ZYXEL

ZYXEL

Firmware Release Note

USG20W-VPN

Release V4.25(ABAR.0)C0

Date: Apr 21, 2017
Author: Rain Lee
Project Leader: Rain Lee

ZYXEL

Contents

ZYXEL USG20W-VPN

Release V4.25(ABAR.0)C0

Release Note

Date: Apr 21, 2017

Supported Platforms:

ZYXEL USG20W-VPN

Versions:

ZLD Version: V4.25(ABAR.0) | 2017-04-21 07:54:38

Files lists contains in the Release ZIP file

File name: 425ABAR0C0.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: 425ABAR0C0.conf

Purpose: This ASCII file contains default system configuration commands.

File name: 425ABAR0C0.pdf

Purpose: This release file.

File name: 425ABAR0C0.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.

ZYXEL

File name: 425ABAR0C0-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: 425ABAR0C0-enterprise.mib, 425ABAR0C0-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: 425ABAR0C0-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 enablement.
2. Recommended upgrade to ZLD4.16 patch1 C0 or later version first before upgrading to ZLD4.25.
3. It is recommended that user backs up "startup-config.conf" file first before upgrading firmware. The backup configuration file can be used if user wants to downgrade to an older firmware version.
4. If user upgrades from previous released firmware to this version, there is no need to restore to system default configuration.
5. When getting troubles in configuring via GUI (popup java script error, etc.), it is recommended to clear browser's cache first and try to configure again.

ZYXEL

6. To reset device to system default, user could press RESET button for 5 seconds and the device would reset itself to system default configuration and then reboot.

- Note: After resetting, the original configuration would be removed. It is recommended to backup the configuration before this operation.

7. If ZyWALL/USG can't reboot successfully after firmware upgrade, please refer to Appendix 3: Firmware Recovery.

8. If you use a WK-Version, please contact local Support Team for Upgrade Information.

ZYXEL

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

   [Workaround]

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

DNS

1. [SPR: 140425458]

   [Symptom]

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

2. [SPR: 150122977]

   [Symptom]

   DNS security option will deny device local out DNS query

   [Condition]

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

GUI

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

Operating System	For Administrator Login	For User Login
Windows 7 (X64) (SP1)	Internet Explorer 10.x, 11.x Chrome latest version Firefox latest version Opera latest version Safari latest version	Internet Explorer 10.x, 11.x Chrome latest version Firefox latest version Opera latest version Safari latest version
Windows 7 (X32) (SP1)	Internet Explorer 10.x, 11.x Chrome latest version Firefox latest version	Internet Explorer 10.x, 11.x Chrome latest version Firefox latest version

	Opera latest version Safari latest version	Opera latest version Safari latest version
Windows 8.0, 8.1 (X64)	Internet Explorer 10.x, 11.x Chrome latest version Firefox latest version Opera latest version Safari latest version	Internet Explorer 10.x, 11.x Chrome latest version Firefox latest version Opera latest version Safari latest version
Windows 8.0, 8.1 (X32)	Internet Explorer 10.x, 11.x Chrome latest version Firefox latest version Opera latest version Safari latest version	Internet Explorer 10.x, 11.x Chrome latest version Firefox latest version Opera latest version Safari latest version
Windows 10 (X64)	Internet Explorer 11.x Chrome latest version Firefox latest version Opera latest version Safari latest version edge latest version	Internet Explorer 11.x Chrome latest version Firefox latest version Opera latest version Safari latest version edge latest version
Linux OS(Ubuntu13.10x86)	Firefox latest version Opera latest version	Firefox latest version Opera latest version
Apple MAC OS X	Safari latest version Firefox latest version	Safari latest version Firefox latest version
iOS	8 latest version 9 latest version 10 latest version	8 latest version 9 latest version 10 latest version
Android	latest version	latest version

* Not support Opera browser 10.6x

2. [SPR: 100415854]

   [Symptom]

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

   [Condition]

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

3. [SPR: 100914249]

   [Symptom]

   IE7/8 sometimes shows "Stop running this script? A script on this page is causing Internet Explorer to run slowly. If it continues to run, your computer may become unresponsive." when configuring device.
   Please update IE patch: http://support.microsoft.com/kb/175500 for fixing this issue

ZYXEL

Interface

1. [SPR: 100105242, 100105292]

    [Symptom]

    PPTP might not be able to connect successfully if it is configured via Installation Wizard/Quick Setup. This is because:

    1. Installation Wizard/Quick Setup only allows PPTP based interface to be configured with Static IP.

    2. Installation Wizard/Quick Setup doesn't allow user to configure PPTP based interface's Gateway IP Address. This may cause PPTP cannot connect successfully if the PPTP Server IP is not at the same subnet with PPTP's based interface

    [Workaround]

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

IPSec VPN

1. [SPR: 070814168]

    [Symptom]

    VPN tunnel could not be established when:

    1. a non ZyWALL/USG peer gateway reboot and

    2. ZyWALL/USG has a previous established Phase 1 with peer gateway, and the Phase 1 has not expired yet. Under those conditions, ZyWALL/USG will continue to use the previous phase 1 SA to negotiate the Phase 2 SA. It would result in phase 2 negotiation to fail.

    [Workaround]

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

2. [SPR: 100429119]

    [Symptom]

    VPN tunnel might be established with incorrect VPN Gateway

    [Condition]

    1. Prepare 2 ZyWALL/USG and reset to factory default configuration on both ZyWALL/USGs

    2. On ZyWALL/USG-A:

        1. Create 2 WAN interfaces and configure WAN1 as DHCP Client

        2. Create 2 VPN Gateways. The "My Address" is configured as Interface type and select WAN1 and WAN2 respectively

3. Create 2 VPN Connections named VPN-A and VPN-B accordingly which bind on the VPN Gateways we just created

3. On ZyWALL/USG-B

1. Create one WAN interface

2. Create one VPN Gateway. The Primary Peer Gateway Address is configured as WAN1 IP address of ZyWALL/USG-A and the Secondary Peer Gateway Address is configured as WAN2 IP address of ZyWALL/USG-A

4. Connect the VPN tunnel from ZyWALL/USG-B to ZyWALL/USG-A and we can see VPN-A is connected on ZyWALL/USG-A

5. Unplug WAN1 cable on ZyWALL/USG-A

6. After DPD triggered on ZyWALL/USG-B, the VPN Connection will be established again

7. On ZyWALL/USG-A, VPN-A is connected. But actually ZyWALL/USG-B should connect to VPN-B after step 5.

[Workaround]

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

3. [SPR: 140304057]

[Symptom]

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

1. IPv4 rules with IKEv2 version

2. IPv4 rules with User-based PSK authentication

3. IPv6 rules

SSL VPN

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

ZYXEL

Applications Operating System	Full Tunnel Mode	Reverse Proxy Mode	RDP	VNC
		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 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 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 Chrome 44.x or previous version Firefox latest version Safari latest version	Internet Explorer 10.x, 11.x	Internet Explorer 10.x, 11.x Chrome 44.x or previous version Firefox latest version Safari latest version
Windows 8, 8.1 (X32) Java 7u45 or later	Internet Explorer 10.x, 11.x Chrome 45.x, 49.x, 50.x to latest version Firefox latest version Safari latest version	Internet Explorer 10.x, 11.x Chrome 45.x, 49.x, 50.x to latest version Firefox latest version Safari latest version	Internet Explorer 10.x, 11.x	Internet Explorer 10.x, 11.x Chrome 45.x, 49.x, 50.x to latest version Firefox latest version Safari latest version
Windows 10 (X64) Java 7u45 or later	Internet Explorer 11.x Chrome 45.x, 49.x, 50.x to latest version Firefox latest version edge latest version	Internet Explorer 11.x Chrome 45.x, 49.x, 50.x to latest version Firefox latest version edge latest version	Internet Explorer 11.x	Internet Explorer 11.x Chrome 45.x, 49.x, 50.x to latest version Firefox latest version
MAC OSX (10.9) Java 7	Safari latest version Chrome latest version Firefox latest version	Safari latest version Chrome latest version	Not support	Firefox 45.0.x

ZYXEL

2. [SPR: 100419034]

[Symptom]

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

L2TP VPN

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

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

2. [SPR: N/A]

[Symptom]

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

User Aware

1. [SPR: 070813119]

[Symptom]

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

[Workaround]

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

IPv6

1. HTTP/HTTPS not support IPv6 link local address in IE7 and IE8.

2. Windows XP default MS-DOS FTP client cannot connection to device's FTP server via iPv6 link-local address.

3. [SPR: 110803280]

[Symptom]

Safari cannot log in web with HTTPS when using IPv6

ZYXEL

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]

   1. Topology:

      PC1 ---LAN1 USG60W WAN1 ---- WAN1 USG60 LAN1 --- PC2 & PC3

   2. USG60W

      WAN1: 10.1.4.45/24

      WAN2: 192.168.9.x/24 (Can reach to 172.23.x.x network through NAT router.)

      LAN1: 192.168.181.x/24

      PC1: 192.168.181.33

   3. USG60

      WAN1: 10.1.6.79/24

      LAN1: 192.168.1.1/24

      PC2: 192.168.1.33

      PC3: 192.168.1.34

   4. USG60 sets a policy route, src=192.168.1.0/24, dst=172.0.0.0/8, next-hop=VPN tunnel

      USG60W sets

      1. policy route, src= 172.0.0.0/8, dst=192.168.1.0/24, next-hop=VPN tunnel

      2. policy route, src=192.168.1.0/24, dst=172.0.0.0/8, next-hop=WAN2

5. PC2 ping 172.23.x.x is OK
6. Add a 1:1NAT rule which is from WAN1 10.1.6.79 mapping to 192.168.1.34 (PC3) on USG60.
7. PC2 ping 172.23.x.x will fail now.
8. Disable 1:1 NAT rule.
9. PC2 still cannot ping to 172.23.x.x.
   *Need to reboot device or wait several minutes, it works.

4. [SPR: 141209575]

    [Symptom]

    IPSec VPN tunnel sometimes can be built up while initiator and responder devices use CA with the same subject name in IKE authentication. This tunnel should not be allowed to build.

5. [SPR: 160106369]

    [Symptom]

    To set up Local ID type in "DNS" mode at Advance setting under IPSec > VPN Gateway > Edit or Add page to make sure the Certificate works normally.

    [Workaround]

    If you are using certificate under the other modes, please go through VPN wizard then login again to VPN Gateway GUI page to modify the setting.

IPv6

1. [SPR: 131226738]

    [Symptom]

    Only one prefix delegation can be added in IPv6 address assignment.

SSL VPN

1. [SPR: N/A]

    [Symptom]

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

    [Workaround]

    You can configure Windows cipher with following information
    http://support.microsoft.com/kb/980868/en-us

2. [SPR: 121203072]

    [Symptom]

    Ext-group name and any password can login SSL VPN

3. [SPR: 160307230]

    [Symptom]

ZYXEL

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

4. [SPR: 160309776]

[Symptom]

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

5. [SPR: 160324728]

[Symptom]

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

System

1. [SPR: 130207529]

[Symptom]

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

2. [SPR: 150529308]

[Symptom]

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

3. [SPR: 160420343]

[Symptom]

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

4. [eITS: 170100444]

[Symptom]

Link sticking/Route Cache for dual WAN cannot work correctly with 4.25 as new implementation will be added at 4.30 Firmware.

GUI

1. [SPR: 151127016]

[Symptom]

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

[Workaround]

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

2. [SPR: 151208533]

ZYXEL

[Symptom]

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

3. [SPR: 151208561]

[Symptom]

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

4. [SPR: 151214778]

[Symptom]

After the IPv4 address object created by "Create New Object" there's no updated IPv4 address object in IP address Pool list in Configuration > VPN >IPSec VPN >VPN connection >IPv4 Configuration > Add page.

[Workaround]

Close the "Add VPN Configuration" window and re-open again.

5. [SPR: 151217001]

[Symptom]

GUI always show "Loading…" message after apply below steps:

1. Apply system default configuration.

2. In[Configuration＞VPN＞IPSec VPN＞VPN Gateway]page, add one rule

   Enable, Name: ike1, interface: wan1 , static address: 10.1.4.x , pre-shared key:12345678

3. In[Configuration＞VPN＞IPSec VPN＞VPN Connection]page, add one rule

4. Enable, Name: ipsec1, site-to-site , VPN gateway : ike1, local policy: LAN1_subnet ,

   remote policy: remote_subnet(use create new object-＞ IPv4 address, Name:

   remote_subnet, address type: subnet, network: 192.168.11.0 , netmask: 255.255.255.0)

5. In[Configuration＞VPN＞IPSec VPN＞VPN Gateway]page, edit ike1 rule

6. GUI always show "Loading…".

[Workaround]

Refresh GUI

6. [SPR: 151223305]

[Symptom]

The changes of "E-mail Server 2"column will not applied after reboot device at Configuration > Log & Report > Log settings > System Log > Active Log and Alert (AP) page.

ZYXEL

7. [SPR: 160411770]

    [Symptom]

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

8. [SPR: 160503266]

    [Symptom]

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

9. [SPR: 161219973]

    [Symptom]

    By using copy and paste to set PPPoE/PPTP IP address on Installation Setup Wizard. "Next" button can't be pressed.

10. [SPR: 170213467]

    [Symptom]

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

11. [SPR: 170328262]

    [Symptom]

    Network risk warning information show null on ZyWALL series device

12. [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.

3G Dongle

1. [SPR: 161215667]

    [Symptom]

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

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	Default 30days trial
USG210 ZyWALL 110	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

ZYXEL

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]

ZYXEL

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

ZYXEL

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.

ZYXEL

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.

ZYXEL

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, "425ABAR0C0.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.

ZYXEL

- 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 (**425ABAR0C0-enterprise.mib** and **425ABAR0C0-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.

ZYXEL

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
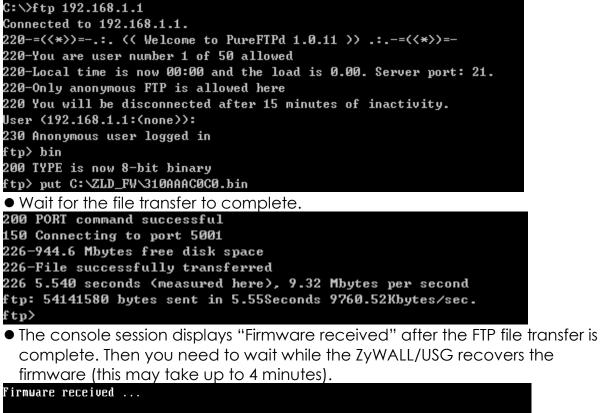
```
ZyWALL 1100> atgof

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.
```

ZYXEL

- 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.

ZYXEL

```
...............................................................................
...............................................................................
...............................................................................
...............................................................................
...............................................................................
...............................................................................
.....
        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!!