ZyXEL

Firmware Release Note

USG60W

Release V4.11(AAKZ.2)C0

Date: April 28, 2015
Author: Shang Lee
Project Leader: Shang Lee

Contents

ZyXEL USG60W

Release V4.11(AAKZ.2)C0

Release Note

Date: April 28, 2015

Supported Platforms:

ZyXEL USG60W

Versions:

ZLD Version: V4.11(AAKZ.2) | 2015-04-20 17:22:36
Boot Module Version: V1.02 | Jul 10 2014 14:05:59

Files lists contains in the Release ZIP file

File name: 411AAKZ2C0.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: 411AAKZ2C0.conf
Purpose: This ASCII file contains default system configuration commands.

File name: 411AAKZ2C0.pdf
Purpose: This release file.

File name: 411AAKZ2C0.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: 411AAKZ2C0-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: 411AAKZ2C0-enterprise.mib, 411AAKZ2C0-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: 411AAKZ2C0-opensource-list.xls

Purpose: This file lists the open source packages.

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

Purpose: Mobile broadband dongle support list.

Read Me First

1. The system default configuration is summarized as below:
   - The default device administration username is “admin”, password is “1234”.
   - The default LAN interface is ge3, which are P3 port on the front panel. The default IP address of lan1 is 192.168.1.1/24.
   - By default, WWW/SSH/SNMP service can only be accessed from LAN subnet.
   - The default WAN interface is ge1, and the secondary WAN interface is ge2. These two interfaces will automatically get IP address using DHCP by default.
2. 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.
3. If user upgrades from previous released firmware to this version, there is no need to restore to system default configuration.
4. 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.
5. 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.
6. If ZyWALL/USG can’t reboot successfully after firmware upgrade, please refer to Appendix 3: Firmware Recovery.

Design Limitations:

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

APP Patrol

1. [SPR: 140425359, 140425375]
   [Symptom]
   If a profile is to block browser only (ex. Chrome, IE), it may not take effect because "user access website" have higher priority for matching.

Build in Service

1. [SPR: 061208575]
   [Symptom]
   If users change port for built-in services (FTP/HTTP/SSH/TELNET) and the port conflicts with other service or internal service, the service might not be brought up successfully. The internal service ports include 50001/10443/10444/1723/2601-2604/953. 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. [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 open the Site Map's help page.[SPR: 100914249][Symptom]IE7/8 sometimes shows "Stop running this script? A script on this page is causing Internet Explorer to run slowly. If it continues to run, your computer may become unresponsive." when configuring device. Please update IE patch: http://support.microsoft.com/kb/175500 for fixing this issue

Interface

1. [SPR: 100105242, 100105292]

   [Symptom]

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

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

   [Workaround]

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

IPsec VPN

1. [SPR: 070814168]

   [Symptom]

   VPN tunnel could not be established when:

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

   [Workaround]

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

2. [SPR: 100429119]

   [Symptom]

   VPN tunnel might be established with incorrect VPN Gateway

   [Condition]

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

1. Create 2 WAN interfaces and configure WAN1 as DHCP Client
2. Create 2 VPN Gateways. The “My Address” is configured as Interface type and select WAN1 and WAN2 respectively
3. Create 2 VPN Connections named VPN-A and VPN-B accordingly which bind on the VPN Gateways we just created

3. On ZyWALL/USG-B
   1. Create one WAN interface
   2. Create one VPN Gateway. The Primary Peer Gateway Address is configured as WAN1 IP address of ZyWALL/USG-A and the Secondary Peer Gateway Address is configured as WAN2 IP address of ZyWALL/USG-A
4. Connect the VPN tunnel from ZyWALL/USG-B to ZyWALL/USG-A and we can see VPN-A is connected on ZyWALL/USG-A
5. Unplug WAN1 cable on ZyWALL/USG-A
6. After DPD triggered on ZyWALL/USG-B, the VPN Connection will be established again
7. On ZyWALL/USG-A, VPN-A is connected. But actually ZyWALL/USG-B should connect to VPN-B after step 5.

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

3. [SPR: 140304057]
   [Symptom]
   After inactivating GRE over IPsec, old connection may remain if the traffic flows continuously. This may cause traffic bounded with old connection.
   [Workaround] Stop traffic for 180 seconds and the internal connection record will time out.
4. [SPR: 140416738]
   [Symptom]
   Ignore don’t fragment setting cannot take effect immediately if there already existed the same connection.
   [Workaround] Stop traffic for 180 seconds and the internal connection record will time out.

SSL VPN

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

Applications Operating System	Full Tunnel Mode	Reverse Proxy Mode File Sharing(Web-based Application)	RDP	VNC
Windows 7 (X64) (SP1) Java 7 -	Internet Explorer 8.x, 9.x, 10.x, 11.x Chrome latest version Firefox latest version Opera latest version	Internet Explorer 8.x, 9.x, 10.x, 11.x Chrome latest version Firefox latest version -	Internet Explorer 8.x, 9.x, 10.x, 11.x	Internet Explorer 8.x, 9.x, 10.x, 11.x Chrome latest version Firefox latest version -

	Safari latest version	Safari latest version		Safari latest version
Windows 7 (X32) (SP1) Java 7 -	Internet Explorer 8.x, 9.x, 10.x, 11.x Chrome latest version Opera latest version Safari latest version	Internet Explorer 8.x, 9.x, 10.x, 11.x Chrome latest version Firefox latest version - Safari latest version	Internet Explorer 8.x, 9.x, 10.x, 11.x	Internet Explorer 8.x, 9.x, 10.x, 11.x Chrome latest version Firefox latest version - Safari latest version
Windows 8 (X64) Java 7	Internet Explorer 10.x, 11.x Chrome latest version Firefox latest version Safari latest version	Internet Explorer 10.x, 11.x Chrome latest version Firefox latest version Safari latest version	Internet Explorer 10.x, 11.x	Internet Explorer 10.x, 11.x Chrome latest version Firefox latest version Safari latest version
Windows 8 (X32) Java 7	Internet Explorer 10.x, 11.x Chrome latest version Firefox latest version Safari latest version	Internet Explorer 10.x, 11.x Chrome latest version Firefox latest version Safari latest version	Internet Explorer 10.x, 11.x	Internet Explorer 10.x, 11.x Chrome latest version Firefox latest version Safari latest version
MAC OSX 10.9 Java 7	Safari 7.0.x Chrome 33.0.x Firefox 27.0.x	Safari 7.0.x Firefox 27.0.x	Not support	Firefox 27.0.x

2. [SPR: 100419034]

   [Symptom]

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

L2TP VPN

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

L2TP Client	OS type	Client Version
Windows L2TP client	Windows 7 32/64 Windows 8 32/64	
iPhone/iPAD L2TP client	iPhone5 iPAD	6.1.2 6.1.2
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)

Device-HA

1. [SPR: N/A]
   [Symptom]
   Backup may send out traffic through its physical MAC address when booting system or during device-HA syncing (a short period)
   [WORKAROUND]
   Set short ARP timeout value on monitored interface's switch and gateway side.

MAC Authentication

1. [SPR: 150127103]
   [Symptom]
   Client use Internal MAC-Auth connection Auth. Server can’t get IP successful.
   [WORKAROUND]
   Set short ARP timeout value on monitored interface's switch and gateway side.

Wireless

1. [SPR: 150127103]

   [Symptom]

   MAC authentication use internal and auth. method set USG, wireless client can’t get IP successful.

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: 150213841]
   [Symptom]
   Not support IKEv2 VPN Configuration Provisioning, so the configuration may apply failed in the following conditions.
   [Condition]
   1. Create phase1 rule a1(ikev1) and a2(ikev2).
   2. Create phase2 rule b with VPN gateway rule a1.
   3. Add one VPN provisioning rule with VPN connection rule b.
   4. Change VPN connection rule b from a1 to a2.
   5. Reboot device, it will apply configuration fail.

IPv6

1. [SPR: 131226738]
   [Symptom]
   Only one prefix delegation can be added in IPv6 address assignment.
2. [SPR: 141125082]
   [Symptom]
   DHCPv6 relay cannot work.

AppPatrol

1. [SPR: 140605105]
   [Symptom]
   DUT cannot block Facebook message.
2. [SPR: 140605113]
   [Symptom]
   DUT cannot block Facebook link/share.
3. [SPR: 140605136]
   [Symptom]
   [App Patrol] Cannot block Skype off-line message

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

System

1. [SPR: 130207529]
   [Symptom]
   When change SSH, Telnet and FTP Service default port, the connect session still exist.

ADP

1. [SPR: 141211702, 150116760]
   [Symptom]
   IPv6 IKE, ICMPv6 packets with size too big to be fragmented may cause false alarm by ADP and block these traffics.

GUI

1. [ITS: 150301008]
   [Symptom]
   It is unable to edit DNS Security Option default rule in GUI.

Features: V4.11(AAKZ.2)C0

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

1. [BUG FIX] eITS#150301005, 150400012

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

Features: V4.11(AAKZ.1)C0

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

1. [BUG FIX] eITS#150301160
   Content Filter doesn't work at all after 4.11 upgrade.
2. [BUG FIX] eITS#150200801
   Radius daemon will fail to launch if the radius server (in AAA server) is configured with domain name and DNS is not ready during device boot-up.

Features: V4.11(AAKZ.0)C0

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

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

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

15. [BUG FIX] eITS#150100588

    Apply configuration failed in the following steps:

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

16. [BUG FIX] eITS#141100503

    Strange behavior when ZyWALL is in DNS proxy role.

    [Condition]

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

17. [BUG FIX] eITS#141200186

    After enabling AS, the throughput is low.

18. [BUG FIX] eITS#141200341, 141200033

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

19. [BUG FIX] eITS#141001029

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

20. [BUG FIX] eITS#141100574

    After rebooting, WAN gateway will disappear.

21. [BUG FIX] eITS#141100745

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

22. [BUG FIX] eITS#141000415

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

23. [BUG FIX] eITS#141100945

    Device HA failed to synchronize backup device with master device.

24. [BUG FIX] eITS#141200132

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

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

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

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

39. [BUG FIX] eITS#140900272

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

40. [BUG FIX] eITS#141100569

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

41. [BUG FIX] eITS#150100603

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

Features: V4.10(AAKZ.2)C0

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

1. [ENHANCEMENT] eITS#140600094
   Update driver to fix IOP issue with Genexis FiberXport device.
2. [ENHANCEMENT]
   Add CLI to show the mapping for internal and external interface. CLI: “debug interface show mapping”
3. [ENHANCEMENT] eITS#141000162
   Change log format as following:
   Before:
   category=”ipsec” level=”error” src=”” dst=”” msg=”Failed to send packet, err=N”N: 1 or 2
   After:
   category=”ipsec” level=”debug” src=”<source and port of packet>” dst=”<destination and port of packet>” msg=”Packet(PROTOCOL) cannot be sent, reason: REASON”
   PROTOCOL: ESP/AH/TCP/UDP/Unknown(protocol number)
   REASON: System dropped/Network congestion/Traffic control dropped
4. [ENHANCEMENT]
   Update bash binary for shellshock bash vulnerability issue
5. [ENHANCEMENT] eITS#140900846
   Support Huawei E303 USB 3G dongle with version 22.318.27.00.00
6. [ENHANCEMENT]
   Add SNMP VPN status and connection counter MIBs.
   The VPN status MIB is a MIB table containing the following information:
   Connection name, VPN gateway, IP version, active status, and connected status.
   The VPN connection counter is a MIB group containing:
   Total VPN connection configured, number of activated connection, number of connected connection, and number disconnected connection.
   Followings are the example of snmpwalk for the added MIBs;
   VPN status MIB table:
   1.3.6.1.4.1.890.1.6.22.2.4.1.1.1 = INTEGER: 1 --> table index
   1.3.6.1.4.1.890.1.6.22.2.4.1.1.2 = INTEGER: 2
   1.3.6.1.4.1.890.1.6.22.2.4.1.1.3 = INTEGER: 3
   1.3.6.1.4.1.890.1.6.22.2.4.1.2.1 = STRING: ""vpnconn1"" --> name
   1.3.6.1.4.1.890.1.6.22.2.4.1.2.2 = STRING: ""vpnconn2""
   1.3.6.1.4.1.890.1.6.22.2.4.1.2.3 = STRING: ""vpn6conn1""
   1.3.6.1.4.1.890.1.6.22.2.4.1.3.1 = STRING: ""usg110_1"" --> gateway

1.3.6.1.4.1.890.1.6.22.2.4.1.3.2 = STRING: ""usg110_1""
1.3.6.1.4.1.890.1.6.22.2.4.1.3.3 = STRING: ""vpn6_1""
1.3.6.1.4.1.890.1.6.22.2.4.1.4.1 = STRING: ""IPv4"" --> IP version
1.3.6.1.4.1.890.1.6.22.2.4.1.4.2 = STRING: ""IPv4""
1.3.6.1.4.1.890.1.6.22.2.4.1.4.3 = STRING: ""IPv6""
1.3.6.1.4.1.890.1.6.22.2.4.1.5.1 = INTEGER: 0 --> active status
1.3.6.1.4.1.890.1.6.22.2.4.1.5.2 = INTEGER: 1
1.3.6.1.4.1.890.1.6.22.2.4.1.5.3 = INTEGER: 1
1.3.6.1.4.1.890.1.6.22.2.4.1.6.1 = INTEGER: 0 --> connected status
1.3.6.1.4.1.890.1.6.22.2.4.1.6.2 = INTEGER: 0
1.3.6.1.4.1.890.1.6.22.2.4.1.6.3 = INTEGER: 0

VPN connection counters:

1.3.6.1.4.1.890.1.6.22.2.5.1.0 = Counter32: 3 --> total connection configured
1.3.6.1.4.1.890.1.6.22.2.5.2.0 = Counter32: 2 --> number of active connection
1.3.6.1.4.1.890.1.6.22.2.5.3.0 = Counter32: 0 --> number of connected connection
1.3.6.1.4.1.890.1.6.22.2.5.4.0 = Counter32: 2 --> number of disconnected connection

The number of disconnected connection is equal to the number of active connection minus the number of connected connection"

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

    [Condition]

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

WAS: WLAN bind with lan1 by default

IS: WLAN bind with lan2 by default

14. [FEATURE CHANGE]

WAS:

Log entry is 256

IS:

Log entry is 512

PS: For ZyWALL 310 and USG310 only

15. [FEATURE CHANGE]

WAS:

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

IS:

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

Please refer to KB:

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

16. [BUG FIX] eITS#140900194

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

17. [BUG FIX] eITS#140800834

USG with wrong CEF syslog format

18. [BUG FIX] eITS#140800642

Device HA status not changed when monitored interface IP changed

19. [BUG FIX] eITS#141000158

SSLVPN reverse proxy RDP cannot work

20. [BUG FIX] eITS#140900380

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

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

Static ARP entry will gone if enabling device HA

22. [BUG FIX] eITS#141000171

USG boot up makes switch function("Loop Guard") blocking port

23. [BUG FIX] eITS#141000157

False alarm in CAPWAP protocol in ADP engine

24. [BUG FIX] eITS#141000155

IKE packet sent at wrong interface and wrong IP

25. [BUG FIX] eITS#141000458

DHCP will clear static ARP entry after send DHCP ACK

26. [BUG FIX] eITS#141001108

USG110 cannot load Firmware if USB memory stick connected

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

    ZyWALL 1100 - VPN connect fail and hang

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

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

Features: V4.10(AAKZ.1)C0

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

Release for manufacturing

Features: V4.10(AAKZ.0)C0

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

First release

Appendix 1. Firmware upgrade / downgrade procedure

The following is the firmware **upgrade** procedure:

1. If user did not backup the configuration file before firmware upgrade, please follow the procedures below:
   - Use Browser to login into ZyWALL/USG as administrator.
   - Click Maintenance > File Manager > Configuration File to open the Configuration File Screen. Use the Configuration File screen to backup current configuration file.
   - Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a .bin extension, for example, "411AAKZ2C0.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 (**411AAKZ2C0-enterprise.mib** and **411AAKZ2C0-private.mib**) and install to your MIBs application (like MIB-browser). You can see 410AAPJ2C0-private.mib (OLD is 1.3.6.1.4.1.890.1.6.22).
2. ZyWALL/USG SNMP is enabled.
3. Using your MIBs application connects to ZyWALL/USG.
4. SNMPv2 private MIBs support three kinds of status in ZyWALL/USG:
    1. CPU usage: Device CPU loading (%)
    2. Memory usage: Device RAM usage (%)
    3. 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!!