ZySH daemon will busy for a while.
13. [BUGFIX] eITS#190900410
    Fix: USG2200 unstable issue by usb xhci debug function.
14. [BUGFIX] eITS#190900659

Fix: IPSec VPN Client has connection not working after disconnected.

15. [BUGFIX] eITS#190900684
    Fix: Fail to authenticate the ext-group-user type which group identifier string has '(' ')' character for L2TP over IPSec function.
16. [BUGFIX] eITS#191000574
    Fix: USG60W local AP drops.
17. [BUGFIX] eITS#191001243
    Fix: Log filter function not working properly sometimes.
18. [BUGFIX] eITS#191100135
    Fix: No Web GUI display after change to "easy mode".
19. [BUGFIX] eITS#191100321
    Fix: 2FA Auth. with AD User on SSL VPN does not work
20. [BUGFIX] eITS#191100475
    Fix: After IPSec tunnel rekey, the SN and system name becomes "N/A".
21. [BUGFIX] eITS#191100955
    Fix: OSPF/RIP dynamic routing protocol does not work on 4.35.
22. [BUGFIX] eITS#191200137
    Fix: The page at Ethernet > edit page cannot be edited.
23. [BUGFIX] eITS#191200741
    Fix: IPv6 firewall rules behave abnormally.
    After restarting the device, the DHCP v6 address cannot notify the firewall to update the ipv6 rules.
24. [BUGFIX] eITS#191200748
    Fix: Cannot save Guest network setting in Easy mode.
25. [BUGFIX] eITS#191200908
    Fix: Wrong spelling of white list
26. [BUGFIX] eITS#200100539
    Fix: IGMP snooping issue causes abnormal reboot.
27. [BUGFIX] eITS#200107098
    Fix: L2TP/IPsec VPN cannot get group information from external AD
28. [BUGFIX] eITS#200107102
    Fix: Cannot edit guest interface in the Expert mode.
29. [BUGFIX] eITS#200201144
    Fix: No duration time at "Monitor > System status > session monitor".
30. [BUGFIX] eITS#200300672
    Fix: GUI display error for default SSL VPN numbers.
31. [BUGFIX] eITS#200300829, 200301264, 200301372

Fix: The program stocked in SMS daemon and user cannot receive the 2FA email.

Features: V4.35(AAKZ.3)C0

Modifications in V4.35(AAKZ.3)C0 - 2020/02/26

1. [BUGFIX][CVE-2020-9054] Web login CGI RCE vulnerability fix
2. [BUGFIX][CVE-2020-8597] Buffer overflow risk in pppd vulnerability fix

Features: V4.35(AAKZ.2)C0

Modifications in V4.35(AAKZ.2)C0 - 2019/12/04

1. [BUGFIX] eITS#191000712
   Associated AP info not showing well on the GUI of Station info.
2. [BUGFIX] eITS#191000719
   No file will be generated after collecting the AP diagnostic
3. [BUGFIX] eITS#191000612, 191000726, 191001071, 191001116
   After upgrading the firmware from 4.33 to 4.35, the device may failed to apply the configuration and roll back to system default configuration in some circumstances.
4. [BUGFIX] eITS#191001080
   AP Group Profile changing from GUI may lead to configuration applying failure during the rebooting.
5. [BUGFIX] eITS#191001056
   Enhance DHCP request format between broadcast and unicast mode, based on ISP's deploying.
6. [BUGFIX] eITS#191000966
   L2TP authentication issue when using Windows login name and password as the L2TP username/password.
7. [BUGFIX] eITS#191000274
   IPsec VPN tunnel cannot built up successfully when "My IP" was set as FQDN.
8. [BUGFIX][CVE-2019-12581, CVE-2019-12583] Related to the Free Time feature
   Cross-Site-Scripting vulnerability fix.

Features: V4.35(AAKZ.0)C0

Modifications in V4.35(AAKZ.0)C0 - 2019/09/25

1. [ENHANCEMENT] Support SecuReporter log categories selection: Security Categories and Network categories.
2. [ENHANCEMENT] Support SecuReporter quick activation banner on Dashboard page
3. [ENHANCEMENT] Support Two-Factor Authentication via SMS/Email for administrator login from GUI/SSH/Telnet.
4. [ENHANCEMENT] Support APC 3.40 adds Managed APs: NWA5123-AC HD, WAC6303D-S, and WAC6552D-S.
5. [ENHANCEMENT]Customized http redirect parameters for Hotspot management.
6. [ENHANCEMENT] Hotspot Management enhance: Extend RADIUS account name length to 128
7. [ENHANCEMENT] Support Hotspot Features on USG60(W)

Model	Default Concurrent Login	
	WAS	IS
USG60(W)	128	200

8. [ENHANCEMENT][VPN] Support Microsoft Azure route-based IPSec Site-to-site VPN:
   b. VTI over IKEv2/IPsec
   c. BGP over IKEv2/IPsec
9. [ENHANCEMENT][VPN] Extend IPSec VPN PSK to 128 characters
10. [ENHANCEMENT][VPN] IPSec VPN support Diffie-Hellman Groups: DH15 to DH18
11. [ENHANCEMENT][Geo-IP] Support Region(Continent) object
12. [ENHANCEMENT] Support Email to SMS
13. [ENHANCEMENT] Support EZ Mode on USG110 and ZyWALL 110
14. [ENHANCEMENT] Support NAT policy matching by source IP address
15. [ENHANCEMENT] Interface connectivity check enhancement, support 2 target IPs healthy check
16. [ENHANCEMENT] Support Web Console
17. [ENHANCEMENT] Support ZON v2.1.0 Dual image firmware update
18. [ENHANCEMENT] User can sort by source IP in Session Monitor page
19. [ENHANCEMENT] Usability enhancement for certificate export
    a. Add download and Email action on My Certificates page

b. Add file extension for certificate export and download

20. [ENHANCEMENT] GUI enhancements:
    a. Ports speed change on GUI
    b. Syslog server port setting on GUI
    c. Add Description column at Interface GUI page
    d. Extend mail server password length to 63 characters
    e. Change Tool Bar icon sequence
21. [ENHANCEMENT] Device HA Pro Enhancements
    a. Bridge interface monitor enhance, either uplink or downlink port fail will trigger failover
    b. Failover flapping mitigation
22. [ENHANCEMENT] extend the following max. number
    a. Extend max. number of Zone from to 32

Model	Max. number of Zone	
	WAS	IS
ZyWALL 310/ USG310	16	32

    b. Extend max. of SSID profiles

Model	Max. of SSID profiles	
	Was	Is
USG1900	256	1024
USG1100	256	1024
USG310	64	1024
USG210	64	128
USG110	64	128
ZyWALL 1100	256	1024
ZyWALL 310	64	1024
ZyWALL 110	64	128
ATP200	32	128
ATP500	64	128
ATP800	128	1024

    c. Extend max. of Security profiles

Model	Max. of Security profiles	
	Was	Is
USG2200-VPN	64	1024
USG2200	64	1024
USG1900	32	1024
USG1100	32	1024
USG310	32	1024
USG210	32	128
USG110	32	128
ZyWALL 1100	32	1024
ZyWALL 310	32	1024
ZyWALL 110	32	128
ATP200	32	128
ATP500	32	128
ATP800	32	1024

23. [ENHANCEMENT]eITS#180900416
    Remove the limitation that virtual server port mapping cannot conflict with device's WWW service port, if user set a different External IP address from External interface IP address.
24. [ENHANCEMENT]eITS#181000571
    "Policy Route" page GUI loading time enhance.
25. [ENHANCEMENT]eITS#181100386
    Further explanation in the error message.
26. [ENHANCEMENT]eITS#181201167
    System default to enable easy mode Wi-Fi have low download speed on LAN1 subnet. Causing by default bridge with LAN1. Change default bridge with LAN2.
27. [ENHANCEMENT]eITS#190500018
    Add a log to address the SSLv3 dropping reason.
28. [ENHANCEMENT]eITS#181000730
    Remove unsafe SSH cipher list (CVE-2016-2183)
29. [Bug Fix] CVE- 2019-11477, CVE-2019-11478, CVE-2019-11479 vulnerability fix for Linux kernel

30. [Bug Fix] Web authentication CGI vulnerability fix
31. [Bug Fix] CVE-2019-9955 Cross-site scripting vulnerability fix
32. [Bug Fix] CVE-2019-12581 Cross-site scripting vulnerability fix
33. [Bug Fix] CVE-2019-12583 vulnerability fix for Hotspot management free time feature
34. [Bug Fix] eITS#180100124
    IPv6 gateway information lost after ISP reconnect.
35. [Bug Fix] eITS#180200790, 180300059
    After upgraded to 4.30 ITS WK06, IP MAC Binding causes client traffic packets dropped.
36. [Bug Fix] eITS#180300552
    Antispam shows wrong session threshold message in the log.
37. [Bug Fix] eITS#180400078
    Issue that users cannot modify static dhcp pool object on GUI.
38. [Bug Fix] eITS#180400129
    DSCP marking function doesn't work.
39. [Bug Fix] eITS#180500500
    LAN host IPv6 routing will disconnect after 6 days later on windows OS.
40. [Bug Fix] eITS#180600574, 181100570
    Fixed FQDN object DNS querying issue.
41. [Bug Fix] eITS#180600692
    Device only allow 1 admin user to create L2TP VPN tunnel, 2nd connection with the same account will be failed.
42. [Bug Fix] eITS#180600810, 180600970
    It is unable to connect SSL VPN on 4.31 WK23 firmware.
43. [Bug Fix] eITS#180700420
    Login to device with easy mode. It always pops out "Guest WiFi Time Expired".
44. [Bug Fix] eITS#180700430
    Remove obsolete command in diagnostic info file.
45. [Bug Fix] eITS#180800036
    Disable ALG FTP will cause sync drop by firewall.
46. [Bug Fix] eITS#180800486
    Wrong message with empty database of Geo IP.
47. [Bug Fix] eITS#180800847
    remove the log which caused by non-support function in sandbox
48. [Bug Fix] eITS#180900110
    Device access deny causing by high disk usage.

49. [Bug Fix] eITS#180900237
    Fix incorrect CEF log format of IDP
50. [Bug Fix] eITS#180900649
    AP List "Recent On-line time" sorting issue
51. [Bug Fix] eITS#180900707
    In GUI, when adding application rule via Configuration > Object > Application > Add > Add (for Application Rule), the users will be logged out.
52. [Bug Fix] eITS# 18100084
    2FA function will not send the SMS after the device reboots
53. [Bug Fix] eITS#181000251
    SSLVPN User cannot be logged out if SSL VPN tunnel was disconnected by SecuExtender.
54. [Bug Fix] eITS#181000401, 181100651
    PPPoE connection stability issue.
55. [Bug Fix] eITS#181000671
    In NAT setting, users can't select the virtual interface as the incoming interface.
56. [Bug Fix] eITS#181000675
    SecuManager campaign for rebooting cli script cannot get device response.
57. [Bug Fix] eITS#181000724
    GUI port role page displaying issue.
58. [Bug Fix] eITS#181000753
    Device shows incorrect log when enable HTTP/HTTPS service.
59. [Bug Fix] eITS#181100020
    "web-auth exceptional-service "XXXX"" CLI command should not be saved in configuration.
60. [Bug Fix] eITS#181100586
    The DHCP table will keep the entries even though the DHCP lease time is expired.
61. [Bug Fix] eITS#181100758
    IDP data in the daily report is incorrect.
62. [Bug Fix] eITS#181101172
    Daily report will carry wrong source IP address.
63. [Bug Fix] eITS#181100886
    Enabling the BWM feature will lead to session dropping.
64. [Bug Fix] eITS#181100980
    After changing the configuration in expert mode, the dashboard of easy

mode will not display correctly.

65. [Bug Fix] eITS#181100991
    Address group object members is gone after firmware updating to wk45.
66. [Bug Fix] eITS#181101269
    The sort function in security policy GUI page.
67. [Bug Fix] eITS#181200058
    VLAN creation failure.
68. [Bug Fix] eITS#181200072
    Special character "-" in FQDN.
69. [Bug Fix] eITS#181200273
    Passing broadcast packets at boot up time.
70. [Bug Fix] eITS#181200437
    802.11r automatically enabled after reboot.
71. [Bug Fix] eITS#190100106
    The duration setting in the WiFi wizard can't be saved to the device.
72. [Bug Fix] eITS#190100341
    When using the VPN wizard to create VPN profile, if the “DPD” is unticked, the VPN phase 2 profile will not be created.
73. [Bug Fix] eITS#190100402
    When user changes the FQDN object name, it will pop up error message.
74. [Bug Fix] eITS#190100839, 190300398
    When creating a PPPoE WAN with VLAN based, the default DUID is not filled.
75. [Bug Fix] eITS#190200778
    Changing user password by using copy/past hotkey on the keyboard, will not working if using IE11.
76. [Bug Fix] eITS#190201159
    Issue when using L2TP VPN authentication function via external RADIUS server.
77. [Bug Fix] eITS#190300736
    L2TP VPN with Domain Name cannot be established.
78. [Bug Fix] eITS#190300744
    Device reboot unexpected.
79. [Bug Fix] eITS#190300993
    When the interface IP address of the address object is changed, the related policy rule which refer the address object will not apply the new IP address.
80. [Bug Fix] eITS#190300999
    When creating a PPPoE WAN with VLAN6 as base, the default DUID is not filled.

81. [Bug Fix] eITS#190400069
    After upgraded firmware from 4.25 to 4.33, PPPoE unable get IPv6 address successfully.
82. [Bug Fix] eITS#190400071
    When the VPN client utilities disabled Mode config feature, device 2FA function will not work.
83. [Bug Fix] eITS#190400434
    Need to reboot the device when applying the rules that implemented the GEO-IP objects.
84. [Bug Fix] eITS#190400684
    Cannot change the type of address object.
85. [Bug Fix] eITS#190400765
    Device keep sending password expire notification to user even though the function was disabled.
86. [Bug Fix] eITS#190400948
    Cannot see "Policy Enforcement" option when selecting '"Site-to-Site with Dynamic Peer' scenario".
87. [Bug Fix] eITS#190500084
    ARP proxy malfunction after the device reboots.
88. [Bug Fix] eITS#190500095
    Unable to force logout an external user.
89. [Bug Fix] eITS#190500256
    BWM functional issue when the BWM rule applies a null address group.
90. [Bug Fix] eITS#190500604
    Can't enable OSPF for specific VLAN IDs.
91. [Bug Fix] eITS#190500841
    After modifying the Radius server settings. The Radius configuration still keeps the original domain name.
92. [Bug Fix] eITS#190501051
    Routing table displaying issue.
93. [Bug Fix] eITS#190501057
    The static route will disappear after rebooting the device.
94. [Bug Fix] eITS#190600182
    The policy control name will disappear when redirected from the dashboard.
95. [Bug Fix] eITS#190600505
    Unable to connect the other devices that use non-standard SSH port (Port 22) in CLI mode

96. [Bug Fix] eITS#190600563
    Special character "&" is not supported by group ID when login SSL VPN via AD ext-group-user.
97. [Bug Fix] eITS#190700068
    VPN tunnel stability issue.
98. [Bug Fix] eITS#190700198
    The new created address object cannot be selected in BWM rule configuration.
99. [Bug Fix] eITS#190700831
    Error message pops up when using packet capture function.
100. [Bug Fix] eITS#190700964
    In interface GUI page, set Metric will clear DHCP unicast settings.

Features: V4.33(AAKZ.0)C0

Modifications in V4.33(AAKZ.0)C0 - 2019/01/10

1. [Enhancement][GUI] Add a download icon at My certificate page and only Admin can download
2. [Enhancement] Enlarge dynamic account numbers of ZyWALL310/USG310/ZyWALL1100/USG1100
   (1) ZyWALL310/USG310: From 2000 to 4000
   (2) ZyWALL1100/USG1100: From 3000 to 4000
3. [Bug Fix] eITS# 180100106, 180900565
   Some SSL VPN network mask setting methods may lead to SSL VPN connection problem.
4. [Bug Fix] eITS# 180300552
   When antispam is activated, there is a message in log "Mail sessions have reached the maximum threshold of 200".
5. [Bug Fix] eITS# 180500318
   In some circumstances, rebooting the device from the Web GUI or CLI may be failed. Users need to power on/off the device.
6. [Bug Fix] eITS# 180500506
   Interface name changing will not be synchronized to the Device HA pro passive device.
7. [Bug Fix] eITS# 180500963
   When rebooting the Device HA pro active device by WebGUI, the passive device will reboot, too.
8. [Bug Fix] eITS# 180501192
   Fixed device stability issue.
9. [Bug Fix] eITS# 180600668
   CNA100 remote access HTTPs issue.
10. [Bug Fix] eITS# 180700145
    Changed username of SMTP authentication cannot be saved.
11. [Bug Fix] eITS# 180700348
    BWM config caused device booting up failure rolled back back to “lastgood.conf”.
12. [Bug Fix] eITS# 180701378
    Renewed password can’t be saved if the new password start by “$$” character.
13. [Bug Fix] eITS# 180800824

TCP behavior improvement.

14. [Bug Fix] eITS# 180800840
    Configuration change of "Active Directory" feature cannot be saved.
15. [Bug Fix] eITS# 180900203
    SSL VPN authenticated by using external AD server cannot work.
16. [Bug Fix] eITS# 180900228
    Facebook wifi connection period is not working as defined.
17. [Bug Fix] eITS# 180900755
    Facebook WIFI malfunction.
18. [Bug Fix] eITS# 181000655
    SecuManager makes a backup of a managed device automatically, when the device reboots even the configuration isn't changed.
19. [Bug Fix] eITS# 181001141
    RDP session drop in SSL VPN tunnel.
20. [Bug Fix] eITS# 181001198
    Routing trace malfunction.
21. [Bug Fix] eITS# 181100177
    The capwap daemon keeps generating configuration file and consumes the memory.
22. [Bug Fix] eITS# 181100380
    SSO function malfunction.

Features: V4.31(AAKZ.1)C0

Modifications in V4.31(AAKZ.1)C0 - 2018/04/17

No update in this version.

Features: V4.31(AAKZ.0)C0

Modifications in V4.31(AAKZ.0)C0 - 2018/04/03

1. [Enhancement]Add Zyxel Biz Forum icon link at Top Tool Bar
2. [Bug Fix] SPR#140425458
   DNS supports *.com A-record PTR.
3. [Bug Fix] SPR#100415854
   The GUI's initial help page's behavior was wrong by pop up Site Map instead of Help.
4. [Bug Fix] SPR#100914249
   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 the fix.
5. [Bug Fix] SPR#100105242, 100105292
   PPTP might not be able to connect successfully if it is configured via Installation Wizard/Quick Setup.
6. [Bug Fix] SPR#100419034
   SSLVPN of VNC cannot work if user connects VNC application by FQDN.
7. [Bug Fix] SPR#121203072
   Ext-group name and any password can login SSL VPN.
8. [Bug Fix] SPR#160307230
   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.
9. [Bug Fix] SPR#150529308
   Console sometimes display "XXX daemon dead" message during reboot.
10. [Bug Fix] SPR#160329256
    In custom UTM Profile > IDP > Custom Signatures > Payload option, if content have"[" word, GUI will show incorrect.
11. [Bug Fix] SPR#151125943
    After changing source address object name, LAN PC will not redirect to correct web portal.
12. [Bug Fix] SPR#160113511
    If Printer is a DHCP Client and IP changed may cause Printer sync fail.
13. [Bug Fix] SPR#151127016

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

14. [Bug Fix] SPR#151208533
    "Object Reference" cannot work at Configuration >Network> Interface > Ethernet > Edit IPv6 Configuration page.
15. [Bug Fix] SPR#151208561
    GUI will not redirect to login page automatically after firmware upgrade by using Chrome browser.
16. [Bug Fix] SPR#151214778
    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.
17. [Bug Fix] SPR#151217001
    GUI always shows "Loading…" message after applying IPSec VPN >edit IKE1 rule.
18. [Bug Fix] SPR#151223305
    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.
19. [Bug Fix] SPR#161219973
    By using copy and paste to set PPPoE/PPTP IP address on Installation Setup Wizard. "Next" button can't be pressed.
20. [Bug Fix] eITS#161100279
    Fix the issue that 'Disconnect Connections Before Falling Back' cannot work.
21. [Bug Fix] eITS#160900224, 170500103
    The NAT rules don't work after upgrading the firmware.
22. [Bug Fix] eITS#170600924
    SSL inspection reach the maximum number of sessions.
23. [Bug Fix] eITS#171001162
    SSL VPN is not working. After clicking on "connect", there is no response.
24. [Bug Fix] eITS#171200383, 171200810
    Httpd will be terminated after firmware upgrade to V4.30.
25. [Bug Fix] eITS#171200317
    The bandwidth is not correctly allocated.
26. [Bug Fix] eITS#171200429
    Fixed GUI layout issue.
27. [Bug Fix] eITS#171200450

Login GUI and SSH show zysh daemon is terminated. The traffic forwarding is fine, but zyshd is malfunctioned.

28. [Bug Fix] eITS#171200806
    The 4.2x firmware configuration file may have backward compatible issue on 4.3x in some circumstance
29. [Bug Fix] eITS#171200181
    With syslog "CAPWAP" category enabled and controller apply configuration to AP, then caused AP very unstable.
30. [Bug Fix] eITS#171200710
    Built-in access point (local AP) sometimes stops working for 1-2 minutes randomly
31. [Bug Fix] eITS#171200805
    Unable to add a new created Geography type of address object to an existing Geography type of address group object.
32. [Bug Fix] eITS#180100224
    Change all wrong wording "diasble" become "disable.
33. [Bug Fix] eITS#180100308
    Proxy arp setting cannot be saved by GUI
34. [Bug Fix] eITS#180100787
    In 4.30 diag-info sometime unable to decompress, it show "file corrupted"
35. [Bug Fix] eITS#180100790
    Device receives SIGPIPE and close daemon without core file.
36. [Bug Fix] eITS#180100943
    There is a mistake on welcome page in French. It is téléphone, not téléphoner
37. [Bug Fix] eITS#180200109
    IDP signature update failed. (Cannot get IDP signature URL form Server.)
38. [Bug Fix] eITS#180200286
    Error in debug log after 4.30WK6 update.

Features: V4.30(AAKZ.0)C0

Modifications in V4.30(AAKZ.0)C0 - 2017/11/24

1. [ENHANCEMENT] GDPR(Privacy statement)
   a. General Privacy Statement
   b. SecuReporter(available in Q3, 2018)
2. [ENHANCEMENT] Key management vulnerabilities of WPA2 protocol: CVE-2017-13077 through CVE-2017-13082, CVE-2017-13084, and CVE-2017-13086 through CVE-2017-13088
   Note: USG40W, USG60W and USG20W-VPN do not support 802.11r.
3. [ENHANCEMENT] Support Facebook Wi-Fi.
4. [ENHANCEMENT] Support Session Clear
5. [ENHANCEMENT] Support Proxy Arp on external and general interface
6. [ENHANCEMENT][GUI] Log Enhancement: Log category grouping
7. [ENHANCEMENT][GUI] Diagnostic tool: Support NSLOOKUP
8. [ENHANCEMENT][GUI] Active sessions on Dashboard and Session Monitor
   a. Dashboard > Active Session, the screen is the same as day one.
   b. Dashboard > Active Session, remove the link to the page of Session Monitor
9. [ENHANCEMENT][GUI] Packet Flow Explore:
   1-1 SNAT with the extra fields of 'protocol' and 'source port'
10. [ENHANCEMENT][GUI] Initial wizard: New add Step 6: Remote management
11. [ENHANCEMENT][GUI][Registration] Refine service with the links of "Activate" and "Buy" at the page of Network Risk Warning.
12. [ENHANCEMENT] GeoIP Address Object
    a. Support sorting by country of Traffic Statistics, Session Monitor, and user login.
    b. Support Geo IP setting of Policy Route, DNS Inbound LB, BWM, Web Authentication, and Session Control.
13. [ENHANCEMENT][Address Object] Support FQDN Address Object
    a. FQDN pattern support wildcard
    b. Support FQDN object apply as source(except Wildcard FQDN) or Destination of Security Policy
    c. Support FQDN object apply as source (except Wildcard FQDN) or Destination of Policy Route /BWM /Web Auth.
14. [ENHANCEMENT] [User Object] Notification of account expiry (support Admin type account only).

15. [ENHANCEMENT] [User Object] Strength of account password
16. [ENHANCEMENT] [Security Policy] Auto backup configuration when rules changed
17. [ENHANCEMENT] [Log] Logged information of account and its IP address when configuration changed
18. [ENHANCEMENT] [Log] Logged the details of firewall rules changed
19. [ENHANCEMENT] [Device-HA Pro]
    a. If Passive device updates firmware failed, it will not trigger Active device firmware update.
    b. Support DHCP table synchronize and IP MAC binding table.
    c. Auto reset the maximum failover counter
    d. Show Passive device information on Active device GUI.
20. [ENHANCEMENT] [Routing Protocol] Support IPv4 eBGP
21. [ENHANCEMENT] [VPN] Support IPv4 eBGP over IPsec VTI tunnel
22. [ENHANCEMENT] [VPN] Support IPv4 OSPF over IPsec VTI tunnel
23. [ENHANCEMENT] [VPN] Support Multicast over IPsec VTI tunnel
24. [ENHANCEMENT] [VPN] Support iOS provision
    Mobile configuration contain three types of VPN: IKEv2, IKEv1/IPSec, L2TP
25. [ENHANCEMENT] [Interface] DHCP options for PXE client.
26. [ENHANCEMENT] [Traffic Statistics] Support web site hits with HTTPS
27. [ENHANCEMENT] [System] System default enable the HTTPs strong cipher
28. [ENHANCEMENT] [Stability] Support Auto recovery- when upgrade firmware fail will auto rollback to previous status.
29. [ENHANCEMENT] [SNMP] OID Support: boot between dual images
30. [ENHANCEMENT] [EZMode] Change internal interface IP and network automatically when WAN IP conflict with internal IP.
31. [ENHANCEMENT] Support APC3.0
    a. AP forward compatibility support
    b. Zymesh
    c. AP NVGRE data tunnel
    d. 802.11r
32. [ENHANCEMENT] Hotspot Management enhancement
    a. Billing Replenish
    b. Change time period range
    c. [Billing] Number at the beginning is allowed
    d. [Freetime] Warning message modification
    e. [Payment] Add new currency BRL

f. [Payment] Add new currency RUB
g. [Printer] Redefine the printer information on GUI
h. [Printer] Empty the description
i. [Printer] Discovered printers divide into different group

33. [ENHANCEMENT] [UA] Enforce data collection
34. [ENHANCEMENT] [WebAuth] Support Session page on/off switch
35. [ENHANCEMENT] Support captive portal redirect with FQDN
36. [ENHANCEMENT] eITS#170400413
    Support user sets the DHCP6 preferred prefix size for delegation in Solicit message in DHCP6 request object by CLI command.
    - CLI cmd:

    Router(config)# dhcp6-request-object < profile name> prefix-delegation prefix-length <1…64>
37. [ENHANCEMENT] eITS#170700287,170700325
    a. Customer would like to using following username format with AD server by 802.1X:
       - sAMAccountNAme= usg\user1
       - userPrincipalName= user1@usg.com
    b. 802.1X auto login
38. [ENHANCEMENT] eITS#170901066
    Remove unwanted error log in the case that when User trusted certificates folder is empty.
39. [ENHANCEMENT] eITS#171000150
    GUI to allow setting schedule object stop Time 00:00 same as 24:00 for overnight schedule usage (e.g. 22:00 - 08:00), user can use a schedule group object to include two schedule object (e.g. 22:00 - 0:00 and 0:00 - 08:00)
40. [ENHANCEMENT][Device-HA Pro] Support spec. changed
    Default life time given after Device registered:
    USG1100, USG1900, USG2200-VPN, ZyWALL 1100
41. [FEATURE CHANGE] [GUI] Re-sort Interface menu list:
    Sequence: External >General >Internal >Others
42. [FEATURE CHANGE] [GUI] Dialogue window popup for new firmware notification now is for ADMIN type only
43. [FEATURE CHANGE] eITS#170300826

[GUI] With feature “Link Aggregation Group”, it no longer provides the field “none” on link-monitoring, balanced-alb and active-backup due to useless.

44. [FEATURE CHANGE] eITS#170500243
    WAS:
    UTM Profile>IDP add profile ""all"" default signature 1051723 action ""VIRUS Eicar test string"" is Reject-BOTH.
    IS:
    To set default create profile for signature 1051723 action NONE
45. [FEATURE CHANGE] eITS#170900224
    Change "Session Limit" log severity level from notice (5) to warning (4) for better troubleshooting.
46. [Bug Fix] eITS#160401060
    After few days, the mail sessions reach the maximum threshold and Anti-Spam stop working.
47. [Bug Fix] eITS#160800459
    AD ext-group-user test fail
48. [Bug Fix] eITS#160900786
    Syslog didn't send out traffic category
49. [Bug Fix] eITS#161000148
    StartSSL Certificate not valid
50. [Bug Fix] eITS#161000226
    BMW does not work with SSO authentication.
51. [Bug Fix] eITS#161000644
    After the launch of the anti-spam (usually after two hours), sometimes any letter does not pass through ZyWALL. They come after 20-30 minutes collectively, then they don`t pass through ZyWALL again, and so each time.
52. [Bug Fix] eITS#161100279
    Open RDP by using IE10, need to add IP address to IE "Compatibility view settings" issue.
53. [Bug Fix] eITS#161100604
    Configuration error when enable SLAAC.
54. [Bug Fix] eITS#161100649, 170100235
    Sometimes user cannot synchronize with myzyxel.com server successfully.
55. [Bug Fix] eITS#161200347, 161200799
    After upgrading to 4.20, change the port speed manually does not work.
56. [Bug Fix] eITS#161200446,170200683

Device will constantly rebooting by out of memory issue.

57. [Bug Fix] eITS#161200483
    Use network PING tool and found that no matter how they switch the interface, the outgoing IP do not get the correct match IP with interface.
58. [Bug Fix] eITS#161200541
    AP management VLAN configuration have limitation on Name field, we cannot create VLAN more than 4.
59. [Bug Fix] eITS#161200618
    The black list now detected before white list.
60. [Bug Fix] eITS#161200797
    VPN policy object not been changed after renaming object
61. [Bug Fix] eITS#161200798
    Default DHCP server not been removed after changed interface type
62. [Bug Fix] eITS#170100012
    The 802.1P Marking functions not work. (In BWM function)
63. [Bug Fix] eITS#170100106
    USG60w reboots when Mac book Wi-Fi try to associate to USG60w's Local AP.
64. [Bug Fix] eITS#170100259,170200190
    Issue with L2TP and security policy user-based
65. [Bug Fix] eITS#170100317
    The SNMP after remove and add VLAN interface, active & passive query mib ifTable .1.3.6.1.2.2.1.x are not the same
66. [Bug Fix] eITS#170100339
    User Agreement Users in Hotspot are registered 3 or 4 times at a single login
67. [Bug Fix] eITS#170100441
    Policy route does not work when configure a service group object as source port match criteria
68. [Bug Fix] eITS#170100457
    Device displays ZySH daemon is busy, and it not accessible via Web GUI
69. [Bug Fix] eITS#170100500
    Email Subjects being truncated with anti-spam enabled.
70. [Bug Fix] eITS#170100679
    Anti-spam tag the dlog in automatic reply emails content
71. [Bug Fix] eITS#170100898

User log in web authentication page by Firefox browser, it doesn't pop-up windows to tips user "You have been logout" when user close user aware browser.

72. [Bug Fix] eITS#170100903
    When the anti-spam activate, the large size (around 1~3mb) mail will delivery to internal mail server for a long time
73. [Bug Fix] eITS#170200027
    When the USG Wan interface connected gateway router reboots, the USG cannot aware SLACC renew. It leads to IPv6 DHCP client Internet access issue.
74. [Bug Fix] eITS#170200028
    The IPv6 of Prefix Delegation address on interface will no longer get value on it.
75. [Bug Fix] eITS#170200095
    Sometimes the Web GUI shows error "File not found" and does not work after booting the USG.
76. [Bug Fix] eITS#170200139
    Firewall rule block SSO user traffic time to time
77. [Bug Fix] eITS#170200161
    AP firmware v4.22 show station issue
78. [Bug Fix] eITS#170200382
    DHCP pool size is incorrect
79. [Bug Fix] eITS#170200530
    HA-Pro does not apply virtual MAC address.
80. [Bug Fix] eITS#170200531
    HA-Pro not sending Gratuitous ARP for virtual 1:1 NAT IP
81. [Bug Fix] eITS#170300098
    Unable to update GeoIP database
82. [Bug Fix] eITS#170300215,170300955,170400039,170400704
    Wrong routing entry for VPN
83. [Bug Fix] eITS#170300611
    Device changes host's source IP address in bridge mode
84. [Bug Fix] eITS#170300783
    Static Route not working after reboot of the USG
85. [Bug Fix] eITS#170300822
    Customer have an issue about USB LED behavior, even the USB stick dose not plug to device port, USB LED is still on.

86. [Bug Fix] eITS#170300826
    In LAG interface, set 802.3ad mode and choosing “none” and “ARP” as link monitoring mode. It will not work.
87. [Bug Fix] eITS#170301030
    High memory usage with HA-Pro
88. [Bug Fix] eITS#170400322
    Security Policy rule modification didn´t take effect when we modify address object, we must disable and enable the rule again to make it take effect.
89. [Bug Fix] eITS#170400331
    The ISP extended VOIP as HD voice
90. [Bug Fix] eITS#170400558
    Vulnerability Fix (CVE-2016-10229)
91. [Bug Fix] eITS#170407062
    IPSecVPN no any connection but log had R_U_THERE message
92. [Bug Fix] eITS#170500088,170500089
    After upgrade to ZLD4.25 firmware, GUI login device will stuck at genie.html page.
93. [Bug Fix] eITS#170500193
    Failed to apply startup-config.conf after modify guest interface name.
94. [Bug Fix] eITS#170500202
    RDP via SSLVPN fail
95. [Bug Fix] eITS#170500260
    Move the mouse cursor to the SIP default port 5060, change nothing and click on Apply. The error message pops up.
96. [Bug Fix] eITS#170500542,170500632
    Login web GUI then pop out a warning message "CLI number 39"
97. [Bug Fix] eITS#170500555
    Cloud-Helper Firmware Auto Update cannot disable
98. [Bug Fix] eITS#170500757
    Device High Memory and Auto Reboot several times / week
99. [Bug Fix] eITS#170500774
    Even if device is registered, the Setup Wizard show up again and finish with unreadable short popup "ERROR".
100. [Bug Fix] eITS#170500826
    Dashboard loading is very slow.
101. [Bug Fix] eITS#170500968
    The HTTPS Domain Filter is sending the wrong Certificate for blocked HTTPS

Pages based on "Enable Content Filter HTTPS Domain Filter Block/Warn Page" under certain condition.

102. [Bug Fix] eITS#170600091
Device HA backup sync error when disable Anti-Virus Black list
103. [Bug Fix] eITS#170600481
“custom web portal files" are not sync to other partition
104. [Bug Fix] eITS#170600635
Device HA backup sync error caused by Content Filter profile CLI ordering is different in some conditions.
105. [Bug Fix] eITS#170600780
When load some kind of customized configuration file, the device will restore to default setting after rebooting.
106. [Bug Fix] eITS#170600954
Unable negotiated PPP connection in IPv6CP phase with BT ISP
107. [Bug Fix] eITS#170700239
[Policy Route] Next-hop set with the interface but not containing gateway, and then the warning message now is given.
108. [Bug Fix] eITS#170700652
Schedule run display wrong info
109. [Bug Fix] eITS#161200163
Add source port(s)/service setting in 1-to-1 NAT zymark iptables rule.
110. [Bug Fix] eITS#170400180, 170400330, 170400796, 170500308, 170600919
Anti-spam session full issue and device daily system hang issue.
111. [Bug Fix] eITS#170500347
Content filter slow, no Warning displayed
112. [Bug Fix] eITS#170500975, 170600470
Anti-spam daemon and ctipd hang issue.
113. [Bug Fix] eITS#170700761
Anti-spam session full issue
114. [Bug Fix] eITS#170721720
The first four packets cannot go to remote DUT then VPN connection will auto-reconnect. After that, traffic was normal.
115. [Bug Fix] eITS#170800053
After changed VLAN priority in VLAN interface, the interface stops response. (Except inactivate and active it again)
116. [Bug Fix] eITS#170800190
Cloud firmware update function will always display Sunday even already

Monday changed.

117. [Bug Fix] eITS#170800299
Update-fw.log file cause high flash usage
118. [Bug Fix] eITS#170800684
PDF corrupted by Anti-Spam
119. [Bug Fix] eITS#170800820
The UDP traffic unable pass to remote access if device already keep the session on WAN1.
120. [Bug Fix] eITS#170803091
VPN dial fail but log had R_U_THERE message
121. [Bug Fix] eITS#170800267, 170800513, 170800565
Warning message pops up when creating a policy route rule
122. [Bug Fix] eITS#170300904
[GUI] The wording "expire" changed from "Ausgelaufen" to "Ablaufdatum"
in German.
123. [Bug Fix] eITS#170600081
The graph of CPU usage is different in the USG daily report and CNC.
124. [Bug Fix] eITS#170800408
RIP stops working
125. [Bug Fix] eITS#170900052
Device soft-lockup when apply customer's configuration
126. [Bug Fix] eITS#170900254
Customer cannot import root certificate at "Configuration > Object > Certificate > "Trusted Certificates", it will pop up error message.
127. [Bug Fix] eITS#170900406
Frontline state that IP 212.52.194.228/255.255.255.224 cannot be saved on ge3 interface, the "OK" button is grey out/not clickable.
128. [Bug Fix] eITS#170900762
Content filter profile specifically rename on Web GUI will cause the configuration file saving problem. Web GUI and start-up configure mismatch.
129. [Bug Fix] eITS#170900923
The object items cannot be selected if we filtered in other page. (GUI bug)
130. [Bug Fix] eITS#170600298
Budget reset mechanism after over budget will cause incorrect budget

interval data and budget statistics in the next connection.

131. [Bug Fix] eITS#170800560
Won´t keep logging settings for SSL inspection

132. [Bug Fix] eITS#170800684
PDF corrupted by Anti-Spam

133. [Bug Fix] eITS#170900820
Customer concerning the VPN VTI interface in trunk interface cannot failover and fallback.

Features: V4.25(AAKZ.1)C0

Modifications in V4.25(AAKZ.1)C0 - 2017/07/13

1. [ENHANCEMENT] System default settings change:
   Doesn't allow access device GUI via HTTPs or SSL VPN connect from WAN in system default.
   Note: This will not change the settings for upgrade from previous firmware version.
2. [ENHANCEMENT] GUI change:
   a. all Service license Status change from "Licensed" "Not Licensed" to "Activated", "Not Activated"
   b. if the license are transferred, then status will show "Not Licensed"
   c. update layout change wording : Firmware Upgrade License to Firmware Upgrade Service
   d. remove License Type and Expiration date from Firmware Management page
   e. Add OneSecurity link (Troubleshooting icon): add icon at Firmware Management GUI page and redirect to OneSecurity Firmware Upgrade SOP
3. [ENHANCEMENT] Support for PayPal Brazilian Real (BRL)/Russian Ruble (RUB) currency
4. [ENHANCEMENT] Initial Wizard add Remote Management on/off switch
5. [BUG FIX] eITS#170500228
   "Email daily report" is missing on web GUI setup page (Configuration > Log & Report > Email daily report).
6. [BUG FIX] eITS#170500089
   After logging into the Web GUI, it will redirect to https://x.x.x.x/ext-js/app/view/pagestore/genie.html instead of the device dashboard
7. [BUG FIX] eITS#161200145
   The authentication will fail when establishing L2TP VPN with MS-CHAPv2
8. [BUG FIX] eITS#170100259, 170200190
   Sometimes user-based security policy rule doesn't work properly.
9. [BUG FIX] eITS#170100903
   Fixed the anti-spam may delay the mail occasionally
10. [BUG FIX] eITS#170100505
    Security Policies does not working properly in some circumstances
11. [BUG FIX] eITS#161200446

When CF and App Patrol are enabled and there are peak abnormal "ACK" packets in the environment sent to the device. The device may reboot

12. [BUG FIX] eITS#170200139
    Firewall rule sometimes will block SSO client's traffic
13. [BUG FIX] eITS#170300098
    Fix: unable to update GeoIP database
14. [BUG FIX] eITS#170400322
    Fix: Security Policy rule modification doesn't take effect immediately after modifying the address objects.
15. [BUG FIX] eITS#170400243
    Fixed the device reboot accidently issue
16. [BUG FIX] eITS#170300955, 170300215 , 170400039, 170400704
    Fixed the VPN tunnel routing issue
17. [BUG FIX] eITS#170300561
    Fixed AP connection lost issue.
18. [BUG FIX] eITS#170100742
    Fixed USG310 Device HA Pro with https port different than 443 issue.

Features: V4.25(AAKZ.0)C0

Modifications in V4.25(AAKZ.0)C0 - 2017/04/21

1. [ENHANCEMENT] Openssl package upgrade to 1.02j
2. [ENHANCEMENT] UTM engine upgrade to 2.3.012
3. [ENHANCEMENT] Default IDP signature upgrade to 3.2.4.040(Base on 3.1.4 and add 518 app-behavior)
4. [ENHANCEMENT] AS and CF engine upgrade to 8.00.0125.1
5. [ENHANCEMENT] Support quick activation wizard to help user register device and activate UTM services in a short time.
6. [ENHANCEMENT] Support Grace Period for subscription license.
7. [ENHANCEMENT] add "Buy"/ "Renew" and "Activate" link at:
    a. Dashboard Security Service List
    b. Configuration > Licensing > Service Status List
    c. Each Service function page
    d. Security Service Warning page
8. [ENHANCEMENT] Support Country code GUI for USG/ZyWALL
    a. Except for USG40W/USG60W/USG20-VPN/USG20W-VPN
9. [ENHANCEMENT] APC built-in FW replacement
    a. Remove NWA5KN & 3KN series AP firmware
    b. Add NWA5123-AC AP firmware
    c. Keep NWA512x series AP firmware
10. [ENHANCEMENT] Support Hotspot Management License for USG110, USG210 and ZyWALL 110 with 30days trial.

Support models	Hotspot Management Service
USG110 USG210 ZyWALL 110	Default 30days trial
	LIC-HSM, Hotspot Management 1 year Subscription License
	LIC-HSM, Hotspot Management One-Time License

11. [ENHANCEMENT] Default value of VLAN DHCP lease time change from infinite to 2 days
12. [ENHANCEMENT] Extend max. number of Address Object for following models:

Models	Address Object Value	
	WAS	IS
USG20(W)-VPN	100	300
USG40(W)	100	300
USG60(W)	200	300

13. [ENHANCEMENT] Support SecuReporter (available in Q3, 2017)
14. [ENHANCEMENT] Support failure recoveries of configuration apply.
15. [ENHANCEMENT] Automatic Firmware update from USB storage
    a. Default action is disable
    b. Do not support Device HA/ Device HA pro scenario
       Note: When using USB firmware upgrade in HA Pro devices, you need to insert USB at Passive device to upgrade Firmware first, and then do USB firmware upgrade at Active device.
16. [ENHANCEMENT] Support DHCP option 60 on External type Ethernet and VLAN interface
17. [ENHANCEMENT] Support SSH Client
18. [ENHANCEMENT] Support GeoIP database auto-check & auto-update
19. [ENHANCEMENT] eITS#160200311
    The log "*Open /tmp/ext_group_info.conf_1 configuration file has failed*."
    Change the log description easy to understand as: Cannot open /tmp/ext_group_info.conf_1 configuration file. Please check the settings of Auth. method and Ext-Group-User Accounts by AAA Server.
20. [ENHANCEMENT] eITS#160300976
    To adjust "DHCP table / User Login" GUI display behavior.
21. [ENHANCEMENT] eITS#160800448
    Manual control of firewall rule "Only FIN bit is set" for abnormal TCP flag packets transmission.
22. [FEATURE CHANGE] eITS#160600471
    Bandwidth management cannot apply accurately by App Patrol
23. [BUG FIX] eITS#161100240
    802.1P marking in BWM is disappeared in ZLD 4.20.
24. [BUG FIX] eITS#161100700
    Fix ALG SIP Settings GUI disappear issue:
    a. Restrict Peer to Peer Signaling Connection
    b. Restrict Peer to Peer Media Connection
25. [BUG FIX] eITS#151200061
    Support LTE E3276 dongle
26. [BUG FIX] eITS#160200024
    No supporting for Huawei E3276 dongle.
27. [BUG FIX] eITS#160200048
    Port statistics shows wrong information on GUI
28. [BUG FIX] eITS#160200540

An over length object name ruins the security policy function, also stop the device boot from start-up config.

29. [BUG FIX] eITS#160200591
    After AP schedule applied, the device cannot boot normally and failover to last good config.
30. [BUG FIX] eITS#160300622
    A standby HA device do download AP firmware. This should not happen if the active role is taken by another device.
31. [BUG FIX] eITS#160300733
    Receiving a "Unicast" DHCP offer on WAN port because customer's ISP did so. (DHCP offer bootp flag: unicast)
32. [BUG FIX] eITS#160300990
    NAT rule didn't work for the specific object.
33. [BUG FIX] eITS#160400211
    Unable to apply NAT policy if a vitrual interface has different subnet from its' physical. This works fine in 4.13 but not in 4.15 (Error message: Original IP address is not comprised in Incoming interface subnet.)
34. [BUG FIX] eITS#160400995
    Cannot use full screen mode on IE11 RDP access. The SSL VPN tunnel works fine. Use RDP access but unable to use full screen mode (on IE11).
35. [BUG FIX] eITS#160500052
    If user shows VLAN 10 in IP/MAC Binding monitor page, both VLAN 10 and VLAN 100 will display.
36. [BUG FIX] eITS#160500699
    NAT rule doesn't work on general type interface.
37. [BUG FIX] eITS#160600575
    Fix: In ZLD V3.30, customer set a set a "ppp" interface and name "eth1" and then users apply the configuration file (startup-config). It will show the error message "% System fatal error: 3005105." on the console.
38. [BUG FIX] eITS#160601251
    A dead Zylogd triggers connectivity check and makes policy route on and off frequently, reboot is a temporarily solution.
39. [BUG FIX] eITS#160700403
    Fix: VPN after rekeying no Traffic in Tunnel
40. [BUG FIX] eITS#160700500, 160101189
    Site-to-site IPSec VPN Tunnel (IKEv1) and AES256/SHA256 encryption in Phase2 burst CPU usage.

41. [BUG FIX] eITS#160800459
    Fix: USG 50. AD ext-group-user test fail
42. [BUG FIX] eITS#160800706
    USG20-VPN will not send out “Forwarded website” to CF report server.
43. [BUG FIX] eITS#160800830
    Modify address object setting didn’t apply to configure file.
44. [BUG FIX] eITS#160800939
    While move to other pages, the sorting by object IP address behavior abnormal.
45. [BUG FIX] eITS#160800995, 160800977
    Unable to upload an overlong file name firmware via GUI.
46. [BUG FIX] eITS#160801122
    The source IP address shows incorrect on Web GUI, (different model support for different pool addresses)
47. [BUG FIX] eITS#160900125
    Fix: OneSecurity Anti-Spam PDF file corrupts.
48. [BUG FIX] eITS#160900128
    Anti-Spam mail scan timeout rate is high.
49. [BUG FIX] eITS#160900147, 160900359
    While DHCP function is disabled on all interfaces, the DNS proxy stop working.
50. [BUG FIX] eITS#160900449
    The VPN throughput of USG1900 is low.
51. [BUG FIX] eITS#160900525
    After SafeSearch enabled, the device did randomly unwanted reboot.
52. [BUG FIX] eITS#160900560
    When editing exist BWM rule, try to enable or disable "Maximize Bandwidth Usage" function. It can't write into configuration.
53. [BUG FIX] eITS#160900579
    After upgraded to ZLD4.20 firmware, there are additional AP image symbolic link in device, it will cause Device-HA Pro sync fail.
54. [BUG FIX] eITS#160900582
    When add Anti-Virus, tick or untick white list, it always saves as enabled.
55. [BUG FIX] eITS#160900603
    The customer creates a new application profile then adds some applications. The GUI meets loading nonstop when he wants to add other object into this application profile by Service searching.

56. [BUG FIX] eITS#160900614
    Error message shows on trying to create Object > Service by just fill in starting port.
57. [BUG FIX] eITS#160900619
    Some settings disappear from the configuration after a power fail.
58. [BUG FIX] eITS#160900702
    Update Anti-Virus crashes Zyshd daemon if there is no connection to myZyXEL.com.
59. [BUG FIX] eITS#160900704
    When the customer creates the new Radio profile, set Channel Selection to DCS, the A-MPDU and A-MSDU are enabled by default. However, after click OK button, then edit this profile again found A-MPDU and A-MSDU was not enabled.
60. [BUG FIX] eITS#160900708
    DHCPv6 Request can't be added to DHCPv6 Request Options in PPPoE.
61. [BUG FIX] eITS#160900760
    After upgraded from 4.15 to 4.20, they need to configure default policy rule as "Allow" instead of "Deny" otherwise they cannot surfing the Internet.
62. [BUG FIX] eITS#160900840
    Fix: After build Device-HA, on backup device linkup and link-down Ge4 port. The Backup device status is standby but GE4 IP address exists. It affects the traffic pass through to Backup device but not master one
63. [BUG FIX] eITS#160901009
    The tunnel interface is on the drop-down list of Public DNS Server setting.
64. [BUG FIX] eITS#160912324
    Fix: [VPN] [info] Send check packet won't send on IKEv2 VPN rule (6in4, 4in6, 6in6)
65. [BUG FIX] eITS#161000053
    If SafeSearch enabled, the Google log will be removed if accessing https://www.google.at or https://www.google.com (google family).
66. [BUG FIX] eITS#161000057
    Remove service object from service-group will be failed.
67. [BUG FIX] eITS#161000062
    Files with long names on Cyrillic (Russian) cannot be downloaded through SSL VPN / File Sharing. Files with short names will work.
68. [BUG FIX] eITS#161000092
    The Interface egress setting will been effects after added virtual interface

69. [BUG FIX] eITS#161000311
    Sorting by priority doesn't work correctly on all pages.
70. [BUG FIX] eITS#161000336
    Fix SNMP location issue.
71. [BUG FIX] eITS#161000353
    It is the VPN between ShrewClient and USG. It works fine under ZLD 4.15; however, after upgrading to ZLD 4.20, USG will send out DEL information to the client after establishing connection.
72. [BUG FIX] eITS#161000562
    If you choose View: all session in Session Monitor, then the first page is displayed normally, but an error occurred on second page.
73. [BUG FIX] eITS#161000654
    Firewall rule of user aware didn't work appropriate with GeoIP address object.
74. [BUG FIX] eITS#161000823
    Fix GUI shows wrong information on NAT setting. (Select 1:1 mode, shows 1: Multiple)
75. [BUG FIX] eITS#161000908
    Special characters are allowed on GUI but invalid in certification "+", ")" or ")".
76. [BUG FIX] eITS#161000911
    Cannot create VLAN100 after VLAN10 on GUI.
77. [BUG FIX] eITS#161000912
    There is no limitation of the DHCP pool range.
78. [BUG FIX] eITS#161017510
    Fix: [VTI]disable VTI interface will be enable after open this disable (VTI)profile and click "OK"
79. [BUG FIX] eITS#161100136
    Device will reboot only when CF is enabled on IPv6 and access some websites.
80. [BUG FIX] eITS#161100230
    Supporting for longer LDAP/AD password length to 63 characters.
81. [BUG FIX] eITS#161100298
    1:1 NAT Port Mapping Type can be select after change type to Virtual server and switch back to 1:1 NAT.
82. [BUG FIX] eITS#161100619
    SSL Inspection not works if set in firewall rule on ZLD4.20

83. [BUG FIX] eITS#161100649
    Fix myzyxel.com SSL time sync issue.
84. [BUG FIX] eITS#161200541
    AP management VLAN configuration have limit on Name field, we cannot create VLAN more than 4.
85. [BUG FIX] eITS#161200689
    Add more than 8 interface into a Trunk is allowed, but this setting got error and is automatically removed after reboot.
86. [BUG FIX] eITS#161200797
    VPN policy object doesn't change after renaming an object.
87. [BUG FIX] eITS#170100010
    "Host Name" and "Description" are missing under IP/MAC Binding
88. [BUG FIX] eITS#170100106
    While just started up, any connection from MAC OS will reboot USG60W. (Android, Windows platform don't have this issue.)
89. [BUG FIX] eITS#170100118
    The FTP function which in packet capture does not work. (Can't upload to external FTP server)
90. [BUG FIX] eITS#170200061
    When added PPP interface in to monitoring interface (Device-HA Pro), it will shows "The interface name is not accepted"
91. [BUG FIX] eITS#170200530
    When Device-HA Pro switching status, the MAC address of secondary is not synced.
92. [BUG FIX] eITS#170200161
    Fix: ZyWALL 310 (WLAN controller) - Some station info will be kept in station info list on the controller even the stations have been dissociated from the AP.
93. [BUG FIX] eITS#161000876
    Unable to turn off Policy Control or Allow Asymmetrical Route via GUI.
94. [BUG FIX] eITS#160301606
    USG310: error code2 drops ICMP Type3 packet
95. [BUG FIX] eITS#160400542
    USG210 Fatal Error Cause System Reboot
96. [BUG FIX] eITS#161100313
    USG110 IKEv2 dynamic tunnel suddenly stopped working
97. [BUG FIX] eITS#161100931

USG20-VPN - SIP Signaling Port not working

98. [BUG FIX] eITS#161100008

Fix: Cannot access some https website after enable domain filtering in CF.

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 USG210 USG310 / ZyWALL 310	100
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.3)C0

Modifications in V4.15(AAKZ.3)C0 - 2016/07/06

1. [BUG FIX] eITS#160601199
   Device can't update license successfully

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 ipicmp-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-Verkehraktivieren" should be corrected to "Intra-BSS-Verkehrblockieren"
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_wwwconfig.
    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, pingwww.zanolari.net
    4. Run CLI 'show ipdns 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 GenexisFiberXport 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, "463AAKZ0C0.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(**463AAKZ0C0-enterprise.mib** and **463AAKZ0C0-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
       ..
```

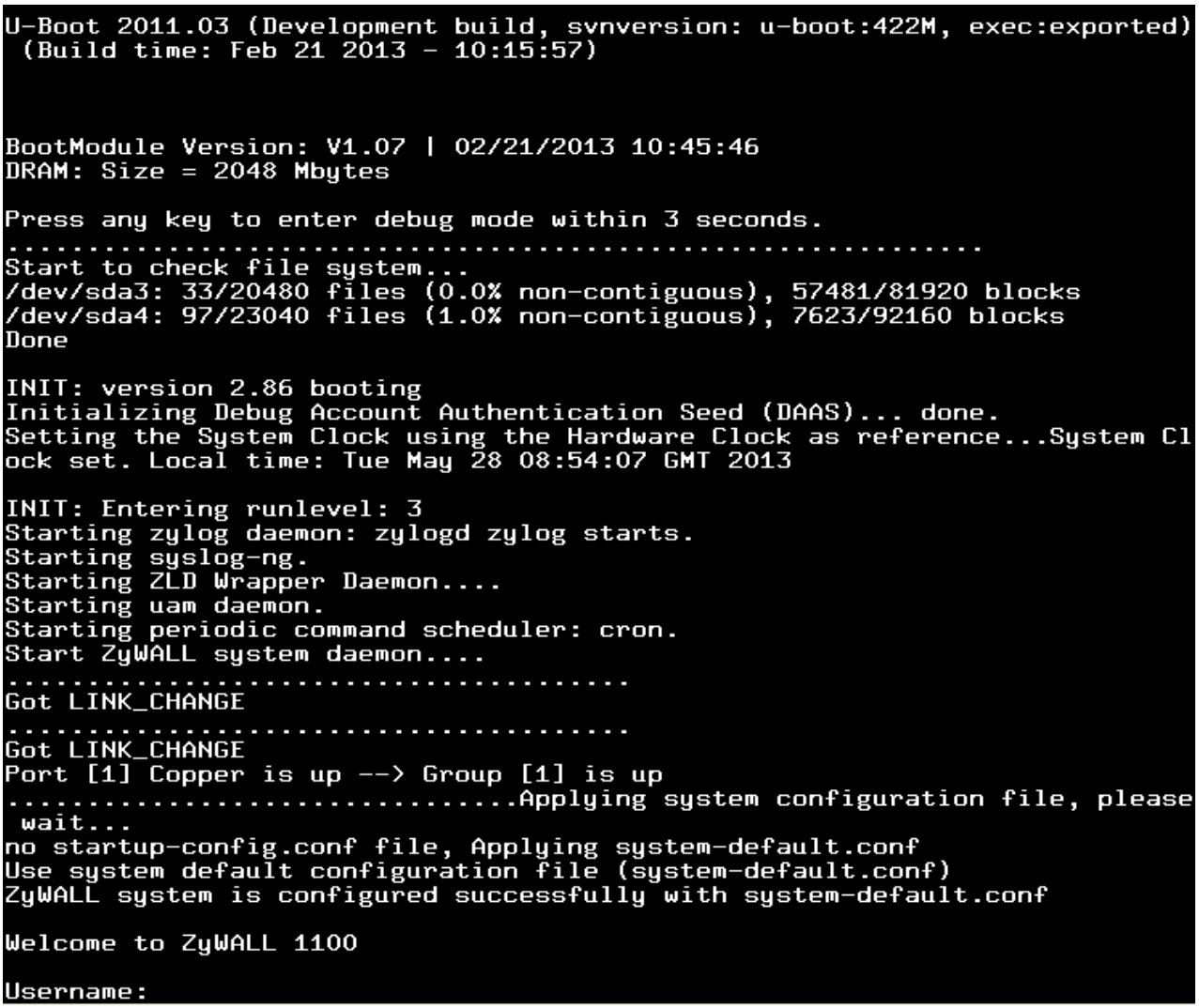
- The message here might be "ZLD-current received". Actually, it is equivalent to "Firmware received".

```
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.



- 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!!