ZYXEL

Firmware Release Note

USG20W-VPN

Release V4.31(ABAR.0)C0

Date: Apr 03, 2018
Author: Nicky Kuo
Project Leader: Eric Shen

Contents

ZYXEL USG20W-VPN

Release V4.31(ABAR.0)C0

Release Note

Date: Apr 03, 2018

Supported Platforms:

ZYXEL USG20W-VPN

Versions:

ZLD Version: V4.31(ABAR.0) | 2018-03-28 00:56:01

Files lists contains in the Release ZIP file

File name: 431ABAR0C0.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: 431ABAR0C0.conf

Purpose: This ASCII file contains default system configuration commands.

File name: 431ABAR0C0.pdf

Purpose: This release file.

File name: 431ABAR0C0.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: 431ABAR0C0-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: 431ABAR0C0-enterprise.mib, 431ABAR0C0-private.mib, ZYXEL-ES-SMI.MIB, ZYXEL-ES-CAPWAP.MIB, ZYXEL-ES-COMMON.MIB and ZYXEL-ES-ProWLAN.MIB. Please import ZYXEL-ES-SMI.MIB first.

File name: 431ABAR0C0-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 lan1, which are P2 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 wan, and the secondary WAN interface is sfp. 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 enablement.
2. Recommended upgrade to ZLD4.20 patch2 C0 or later version first before upgrading to ZLD4.31.
3. Please note we made some changes to download the latest security gateway firmware, for latest firmware download instruction please reference to: Firmware Upgrade Service Guide.
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. If user upgrades from previous released firmware to this version, there is no need to restore to system default configuration.

6. 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.
7. 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.
8. If ZyWALL/USG can't reboot successfully after firmware upgrade, please refer to Appendix 3: Firmware Recovery.
9. If you use a WK-Version, please contact local Support Team for Upgrade Information.
10. FCS 4.31 version wk date code is from 2017wk44 to 2017wk53.

Design Limitations:

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

DNS

1. [SPR: 150122977]

   [Symptom]

   DNS security option will deny device local out DNS query

   [Condition]

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

GUI

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

Operating System	Browsers	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 7 (X32) (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	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	latest version 5.0 (Chrome)	latest version 5.0 (Chrome)

* Not support Opera browser 10.6x

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
   c. IPv6 rules

SSL VPN

1. Following are the table list for SSL VPN supporting applications and operating systems:
   - SSL VPN Client (SecuExtender) support : Windows 7/8/10 and Mac OS 10.7 or later.

Applications	Reverse Proxy Mode	RDP	VNC
Operating System	File Sharing(Web-based Application)		
Windows 7 (X64) (SP1) Java 7u45 or later	Internet Explorer 10.x, 11.x Chrome 45.x, 49.x, 50.x to latest version Firefox latest version Safari latest version	Internet Explorer 10.x, 11.x	Internet Explorer 10.x, 11.x Chrome 45.x, 49.x, 50.x to latest version Firefox latest version Safari latest version
Windows 7 (X32) (SP1) Java 7u45 or later	Internet Explorer 10.x, 11.x Chrome 45.x, 49.x, 50.x to latest version Firefox latest version Safari latest version	Internet Explorer 10.x, 11.x	Internet Explorer 10.x, 11.x Chrome 45.x, 49.x, 50.x to latest version Firefox latest version Safari latest version
Windows 8, 8.1 (X64) Java 7u45 or later	Internet Explorer 10.x, 11.x Chrome 44.x or previous version Firefox latest version Safari latest version	Internet Explorer 10.x, 11.x	Internet Explorer 10.x, 11.x Chrome 44.x or previous version Firefox latest version Safari latest version
Windows 8, 8.1 (X32) Java 7u45 or later	Internet Explorer 10.x, 11.x Chrome 45.x, 49.x, 50.x to latest version	Internet Explorer 10.x, 11.x	Internet Explorer 10.x, 11.x Chrome 45.x, 49.x, 50.x to

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

L2TP VPN

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

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

2. [SPR: N/A]

   [Symptom]

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

User Aware

1. [SPR: 070813119]

   [Symptom]

   Device supports authenticating user remotely by creating AAA method which includes AAA servers (LDAP/AD/Radius). If a user uses an account which exists in 2 AAA server and supplies correct password for the latter AAA server in AAA method, the authentication result depends on what the former AAA server is. If the former server is Radius, the authentication would be granted, otherwise, it would be rejected.

   [Workaround]

   Avoid having the same account in AAA servers within a method.

IPv6

1. HTTP/HTTPS not support IPv6 link local address in IE7 and IE8.
2. Windows XP default MS-DOS FTP client cannot connection to device's FTP server via iPv6 link-local address.
3. [SPR: 110803280]

   [Symptom]

   Safari cannot log in web with HTTPS when using IPv6
4. [SPR: 110803293]

   [Symptom]

   Safari fails to redirect http to https when using IPv6
5. [SPR: 110803301]

   [Symptom]

   Safari with IPv6 http login when change web to System > WWW, it pop up a logout message. (HTTP redirect to HTTPS must enable)

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

1. Windows 7 users have not done Windows update before may have SecuExtender virtual Network interface card detection issue.

   [Workaround]

   Recommend installing all windows security patches before installing SecuExtender.

   One of reference: https://support.microsoft.com/en-us/kb/3033929

Known Issues:

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

IPSec VPN

1. [SPR: 120110586]
   [Symptom]
   When set IPSec VPN with certificate and enable x.509 with LDAP, the VPN session must dial over two times and the session will connect successfully
2. [SPR: 140317624]
   [Symptom]
   DUT fails to fall back using primary WAN port when all DUT WAN's IP address were same subnet.
3. [SPR: 140818615]
   [Symptom]
   After Enable and Disable NAT rule, IPSec VPN traffic cannot forward to LAN subnet immediately.
   [Condition]
   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
      - policy route, src= 172.0.0.0/8, dst=192.168.1.0/24, next-hop=VPN tunnel
      - 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.

4. [SPR: 141209575]
   [Symptom]
   IPSec VPN tunnel sometimes can be built up while initiator and responder devices use CA with the same subject name in IKE authentication. This tunnel should not be allowed to build.
5. [SPR: 160106369]
   [Symptom]
   To set up Local ID type in “DNS” mode at Advance setting under IPSec > VPN Gateway > Edit or Add page to make sure the Certificate works normally.
   [Workaround]
   If you are using certificate under the other modes, please go through VPN wizard then login again to VPN Gateway GUI page to modify the setting.
6. [SPR: 171115186]
   [Symptom]
   VPN pre-share key cannot accept some special characters from SecuManager Server.

IPv6

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

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.

System

1. [SPR: 130207529]
   [Symptom]
   When change SSH, Telnet and FTP Service default port, the connect session still exist.
2. [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.
3. [eITS: 170100444]
   [Symptom]
   Link sticking/Route Cache for dual WAN cannot work correctly with 4.25 as new implementation.

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: 170213467]

   [Symptom]

   Click "Buy" link will show 404 not found when enable HTTPS Domain Filter for HTTPS traffic.

4. [SPR: 170328262]

   [Symptom]

   Network risk warning information show null on ZyWALL series device

5. [SPR: 170323020]

   [Symptom]

   Exchange language setting, click MONITOR>>System Status>>Port Statistics start/stop button, it will show wrong language and need to click twice stop button to stop.

6. [SPR: 171103077]

   [Symptom]

   Firmware upgrade via GUI may lead to fail with the message "ajax communication failed".

   [Workaround]

   Re-login can solve it.

7. [SPR: 171016187]

   [Symptom]

   Easy mode ＞ click Network Client list button may cause page always loading status

3G Dongle

1. [SPR: 161215667]

   [Symptom]

   Budget set only download, action upload still has budget logs.

Single Sign On

1. [SPR: 171002024]

   [Symptom]

   SSO Agent on workstation and AD use windows 2016 server cannot work

   SSO Agent version 1.0.6 cannot work as below:

   AD windows 2016 server

   Windows 7 x64

   Windows 8.1 x64

   Windows 10 x64

Features: V4.31(ABAR.0)C0

Modifications in V4.31(ABAR.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(ABAR.0)C0

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

39. [ENHANCEMENT] GDPR(Privacy statement)
    a. General Privacy Statement
    b. SecuReporter(available in Q3, 2018)
40. [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.
41. [ENHANCEMENT] Support Facebook Wi-Fi.
42. [ENHANCEMENT] Support Session Clear
43. [ENHANCEMENT] Support Proxy Arp on external and general interface
44. [ENHANCEMENT][GUI] Log Enhancement: Log category grouping
45. [ENHANCEMENT][GUI] Diagnostic tool: Support NSLOOKUP
46. [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
47. [ENHANCEMENT][GUI] Packet Flow Explore:
    1-1 SNAT with the extra fields of ‘protocol’ and ‘source port’
48. [ENHANCEMENT][GUI] Initial wizard: New add Step 6: Remote management
49. [ENHANCEMENT][GUI][Registration] Refine service with the links of “Activate” and “Buy” at the page of Network Risk Warning.
50. [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.
51. [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.
52. [ENHANCEMENT] [User Object] Notification of account expiry (support Admin type account only).
53. [ENHANCEMENT] [User Object] Strength of account password

54. [ENHANCEMENT] [Security Policy] Auto backup configuration when rules changed
55. [ENHANCEMENT] [Log] Logged information of account and its IP address when configuration changed
56. [ENHANCEMENT] [Log] Logged the details of firewall rules changed
57. [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.
58. [ENHANCEMENT] [Routing Protocol] Support IPv4 eBGP
59. [ENHANCEMENT] [VPN] Support IPv4 eBGP over IPsec VTI tunnel
60. [ENHANCEMENT] [VPN] Support IPv4 OSPF over IPsec VTI tunnel
61. [ENHANCEMENT] [VPN] Support Multicast over IPsec VTI tunnel
62. [ENHANCEMENT] [VPN] Support iOS provision
    Mobile configuration contain three types of VPN: IKEv2, IKEv1/IPSec, L2TP
63. [ENHANCEMENT] [Interface] DHCP options for PXE client.
64. [ENHANCEMENT] [Traffic Statistics] Support web site hits with HTTPS
65. [ENHANCEMENT] [System] System default enable the HTTPs strong cipher
66. [ENHANCEMENT] [Stability] Support Auto recovery- when upgrade firmware fail will auto rollback to previous status.
67. [ENHANCEMENT] [SNMP] OID Support: boot between dual images
68. [ENHANCEMENT] [EZMode] Change internal interface IP and network automatically when WAN IP conflict with internal IP.
69. [ENHANCEMENT] Support APC3.0
    a. AP forward compatibility support
    b. Zymesh
    c. AP NVGRE data tunnel
    d. 802.11r
70. [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

71. [ENHANCEMENT] [UA] Enforce data collection
72. [ENHANCEMENT] [WebAuth] Support Session page on/off switch
73. [ENHANCEMENT] Support captive portal redirect with FQDN
74. [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>
75. [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
76. [ENHANCEMENT] eITS#170901066

    Remove unwanted error log in the case that when User trusted certificates folder is empty.
77. [ENHANCEMENT] eITS#171000150

    GUI to allow setting schedule object stop Time 00:00 same as 24:00 for overnight schedule usage (e.q. 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)
78. [ENHANCEMENT][Device-HA Pro] Support spec. changed

    Default life time given after Device registered:

    USG1100, USG1900, USG2200-VPN, ZyWALL 1100
79. [FEATURE CHANGE] [GUI] Re-sort Interface menu list:

    Sequence: External >General >Internal >Others
80. [FEATURE CHANGE] [GUI] Dialogue window popup for new firmware notification now is for ADMIN type only
81. [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.
82. [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

83. [FEATURE CHANGE] eITS#170900224

    Change "Session Limit" log severity level from notice (5) to warning (4) for better troubleshooting.

84. [Bug Fix] eITS#160401060

    After few days, the mail sessions reach the maximum threshold and Anti-Spam stop working.

85. [Bug Fix] eITS#160800459

    AD ext-group-user test fail

86. [Bug Fix] eITS#160900786

    Syslog didn't send out traffic category

87. [Bug Fix] eITS#161000148

    StartSSL Certificate not valid

88. [Bug Fix] eITS#161000226

    BMW does not work with SSO authentication.

89. [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.

90. [Bug Fix] eITS#161100279

    Open RDP by using IE10, need to add IP address to IE "Compatibility view settings" issue.

91. [Bug Fix] eITS#161100604

    Configuration error when enable SLAAC.

92. [Bug Fix] eITS#161100649, 170100235

    Sometimes user cannot synchronize with myzyxel.com server successfully.

93. [Bug Fix] eITS#161200347, 161200799

    After upgrading to 4.20, change the port speed manually does not work.

94. [Bug Fix] eITS#161200446,170200683

    Device will constantly rebooting by out of memory issue.

95. [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.

96. [Bug Fix] eITS#161200541

AP management VLAN configuration have limitation on Name field, we cannot create VLAN more than 4.

97. [Bug Fix] eITS#161200618
    The black list now detected before white list.
98. [Bug Fix] eITS#161200797
    VPN policy object not been changed after renaming object
99. [Bug Fix] eITS#161200798
    Default DHCP server not been removed after changed interface type
100. [Bug Fix] eITS#170100012
    The 802.1P Marking functions not work. (In BWM function)
101. [Bug Fix] eITS#170100106
    USG60w reboots when Mac book Wi-Fi try to associate to USG60w's Local AP.
102. [Bug Fix] eITS#170100259,170200190
    Issue with L2TP and security policy user-based
103. [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
104. [Bug Fix] eITS#170100339
    User Agreement Users in Hotspot are registered 3 or 4 times at a single login
105. [Bug Fix] eITS#170100441
    Policy route does not work when configure a service group object as source port match criteria
106. [Bug Fix] eITS#170100457
    Device displays ZySH daemon is busy, and it not accessible via Web GUI
107. [Bug Fix] eITS#170100500
    Email Subjects being truncated with anti-spam enabled.
108. [Bug Fix] eITS#170100679
    Anti-spam tag the dlog in automatic reply emails content
109. [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.
110. [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
111. [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.

112. [Bug Fix] eITS#170200028
The IPv6 of Prefix Delegation address on interface will no longer get value on it.
113. [Bug Fix] eITS#170200095
Sometimes the Web GUI shows error "File not found" and does not work after booting the USG.
114. [Bug Fix] eITS#170200139
Firewall rule block SSO user traffic time to time
115. [Bug Fix] eITS#170200161
AP firmware v4.22 show station issue
116. [Bug Fix] eITS#170200382
DHCP pool size is incorrect
117. [Bug Fix] eITS#170200530
HA-Pro does not apply virtual MAC address.
118. [Bug Fix] eITS#170200531
HA-Pro not sending Gratuitous ARP for virtual 1:1 NAT IP
119. [Bug Fix] eITS#170300098
Unable to update GeoIP database
120. [Bug Fix] eITS#170300215,170300955,170400039,170400704
Wrong routing entry for VPN
121. [Bug Fix] eITS#170300611
Device changes host's source IP address in bridge mode
122. [Bug Fix] eITS#170300783
Static Route not working after reboot of the USG
123. [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.
124. [Bug Fix] eITS#170300826
In LAG interface, set 802.3ad mode and choosing “none” and “ARP” as link monitoring mode. It will not work.
125. [Bug Fix] eITS#170301030
High memory usage with HA-Pro
126. [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.

127. [Bug Fix] eITS#170400331
The ISP extended VOIP as HD voice
128. [Bug Fix] eITS#170400558
Vulnerability Fix (CVE-2016-10229)
129. [Bug Fix] eITS#170407062
IPSecVPN no any connection but log had R_U_THERE message
130. [Bug Fix] eITS#170500088,170500089
After upgrade to ZLD4.25 firmware, GUI login device will stuck at genie.html page.
131. [Bug Fix] eITS#170500193
Failed to apply startup-config.conf after modify guest interface name.
132. [Bug Fix] eITS#170500202
RDP via SSLVPN fail
133. [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.
134. [Bug Fix] eITS#170500542,170500632
Login web GUI then pop out a warning message "CLI number 39"
135. [Bug Fix] eITS#170500555
Cloud-Helper Firmware Auto Update cannot disable
136. [Bug Fix] eITS#170500757
Device High Memory and Auto Reboot several times / week
137. [Bug Fix] eITS#170500774
Even if device is registered, the Setup Wizard show up again and finish with unreadable short popup "ERROR".
138. [Bug Fix] eITS#170500826
Dashboard loading is very slow.
139. [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.
140. [Bug Fix] eITS#170600091
Device HA backup sync error when disable Anti-Virus Black list
141. [Bug Fix] eITS#170600481
“custom web portal files" are not sync to other partition
142. [Bug Fix] eITS#170600635
Device HA backup sync error caused by Content Filter profile CLI ordering is different in some conditions.

143. [Bug Fix] eITS#170600780
When load some kind of customized configuration file, the device will restore to default setting after rebooting.
144. [Bug Fix] eITS#170600954
Unable negotiated PPP connection in IPv6CP phase with BT ISP
145. [Bug Fix] eITS#170700239
[Policy Route] Next-hop set with the interface but not containing gateway, and then the warning message now is given.
146. [Bug Fix] eITS#170700652
Schedule run display wrong info
147. [Bug Fix] eITS#161200163
Add source port(s)/service setting in 1-to-1 NAT zymark iptables rule.
148. [Bug Fix] eITS#170400180, 170400330, 170400796, 170500308, 170600919
Anti-spam session full issue and device daily system hang issue.
149. [Bug Fix] eITS#170500347
Content filter slow, no Warning displayed
150. [Bug Fix] eITS#170500975, 170600470
Anti-spam daemon and ctipd hang issue.
151. [Bug Fix] eITS#170700761
Anti-spam session full issue
152. [Bug Fix] eITS#170721720
The first four packets cannot go to remote DUT then VPN connection will auto-reconnect. After that, traffic was normal.
153. [Bug Fix] eITS#170800053
After changed VLAN priority in VLAN interface, the interface stops response. (Except inactivate and active it again)
154. [Bug Fix] eITS#170800190
Cloud firmware update function will always display Sunday even already Monday changed.
155. [Bug Fix] eITS#170800299
Update-fw.log file cause high flash usage
156. [Bug Fix] eITS#170800684
PDF corrupted by Anti-Spam
157. [Bug Fix] eITS#170800820
The UDP traffic unable pass to remote access if device already keep the session on WAN1.
158. [Bug Fix] eITS#170803091
VPN dial fail but log had R_U_THERE message

159. [Bug Fix] eITS#170800267, 170800513, 170800565
Warning message pops up when creating a policy route rule
160. [Bug Fix] eITS#170300904
[GUI] The wording “expire” changed from “Ausgelaufen” to
“Ablaufdatum”
in German.
161. [Bug Fix] eITS#170600081
The graph of CPU usage is different in the USG daily report and CNC.
162. [Bug Fix] eITS#170800408
RIP stops working
163. [Bug Fix] eITS#170900052
Device soft-lockup when apply customer's configuration
164. [Bug Fix] eITS#170900254
Customer cannot import root certificate at “Configuration > Object > Certificate > “Trusted Certificates”, it will pop up error message.
165. [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.
166. [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.
167. [Bug Fix] eITS#170900923
The object items cannot be selected if we filtered in other page. (GUI bug)
168. [Bug Fix] eITS#170600298
Budget reset mechanism after over budget will cause incorrect budget interval data and budget statistics in the next connection.
169. [Bug Fix] eITS#170800560
Won´t keep logging settings for SSL inspection
170. [Bug Fix] eITS#170800684
PDF corrupted by Anti-Spam
171. [Bug Fix] eITS#170900820
Customer concerning the VPN VTI interface in trunk interface cannot failover and fallback.

Features: V4.25(ABAR.1)C0

Modifications in V4.25(ABAR.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(ABAR.0)C0

Modifications in V4.25(ABAR.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(ABAR.2)C0

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

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

Features: V4.20(ABAR.1)C0

Modifications in V4.20(ABAR.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(ABAR.0)C0

Modifications in V4.20(ABAR.0)C0 - 2016/08/04

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 2.0 Support, 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) Geo IP blocking

   Support IPv4/IPv6 geography type address object as the source or destination address of
   security policy.

   (3) 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]
   Web GUI and SSL VPN login support TLS1.2
7. [ENHANCEMENT]
   Auto sync Time-Zone and Daylight-Saving from ZyXEL cloud server
8. [ENHANCEMENT]
   Support L2TP WAN connection type
9. [ENHANCEMENT]
   Service redirect for HTTP and SMTP traffic
10. [ENHANCEMENT]
    DHCP clients table add leasing expiration time information
11. [ENHANCEMENT]
    Add DHCP clients table in daily report
12. [ENHANCEMENT]
    ZON utility support update location and system name
13. [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

14. [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

15. [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)

16. [ENHANCEMENT]

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

17. [ENHANCEMENT]"Use Static-Dynamic Route to Control 1-1 NAT Route" is enabled on system default setting.
18. [ENHANCEMENT]BEAST vulnerability mitigation

    Support new CLI to disable TLS 1.0,

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

19. [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.

20. [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

21. [BUG FIX] eITS#150701032

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

22. [BUG FIX] eITS#150900398

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

23. [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)

24. [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.

25. [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.

26. [BUG FIX] eITS#150600519

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

27. [BUG FIX] eITS#150900987

    USG1900 doesn't detect LTE dongle WLTUBA-107

28. [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.

29. [BUG FIX] eITS#151001056

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

30. [BUG FIX] eITS#150901015

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

31. [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.

32. [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.

33. [BUG FIX] eITS#150901170

    The L2TP tunnel will frequent disconnects.

34. [BUG FIX] eITS#151001230, 151100428

    Device reboot time to time

35. [BUG FIX] eITS#150800878

    Error IP format still saved into configuration by CLI command

36. [BUG FIX] eITS#150900889

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

37. [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.

38. [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.

39. [BUG FIX] eITS#151200212

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

40. [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.
41. [BUG FIX] eITS#151100310

    Not possible delete VPN rules created by L2TP wizard
42. [BUG FIX] eITS#141001045

    It shows incorrect expiration date of licenses on the GUI.
43. [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
44. [BUG FIX] eITS#160100981

    One wrong Russian translation
45. [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.
46. [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.

47. [BUG FIX] eITS#160101287

    The mail server can't receive mail from internet.

    [Condition]

    Device response "reached the maximum threshold of 200."

48. [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.

49. [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.

50. [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.

51. [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.

52. [BUG FIX] eITS#150800388, 150800459

    Proxy Cap SSH connection through USG

    [Condition]

    SSH daemon TCP forwarding does not work.

53. [BUG FIX] eITS#160200257

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

54. [BUG FIX] eITS#160500683

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

55. [BUG FIX] eITS#160601226

    Memory leakage

56. [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.

57. [BUG FIX] eITS#160300715

    When CF is active no http/https traffic possible

Features: V4.16(ABAR.1)C0

Modifications in V4.16(ABAR.1)C0 - 2016/2/3

1. [BUG FIX]

   Fix auto-reboot caused by set special secure-policy.

   [Condition]

   If the security-policy use an address group object which without any address object included.

Features: V4.16(ABAR.0)C0

Modifications in V4.16(ABAR.0)C0 - 2015/12/25

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, "431ABAR0C0.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

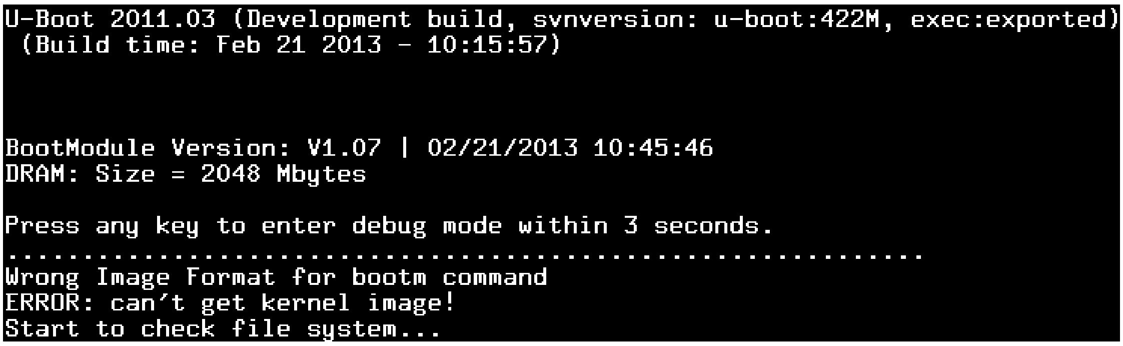
SNMPv2 private MIBs provides user to monitor ZyWALL/USG platform status. If user wants to use this feature, you must prepare the following step:

1. Have ZyWALL/USG mib files (**431ABAR0C0-enterprise.mib** and **431ABAR0C0-private.mib**) and install to your MIBs application (like MIB-browser). You can see 416ABAR0C0-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. VPNIpsecTotalThroughput: The VPN total throughput (Bytes/s), Total means all packets (Tx + Rx) through VPN.

Appendix 3. Firmware Recovery

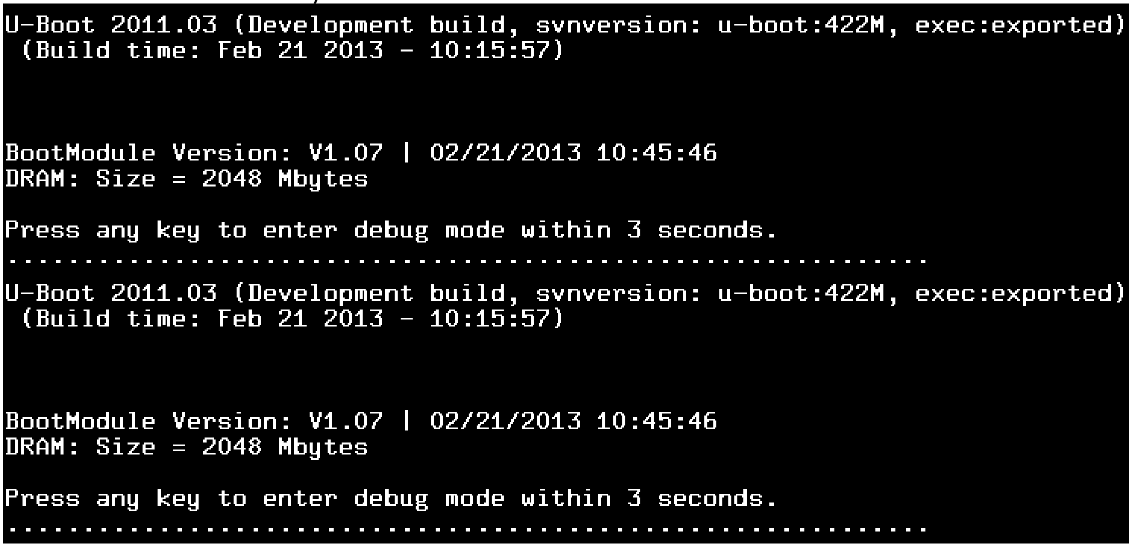
In some rare situation(symptom as following), ZyWALL/USG might not boot up successfully after firmware upgrade. The following procedures are the steps to recover firmware to normal condition. Please connect console cable to ZyWALL/USG.

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



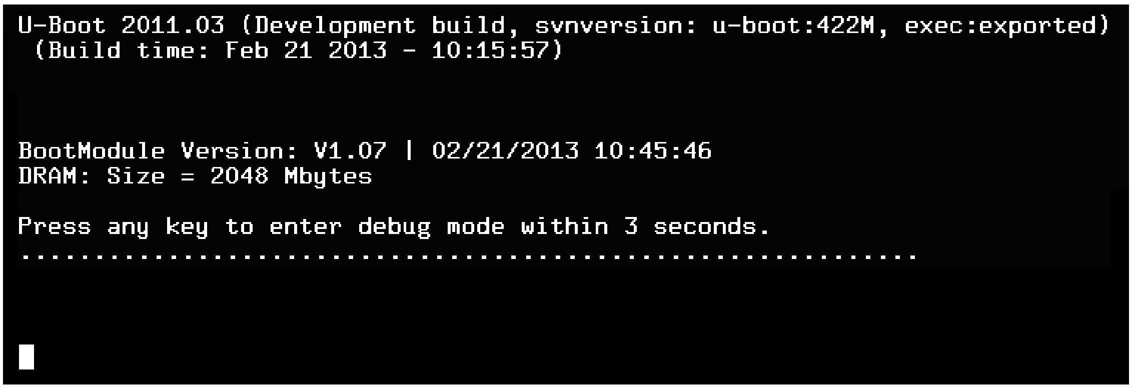
```
U-Boot 2011.03 (Development build, svnversion: u-boot:422M, exec:exported)
 (Build time: Feb 21 2013 - 10:15:57)



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

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

   - Device reboot infinitely.



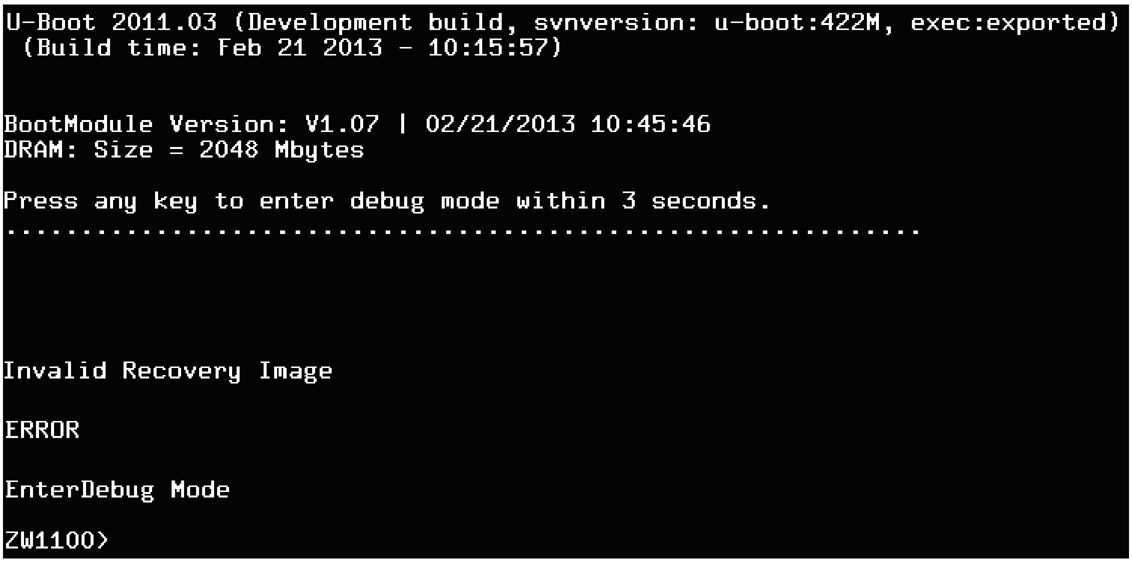
```
U-Boot 2011.03 (Development build, svnversion: u-boot:422M, exec:exported)
 (Build time: Feb 21 2013 - 10:15:57)



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

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



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

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

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



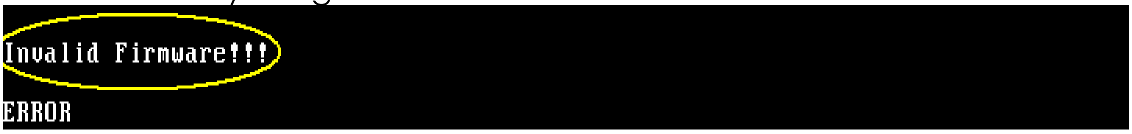
```
U-Boot 2011.03 (Development build, svnversion: u-boot:422M, exec:exported)
 (Build time: Feb 21 2013 - 10:15:57)



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

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

   - Startup message displays “Invalid Recovery Image”.



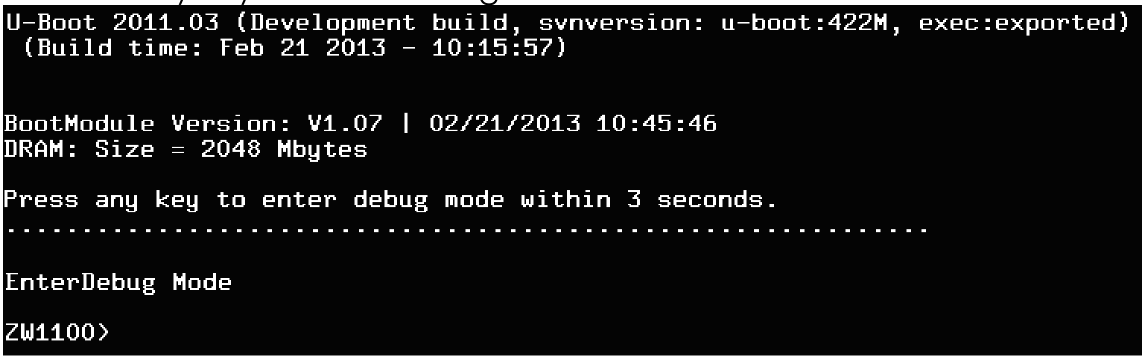
```
U-Boot 2011.03 (Development build, svnversion: u-boot:422M, exec:exported)
 (Build time: Feb 21 2013 - 10:15:57)


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

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




Invalid Recovery Image

ERROR

EnterDebug Mode

ZW1100>
```

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



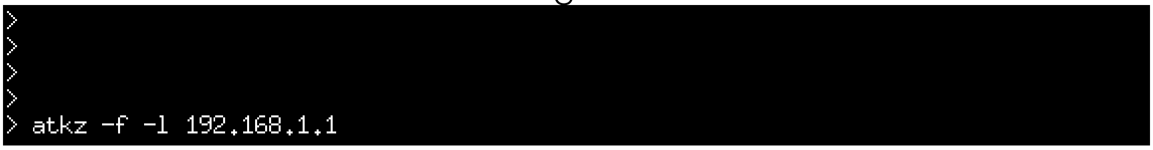
```
Invalid Firmware!!!

ERROR
```

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



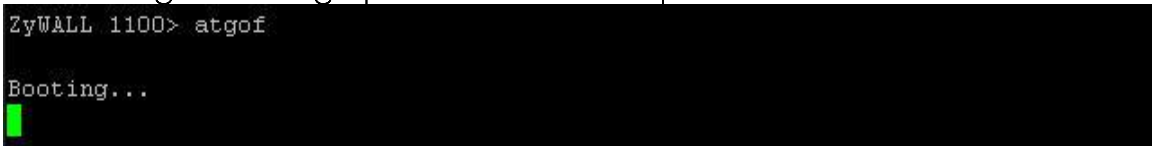
```
U-Boot 2011.03 (Development build, svnversion: u-boot:422M, exec:exported)
 (Build time: Feb 21 2013 - 10:15:57)


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

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

EnterDebug Mode

ZW1100>
```

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



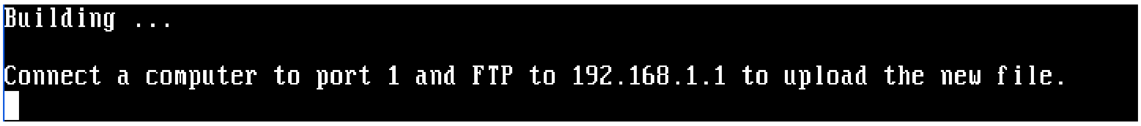
```
>
>
>
>
> atkz -f -l 192.168.1.1
```

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



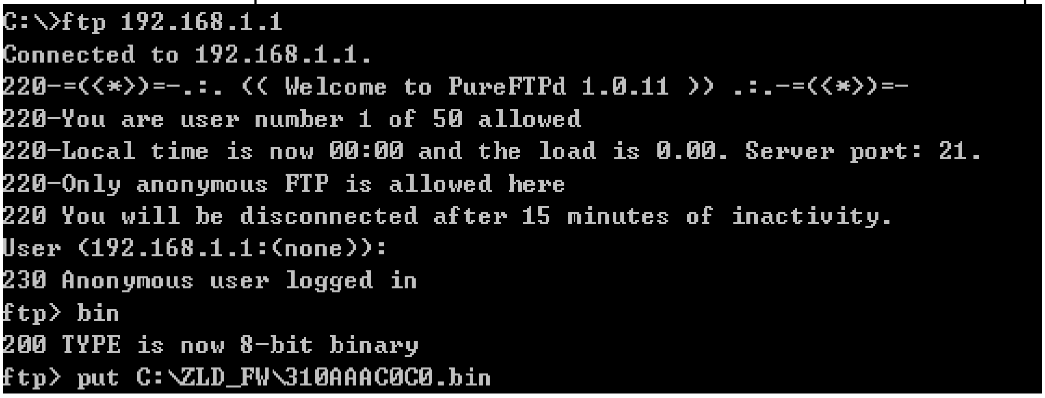
```
ZyWALL 1100> atgof

Booting...
```

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



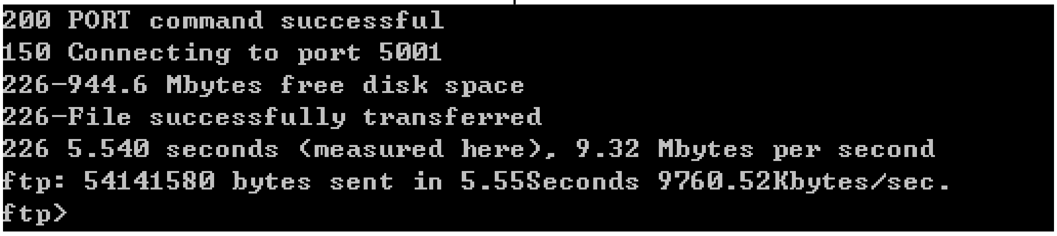
```
Building ...

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

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



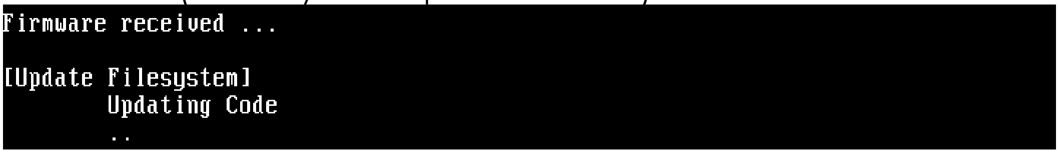
```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220-=(<*>)=-.:. (( Welcome to PureFTPd 1.0.11 )) .:.-=(<*>)=-
220-You are user number 1 of 50 allowed
220-Local time is now 00:00 and the load is 0.00. Server port: 21.
220-Only anonymous FTP is allowed here
220 You will be disconnected after 15 minutes of inactivity.
User (192.168.1.1:(none)):
230 Anonymous user logged in
ftp> bin
200 TYPE is now 8-bit binary
ftp> put C:\ZLD_FW\310AAAC0C0.bin
```

- Wait for the file transfer to complete.



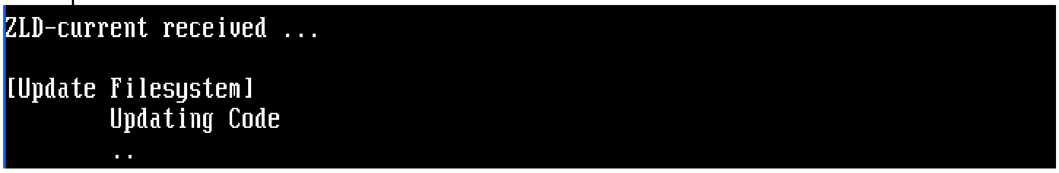
```
200 PORT command successful
150 Connecting to port 5001
226-944.6 Mbytes free disk space
226-File successfully transferred
226 5.540 seconds (measured here), 9.32 Mbytes per second
ftp: 54141580 bytes sent in 5.55Seconds 9760.52Kbytes/sec.
ftp>
```

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



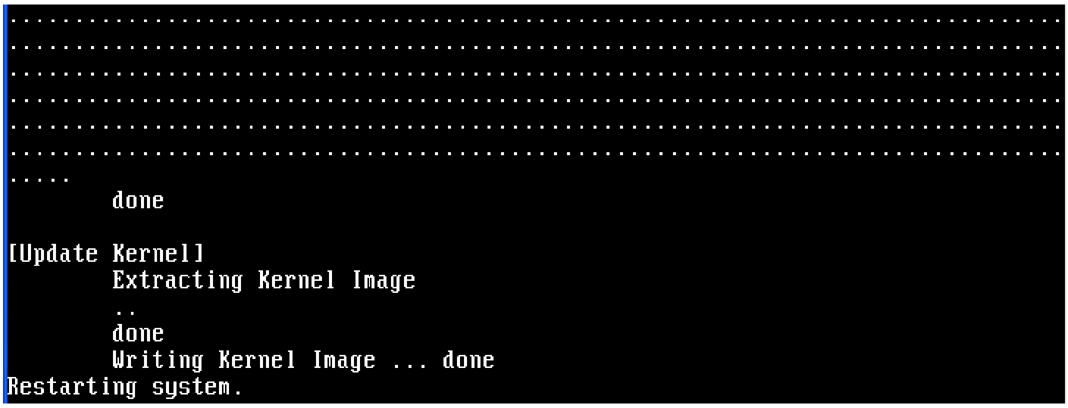
```
Firmware received ...

[Update Filesystem]
       Updating Code
       ..
```

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



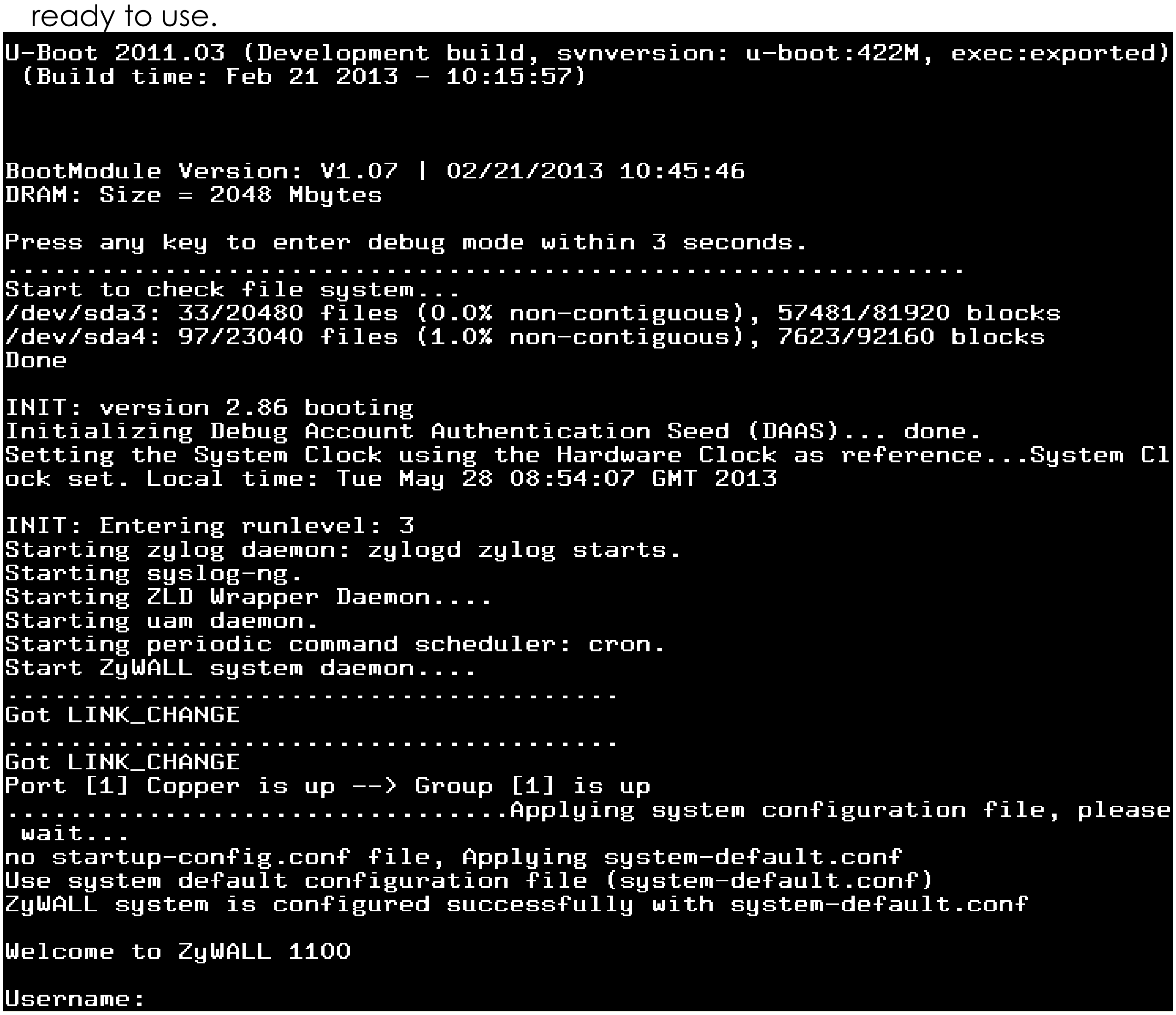
```
ZLD-current received ...

[Update Filesystem]
       Updating Code
       ..
```

- The console session displays "done" when the firmware recovery is complete. Then the ZyWALL/USG automatically restarts.



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

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

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



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



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

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

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

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

Welcome to ZyWALL 1100

Username:
```

- If one of the following cases occurs, you need to do the “firmware recovery process” again. Note that if the process is done several time but the problem remains, please collect all the console logs and send to ZyXEL/USG for further analysis.

- One of the following messages appears on console, the process must be performed again ./bin/sh: /etc/zyxel/conf/ZLDconfig: No such file Error: no system default configuration file, system configuration stop!!