www.zyxel.com

Release Note

USG FLEX 500

Version 5.39(ABUJ.0)C0

August 22, 2024

Contents

USG FLEX 500

Release V5.39(ABUJ.0)C0

Release Note

Date: August 22, 2024

Supported Platforms:

USG FLEX 500

Versions:

ZLD Version: V5.39(ABUJ.0) | 2024-08-22 02:14:33

Files lists contains in the Release ZIP file

File name: 539ABUJ0C0.bin
Purpose: This binary firmware image file is for normal system update.
Note: The firmware update may take five minutes or more depending on the scale of device configuration. The more complex the configuration is, the longer the update time will be. Do not turn off or reset the ZyWALL Firewall while the firmware update is in progress. The firmware might damage if device loses 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: 539ABUJ0C0.conf
Purpose: This ASCII file contains default system configuration commands.

File name: 539ABUJ0C0.pdf
Purpose: This release file.

File name: 539ABUJ0C0.ri
Purpose: This binary firmware recovery image file is for emergent system firmware damage recovery only.

Note: The ZyWALL Firewall firmware could be damaged, for example if the device is powered off or the Reset button is pressed in the middle of firmware update process.

File name: USG FLEX 500_V5.39(ABUJ.0)C0-foss.pdf
Purpose: The PDF file is ZNet only grants you the software license declaration document.

Read Me First

1. The system default configuration is summarized as below:
   - The default device administration username is "admin", password is "1234".
   - The default LAN interface is lan1, which are P3 port on the front panel. The default IP address of ge4 is 192.168.1.1/24.
   - By default, WWW/SSH/SNMP service can only be accessed from LAN subnet.
   - The default WAN interface is wan, the interfaces will automatically get IP address using DHCP by default.
   - For new model, requires connecting to myZyxel to complete device registration and Security Service activation.
2. 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 a previous firmware version.
3. Please **DO NOT** turn off the power during the firmware upgrade. Please wait until the device reboots and the SYS light stays on
4. We recommended upgrade to ZLD5.38C0 or later version to **Standby partition** first before upgrading to ZLD5.39.
5. When getting troubles in configuring via GUI (popup java script error, etc.), it is recommended to clear browser's cache first and try to configure again.
6. To reset device to system default, user could press RESET button for 5 seconds and the device would reset itself to system default configuration and then reboot.
   - Note: After resetting, the original configuration would be removed. It is recommended to back up the configuration before this operation.
7. If ZyWALL Firewall can't reboot successfully after firmware upgrade, please refer to Appendix 3: Firmware Recovery.

8. [APC] Support AP List

APC Version	ZLD version	Support AP (Managed AP)
APC6.75	ZLD5.39	NWA3160-N NWA3550-N NWA3560-N NWA5160N NWA5550-N NWA5560-N NWA5121-NI NWA5123-NI NWA5121-N NWA5301-NJ WAC6502D-E WAC6502D-S WAC6503D-S WAC6553D-E WAC6552D-S WAC6103D-I NWA5123-AC WAC5302D-S NWA5123-AC-HD WAC6303D-S WAX650S WAX510D WAX610D WAC5302D-Sv2 WAC500 WAC500H WAX630S WAX640S-6E WAX620D-6E WAX655E WAX300H WBE660S

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 53/179/953/1723/2158/2601-2605/10443/10444/11080/50001. 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: 150122977]
   [Symptom]
   DNS security option will deny device local out DNS query
   [Condition]
   a. Edit the customize rule of DNS security option, and set the query recursion as deny.
   b. If device's WAN IP address is in the customize address range, device local-out DNS query will be denying.

GUI

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

Operating System	For Administrator Login Browsers	For User Login Browsers
Windows 10 (X64)	Safari 5.1.7(7534.57.2) or later	Safari 5.1.7(7534.57.2) or later
	Edge 20.10240.16384.0 or later	Edge 20.10240.16384.0 or later
	Firefox 50.0.2 or later	Firefox 50.0.2 or later
	Opera 47.0.2631.55 or later	Opera 47.0.2631.55 or later
	Chrome latest version 60.0.3112.101	Chrome latest version 60.0.3112.101
	Safari latest version 10.1.2(12603.3.8)	Safari latest version 10.1.2(12603.3.8)
Linux OS (Ubuntu)	Firefox latest version 50.0.2	Firefox latest version 50.0.2
	9 latest version 9.3.3 (Safari)	Safari 9 latest version 9.3.3

Apple MAC OS X	10 latest version 10.3.2 (Safari)	Safari10 latest version 10.3.2
	latest version 5.0 (Chrome)	latest version 5.0 (Chrome)
	Firefox latest version	Firefox latest version
Apple iOS (Tablet)	Latest Safari version 13.1.2/ 14.1/15.0	Latest Safari version 13.1.2/ 14.1/15.0
	latest version 5.0 (Chrome)	latest version 5.0 (Chrome)
Android (Tablet)	Chrome 59.0.3071.115 or later	Chrome 59.0.3071.115 or later

* Not support Opera browser 10.6x

* Not support Mobile OS

2. [SPR: 171030438]

[Symptom]

IE browser will download the privacy statement when accessing the related page, instead of reading on browser.

IPSec VPN

1. [SPR: 070814168]

[Symptom]

VPN tunnel could not be established when:

a. a non ZyWALL Firewall peer gateway reboot and

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

2. [SPR: 100429119]

[Symptom]

VPN tunnel might be established with incorrect VPN Gateway

[Condition]

a. Prepare 2 ZyWALL Firewall and reset to factory default configuration on both ZyWALL Firewalls

b. On ZyWALL Firewall-A:

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

c. On ZyWALL Firewall-B
   - Create one WAN interface
   - Create one VPN Gateway. The Primary Peer Gateway Address is configured as WAN1 IP address of ZyWALL Firewall-A and the Secondary Peer Gateway Address is configured as WAN2 IP address of ZyWALL Firewall-A

d. Connect the VPN tunnel from ZyWALL Firewall-B to ZyWALL Firewall-A and we can see VPN-A is connected on ZyWALL Firewall-A
e. Unplug WAN1 cable on ZyWALL Firewall-A
f. After DPD triggered on ZyWALL Firewall-B, the VPN Connection will be established again
g. On ZyWALL Firewall-A, VPN-A is connected. But actually ZyWALL Firewall-B should connect to VPN-B after step 5.

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

3. [SPR: 120110586]
   [Symptom]
   When user 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
4. [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.
5. [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.
6. The following VPN Gateway rules configured on the ZyWALL Firewall cannot be provisioned to the IPSec VPN Client:
   a. IPv4 rules with IKEv2 version

b. IPv4 rules with User-based PSK authentication
c. IPv6 rules

7. Not support site to site VPN behind NAT scenario both in On-Premises mode and On-Cloud mode

SSL VPN

1. Following are the list for SSL VPN supporting applications and operating systems:
   - SecuExtender SSL VPN Client support: Windows 10/11 (32- and 64-bit) and macOS 10.15 or later version.

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 10/11 (32- and 64-bit)
iPhone/iPad L2TP client	iOS 15 or later
Mac L2TP client	macOS 10.15 or later

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 don't support IPv6 link local address in IE7 and IE8.
2. Windows XP default MS-DOS FTP client cannot connect to device's FTP server via iPv6 link-local address.
3. [SPR: 110803280]
   [Symptom]
   Safari cannot log in web with HTTPS when using IPv6
4. [SPR: 110803293]
   [Symptom]
   Safari fails to redirect http to https when using IPv6
5. [SPR: 110803301]
   [Symptom]
   Safari with IPv6 http login when change web to System > WWW, it pops up a logout message. (HTTP redirect to HTTPS must enable)

MAC Authentication

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

SecuExtender SSL VPN Client

1. Windows 7 users who have not executed Windows update before may have issues with SecuExtender virtual Network interface card detection.
   [Workaround]
   It's recommended to install all windows security patches before installing SecuExtender.
   One of reference: https://support.microsoft.com/en-us/kb/3033929

Anti-Malware

1. [SPR: 181205082]
   [Symptom]
   Cloud Query FTP protocol Conditional support: Depends on File Server.

Known Issues:

Note: These known issues listed below represent are not fixed in the current firmware release. And we already plan to fix them in the future firmware release.

[On Premises mode]

IPSec VPN

1. [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.
2. [SPR: 171108122]
   [Symptom]
   The number of VPN connected tunnels in VPN Dashboard may display incorrectly under stress with Zyxel VPN client
3. [SPR: 210128308]
   [Symptom]
   [Crash][IPSec VPN] DUT had crash when send mail via Bridge VPN.
4. [SPR: 210917118]
   [Symptom]
   The VPN authentication failed with external user which is not in the first order of authentication method profile
   [Workaround]
   Move AAA server stores external user to the first order of authentication method profile.

IPv6

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

SSL VPN

1. [SPR: N/A]
   [Symptom]
   Windows 7 users cannot use SSL cipher suite selection as AES256.

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

2. [SPR: 160309776]
[Symptom]
GUI login can't auto connect/disconnect new SecuExtender tool in windows.
3. [SPR: 170517424]
[Symptom]
SecuExtender after ZLD4.30 will not support Windows XP due to strong cipher suite activated by default. Please upgrade client OS or allow ZLD with unsecure cipher suite via CLI, "no ip http secure-server strong-cipher".

SSL Inspection

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

Wireless

1. [SPR: 150701137]
[Symptom]
Try to manage too many external APs over service/license count may cause capwap_srv daemon dead.
2. [SPR: 151119567]
[Symptom]
When AP firmware fails to synchronize with cloud server, alert log will display frequently
3. [SPR: 151208470]
[Symptom]
When AP firmware download failed from cloud server, exist AP firmware will be deleted and GUI show "to be downloaded" message at Configuration > Wireless >AP Management >Firmware page.
4. [SPR: 151203302]
[Symptom]

It takes 30 seconds or above to update the AP controller information when using Zyxel Wireless Optimizer (ZWO) tool to monitor the status.

5. [SPR: 160603272]
   [Symptom]
   AP traffic Tx/Rx value show incorrectly in Email Daily Report.
6. [SPR: 170830306]
   [Symptom]
   [Station info] When client from 2.4G Wi-Fi to 5G Wi-Fi, the station info will show client connect to 2.4G Wi-Fi.
7. [eITS: 191200588]
   [Symptom]
   The station gets wrong VLAN IP addresses in Dynamic VLAN when it roams.
   [Workaround] set reauth time to 0.
8. [eITS: 191200915 / 191200600]
   [Symptom]
   AP may reboot unexpectedly with LLDP application.
   [Workaround] Disable LLDP.
9. [eITS: 200800669, 200801106, 200901105]
   [Symptom]
   The station cannot surf the internet or get disconnect very frequency. (WAC6303D-S)
   [Workaround] Ask date firmware from ZYXEL.
10. [eITS: 200900430]
    [Symptom]
    We can see “cron daemon dead” in the logs.
11. [eITS: 200901198]
    [Symptom]
    The AP can’t upgrade the firmware successfully from NXC or the Controller device.
    [Workaround] Reboot the Controller device.
12. [eITS: 200900931]
    [Symptom]
    When the customer click preview in Configuration > Captive portal > Custom captive portal, it’s not able to show in Chrome browser.
13. [SPR: 201217349]
    [Symptom]
    MAC-User cannot be applied in firewall or routing rule.

14. [SPR: 201223508]
    [Symptom]
    AP information will not hide advanced settings after reloading the page.
15. [eITS: 210200970]
    [Symptom]
    NWA1123ACv3 --- LTE3316 --- 4G NWA1123ACv3 cannot be online. Must adjust MTU size of the AP to be smaller to make it be online.
16. [eITS: 210300463]
    [Symptom]
    Enable 5 GHz DFS Aware wording in Chinese is incorrect.
17. [Symptom] AP Firmware update will fail when using FTP
    [Solution] Please use CAPWAP to update AP firmware.

APC

1. [eITS: 210800912]
   [Symptom]
   SSID schedule may not work if APC enables daylight saving setting.

GUI

1. [SPR: 171016187]
   [Symptom]
   Easy mode > click Network Client list button may cause page always loading status
2. [SPR: N/A]
   [Symptom]
   Sometimes GDPR dialog will be blocked by device dashboard loading mask. Please move the dialog to usable place for advanced operations or wait for the loading mask finished.
3. [SPR: 210916116]
   [Symptom]
   After changing from Built-in AP mode to Controller mode, the Monitor > Wireless > Wireless Health will keep loading
4. [SPR: 220302038]
   [Symptom]
   The description field does not support "," symbol and a warning message will be displayed to notify the user to modify.

Device HA Pro

1. [SPR: 160226958]
   [Symptom]
   When the physical interface link down, the HTTP file downloading will terminate after failover to passive device.
2. [SPR: 160623509]
   [Symptom]
   Upgrade firmware from Active device and the upgrade process is to upgrade Passive device first. After Passive device finished firmware upgrade it will show device sync fail because of Active device is doing firmware upgrade and reboot.

3G Dongle

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

Anti-Malware

1. [SPR: 171222271]
   [Symptom]
   Anti-Malware can't detect eicar.txt by upload with HTTP 8080 port.
2. [SPR: N/A]
   [Symptom]
   The behavior of file-captured by http uploading is not supported yet.

ALG

1. [SPR: 180504123]
   [Symptom]
   Sandbox, Anti-malware FTP port cannot support multiple ports.

Remote Access VPN wizard

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

Routing traces

1. [SPR: 210310085]
   [Symptom]
   When device with heavy traffic load and complex routing rules may cause unexpected reboot.

Web Content Filter

1. [SPR: 210324205, 210324206]
   [Symptom]
   [VPN][L2TP] Remote access VPN_The html picture is broken on warning page (Content Filter/URL threat filter) for http website.
2. [SPR: 211103043]
   [Symptom]
   The picture at URL Threat Filter block page cannot be displayed when using Google Chrome (version 95 or above) or Microsoft Edge (version 95 or above) browser.

Billing

1. [SPR: 211223226, 211223229]
   [Symptom]
   The Bandwidth Management is not working on Billing user type.

Features: V5.39(ABUJ.0)C0

Modifications in V5.39(ABUJ.0)C0 - 2024/08/22

[On Premises mode]

1. [ENHANCEMENT] CLI created to enable "Drop TCP SYN packets with data".
2. [ENHANCEMENT] Optimize URL Threat Filter/Content Filter scan flow to avoid unnecessary inspections.
3. [Bug Fixed] eITS#240401350, 240401693, 240501058, 240701813
   a. Content Filtering is not working because TLS 1.3 Kyber support is introduced in Chrome.
4. [Bug Fixed] eITS#240501893
   a. Device becomes unresponsive after interface is disabled in device HA.
5. [Bug Fixed] eITS#240600228
   a. SSL inspection can't work within latest Chrome version.
6. [Bug Fixed] eITS#240700190
   a. Unable to backup configuration file from SecuManager
7. [Bug Fixed] eITS#240701292
   a. Mitigation for CVE-2024-42057

[On Cloud mode]

N/A

[AP Controller]

1. [Bug Fixed] eITS#240301525
   a. Controller pushed VLAN settings to AP but not updated.
2. [Bug Fixed] eITS#240400026
   a. Unable to load the Station Top N page.
3. [Bug Fixed] eITS#240400683
   a. Controller pushed settings to AP issue.
4. [Bug Fixed] eITS#240500682
   a. Device unresponsive after changing MAC-filter settings.

[Common vulnerabilities and Exposures]

ZLD5.39 Patch0 is no longer vulnerable to the following CVE References:

- CVE-2024-3596
- CVE-2024-6343
- CVE-2024-6387
- CVE-2024-7203
- CVE-2024-42057
- CVE-2024-42058
- CVE-2024-42059
- CVE-2024-42060
- CVE-2024-42061

Features: V5.38(ABUJ.0)C0

Modifications in V5.38(ABUJ.0)C0 - 2024/03/29

[On Premises mode]

1. [ENHANCEMENT] [eITS#230800065, 230801657, 240100888]: ADP allow list support extend to include protocol anomaly.
2. [ENHANCEMENT]: Add last update time on SecuReporter Allow list table.
3. [ENHANCEMENT]: System protection log category change to system.
4. [Feature Change]: Not support certificate signed using weak hashing algorithm (Md5 or SHA1).
5. [Feature Change]: Cannot set the password to "1234" after the first login for "admin" account.
6. [Feature Change]: Adjust USG20(W)-VPN & USG FLEX 50 default SSL VPN active user to 15.
7. [Bug Fix] eITS#230600172
   a. Change wording of outing column in SNAT flow for Remote Access VPN.
8. [Bug Fix] eITS#230900510
   a. Fix: VPN won't rollback to the primary link when the primary link comes up.
9. [Bug Fix] eITS#231000331
   a. Fix: Hotspot clients connectivity Issue.
10. [Bug Fix] eITS#231001935, 240201158
    a. Fix: Certificate synchronization issue in HA Pro scenario.
11. [Bug Fix] eITS#231001977, 231201224
    a. Fix: Shorten the booting up time in certain conditions.
12. [Bug Fix] eITS#231002090, 240201323
    a. Fix: CAPWAP no response and AP disconnect from APC.
13. [Bug Fix] eITS#231002128
    a. Fix: External IP Black list update fail on IPv6 address.
14. [Bug Fix] eITS#231002194
    a. Fix: Device does not response to https/ssh/console access when using FQDN object in BWM.
15. [Bug Fix] eITS#231100767
    a. Fix: ssl inspection doesn't work as expects due to abnormal memory usage.
16. [Bug Fix] eITS#231101460
    a. Fix: Remove "MOVE" icon in ADP policies.
17. [Bug Fix] eITS#231101571
    a. Fix release notes pop-up window resize issue.

18. [Bug Fix] eITS#231200559
    a. Fix: Configuration synchronize issue when device ha role swap.
19. [Bug Fix] eITS#231200687
    a. Enhancement: Cache memory recycling mechanism.
20. [Bug Fix] eITS#231200814
    a. Fix: The tftp traffic can't get files from the tftp server through the VPN tunnel.
21. [Bug Fix] eITS#231201080
    a. Fix: Web Authentication portal can't popup when browsing the page via https.
22. [Bug Fix] eITS#231201250
    a. Fix: SSH accessibility issue to XGS4600 when going through firewall.
23. [Bug Fix] eITS#231201383
    a. Fix: LLDP packets can't be sent out.
24. [Bug Fix] eITS#240100074
    a. Fix: BWM malfunctioning when using vlan interfaces.
25. [Bug Fix] eITS#240100387
    a. Fix: speedtest server select doesn't work.
26. [Bug Fix] eITS#240101503
    a. Enhancement: Add cli command to support "year" information in syslog.
27. [Bug Fix] eITS#240200401
    a. Fix: Add "Responder Only" CLI for IPsec VPN.
    b. crypto map [CRYPTO_NAME] responder-only
    c. crypto map [CRYPTO_NAME] no responder-only
28. [Bug Fix] eITS#240200927
    a. Fix: speedtest sometimes cannot get the result.
29. [Bug Fix] eITS#240200968
    a. Fix: 2FA OTP mail can only be sent to 1 email account.
30. [Bug Fix] eITS#240201103
    a. Fix: rip/ospf can't work on VTI interface.
31. [Bug Fix] eITS#240201114
    a. Fix: Content Filter Profile icon status incorrect.
32. [Bug Fix] eITS#240300167
    a. Fix: Wording adjustment.
33. [Bug Fix] eITS#240300451, 240301211
    a. Fix: Device reboots unexpectedly.

[On Cloud mode]

1. [ENHANCEMENT]: DNS Content Filter support Google/ YouTube/ Microsoft Bing Safe Search.
2. [ENHANCEMENT]: Support change to a different ISP (WAN fallback).
3. [Bug Fix] eITS#231201567
   a. Fix: pppoe connection issue when multiple pppoe instances are configured
4. [Bug Fix] eITS#240201203
   a. Fix: Device becomes unresponsive after losing connection to Nebula server.

[AP Controller]

1. [ENHANCEMENT]: Update AP version to V6.70(.2)
2. [ENHANCEMENT]: The WBE660S is fully supported in this release. Introducing the WBE660S, a NebulaFlex Pro AP powered by cutting-edge WiFi 7 technology that comes with 3 management modes: standalone, controller managed and Nebula cloud managed modes.
3. [ENHANCEMENT]: Added more supported countries for WiFi 6E and WiFi 7 (6Ghz) models.
4. [ENHANCEMENT]: Boost GUI efficiency by optimizing handling of extensive access points and client data influx.
5. [Limitation]
   a. When WBE660S (and forth coming new AP) is managed by USG FLEX/ATP with latest ZLD 5.38 firmware, the Zymesh is no longer supported.

[Common vulnerabilities and Exposures]

ZLD5.38 Patch0 is no longer vulnerable to the following CVE References:

- CVE-2023-48795

Features: V5.37(ABUJ.2)C0

Modifications in V5.37(ABUJ.2)C0 - 2024/01/22

[On Premises mode]

1. [Bug Fix] eITS#231101413, 231101432
   a. Fix: 802.1X wireless station authentication failure.
2. [Bug Fix] eITS#231101439
   a. Fix: Failed to apply configuration file due to certificate.
3. [Bug Fix] eITS#231200479
   a. Fix: Import pkcs12 certificate fail
4. [Bug Fix] eITS#231200577
   a. Fix: some debug information missing in diagnostics collection.
5. [Bug Fix] eITS#231200592
   a. Fix: IDP system protect causes the device reboot unexpectedly.
6. [Bug Fix] eITS#231201567
   a. Fix: WAN PPPoE cannot be established once the device is upgraded to 5.37P1. You need to edit the PPPoE username or password on Nebula and save it again to make PPPoE work.

[On Cloud mode]

1. [Bug Fix] eITS#231200717
   a. Fix: High CPU load on cloud mode.

[AP Controller]

1. [Bug Fix] eITS#231100445
   a. Fix: APC abnormally displays 6GHz wireless client count while there is no 6GHz client connected.

[Common vulnerabilities and Exposures]

ZLD5.37 Patch2 is no longer vulnerable to the following CVE References:

- CVE-2023-6397
- CVE-2023-6398
- CVE-2023-6399
- CVE-2023-6764

Features: V5.37(ABUJ.1)C0

Modifications in V5.37(ABUJ.1)C0 - 2023/11/10

[On Premises mode]

1. [ENHANCEMENT]: IP Reputation to scan device local in/out traffic.
2. [ENHANCEMENT]: Show allow action from SecuReporter including IP Reputation, DNS & URL Threat Filter.
3. [ENHANCEMENT]: New network tools - Speed Test.
4. [Feature Change]: Update OpenSSL package to 3.0.10 and not support TLS1.0/1.1 protocol anymore for these features:
   a. AAA Server
   b. SSL inspection
   c. Web GUI
   d. SecuManager
   e. Certificate
5. [Feature Change]: To ensure the highest level of security, after the first login, it is not possible to set the password to "1234".
6. [Feature Change]: To increase session control “default session limit” to 20,000 and “create new object session limit” to 40,000.
7. [Feature Change]: [eITS#230501617] Fine tune the CEF log format.
8. [Feature Change] User Interface/Description change:
   a. Remove "Cloud Email Security” icon in Email Security page.
9. [Bug Fix] eITS#221001398
   a. Fix: Stability issue when "Failback to Primary Peer Gateway when possible" is enabled.
10. [Bug Fix] eITS#221001970
    a. Fix: Many duplicated dynamic VPN routing entries are on the MAINTENANCE > Packet Flow Explore > Dynamic VPN > Routing Table.
11. [Bug Fix] eITS#230500501
    a. Fix: Web authentication using External Web Portal with 3rd party App doesn't work.
12. [Bug Fix] eITS#230501662
    a. Fix: Device reboots unexpectedly.
13. [Bug Fix] eITS#230600461
    a. Fix: HA failover doesn't work.
14. [Bug Fix] eITS#230601375
    a. Fix: The device lost all SSL Inspection Exclude List after it rebooted.

15. [Bug Fix] eITS#230700228
    a. Fix: Move "Radius Server is enable" log to debug level.
16. [Bug Fix] eITS#230700420
    a. Fix: DHCP server cannot release IP address.
17. [Bug Fix] eITS#230700642
    a. Fix: Go to CONFIGURATION > Mgmt. & Analytics > Nebula but the page keeps loading.
18. [Bug Fix] eITS#230700646
    a. Fix: The device rebooted unexpectedly.
19. [Bug Fix] eITS#230701080
    a. Fix: When the VPN client uses domain user to login in, it can still be established without 2FA authentication even if the authentication is expired.
20. [Bug Fix] eITS#230701237
    a. Fix: The SFP port with DHCP IP sometimes will lost WAN connection unless you manually release DHCP IP from Web-GUI or re-activate the SFP interface.
21. [Bug Fix] eITS#230701499
    a. Fix: iOS device is not redirected to authentication page automatically.
22. [Bug Fix] eITS#230800292
    a. Fix: The CSV file is not fully imported to the static DHCP table. Weird three lines appear at the bottom of the DHCP table and prevent saving any changes.
23. [Bug Fix] eITS#230800764
    a. Fix: Incorrect status on login users page when SSH client closed the session.
24. [Bug Fix] eITS#230801489
    a. Fix: The HTTPS Service control filter to access the administration interface from a particular Public IP does not work.
25. [Bug Fix] eITS#230900423
    a. Fix: Once the based port of the VLAN interface is modified, the device will get stuck and need a reboot to recover.
26. [Bug Fix] eITS#230901380
    a. Fix: The character comma is not supported in the log settings of email password but the i-note says it is supported.
27. [Bug Fix] eITS#231000246
    a. Fix: DHCP lease time is expired but the expired IP address still exists in the DHCP table.

28. [Bug Fix] eITS#231000270
    a. Fix: Configure a security policy rule to block devices with device insight but all devices are still able to access Internet.
29. [Bug Fix] eITS#231000905
    a. Fix: Content Filter does not work correctly in certain condition.

[On Cloud mode]

1. [Feature Change] Remove ZTP from ZLD5.37 Patch1:
    a. For USG FLEX/ATP series, please go to Nebula Control Center deployment method and choose the "Nebula native mode".
2. [Bug Fix] eITS#230601419
    a. Fix: Connectivity Status always shows "Success" even no IP is on wan interface.
3. [Bug Fix] eITS#230801049
    a. Fix: The device is nebula mode but the web GUI shows on-premises style.
4. [Bug Fix] eITS#230801380
    a. Fix: When web authentication is disabled, client is not able to query walled garden list domain via external DNS server.

[AP Controller]

N/A

[Common vulnerabilities and Exposures]

ZLD5.37 Patch1 is no longer vulnerable to the following CVE References:

- CVE-2021-25217
- CVE-2022-44792
- CVE-2022-44793
- CVE-2023-35136
- CVE-2023-35139
- CVE-2023-37925
- CVE-2023-37926
- CVE-2023-4397
- CVE-2023-4398
- CVE-2023-5650

- CVE-2023-5797
- CVE-2023-5960

Features: V5.37(ABUJ.0)C0

Modifications in V5.37(ABUJ.0)C0 - 2023/06/30

[On Premises mode]

1. [ENHANCEMENT] Support management with Nebula Cloud Monitoring Mode
2. [ENHANCEMENT] Enable VPN Service switch in VPN Connection
3. [ENHANCEMENT] DNS Content Filter support Google/ YouTube/ Microsoft Bing Safe Search
4. [ENHANCEMENT] [eITS#230100967] Add test site & feedback link to Content Filter and URL Threat Filter page.
5. [ENHANCEMENT] Support Single sign-on feature included in Network Premium license
6. [Feature Change] Change ATP100 and ATP100W max. VTI / VPN Tunnels number to 50
7. [Feature Change] Remove Facebook Wi-Fi Portal Authentication feature due to Meta had end of the Facebook Wi-Fi service by June 12, 2023
8. [Feature Change] Remove “Continuously capture and overwrite old ones” setting at Packet Capture page
9. [Bug Fix] eITS#230100260
   a. Fix: App Patrol signature failed to update if you use external update server.
10. [Bug Fix] eITS#230100530
    a. Fix: GUI wording remove "Google Authenticator" for Guess user /Ext-user /Ext-group-user because MFA Google Authenticator only support Local User.
11. [Bug Fix] eITS#230100675
    a. Fix: Enable "User" category in E-mail server 2 only but the E-mail server 2 still receives the same email logs as E-mail server 1.
12. [Bug Fix] eITS#230101190
    a. Enhancement: Improve web-auth force auth redirect.
13. [Bug Fix] eITS#230200165
    a. Fix: Reference incorrect for address object.
14. [Bug Fix] eITS#230300454
    a. Fix: Stability issue for hotspot feature.
15. [Bug Fix] eITS#230300761
    a. Fix: The device always uses the first IP of the local subnet to run connectivity check in VPN Phase 2.
16. [Bug Fix] eITS#230301073

a. Fix: It shows "Your device is managed by nebula" in Initial Setup Wizard but the device is not registered on nebula.

17. [Bug Fix] eITS#230301243
    a. Fix: On iOS, only one VPN profile can be installed. Once the new vpn profile is installed, the old one is overwritten.
18. [Bug Fix] eITS#230301453
    a. Fix: The Device Insight page shows only 50 entries initially. The page displays the correct number of hosts after "Show Advanced Settings" is clicked.
19. [Bug Fix] eITS#230301541
    a. Fix: After a pfx certificate is imported to "My Certificates", the existing certificates disappeared.
20. [Bug Fix] eITS#230400133
    a. Fix: Device reboots unexpectedly.
21. [Bug Fix] eITS#230400136
    a. Fix: Anti-Malware Threat Intelligence Machine Learning signature was stuck with the version 2017-12-11.
22. [Bug Fix] eITS#230400523
    a. Fix: Site-to-site VPN can be established when authentication of one site is Pre-Shared Key and the remote site is certificate.
23. [Bug Fix] eITS#230400756
    a. Fix: Visit an unrated web site and you receive UNRATED alert from firewall. After clicking on the button "Continue", you will see "Blocked".
24. [Bug Fix] eITS#230401085
    a. Fix: AAA server ad profile always remains case-sensitive enabled after a reboot.
25. [Bug Fix] eITS#230401149
    a. Fix: PCI compliance failure.
26. [Bug Fix] eITS#230401189
    a. Fix: System name displays incompletely on IPSec Monitor page.
27. [Bug Fix] eITS#230401252
    a. Fix: Wrong status of connectivity check of policy route rule when a routing rule with higher priority is deleted.
28. [Bug Fix] eITS#230401358
    a. Fix: Apply configuration file failed.
29. [Bug Fix] eITS#230401397
    a. Fix: App Patrol log messages show javascript.
30. [Bug Fix] eITS#230401486

a. Fix: On USG20W-VPN, unable to modify SSID settings directly on this page by clicking "Edit".

31. [Bug Fix] eITS#230500682
    a. Fix: HA Pro sync issue.
32. [Bug Fix] eITS#230500913
    a. Fix: Session monitor service display issue when searching for service type.
33. [Bug Fix] eITS#230501004
    a. Fix: Some local users cannot receive 2FA mail.
34. [Bug Fix] eITS#230501063
    a. Fix: SecuManager rpc cannot get the device status.
35. [Bug Fix] eITS#230501341
    a. Fix: Abnormal link change log.
36. [Bug Fix] eITS#230501549
    a. Fix: Fail to apply configuration file when the device boots up.
37. [Bug Fix] eITS#230501570
    a. Fix: IP Reputation and URL Threat Filter signatures cannot be updated when external update server is configured.
38. [Bug Fix] eITS#230600177
    a. Fix: There is no user info in the Traffic Statistics. It shows IP address only without username.
39. [Bug Fix] eITS#230600769
    a. Enhancement: Check local default certificate's integrity.
40. Common vulnerabilities and Exposures:
    ZLD5.37 Patch0 is no longer vulnerable to the following CVE References:
    - CVE-2022-4304
    - CVE-2022-4450
    - CVE-2023-0215
    - CVE-2023-0286
    - CVE-2023-34138
    - CVE-2023-34139

[On Cloud mode]

1. [ENHANCEMENT] VPN policy support DH Group 19, 20, 21
2. [Bug Fix] eITS#221201018
    a. Fix: The client page shows two hosts with the same IP address for two different MAC addresses.

3. [Bug Fix] eITS#230100095
   a. Fix: DNS address records are not resolved to the internal IP address.
4. [Bug Fix] eITS#230301050
   a. Fix: L2TP VPN suddenly stopped working.
5. Common vulnerabilities and Exposures:
   ZLD5.37 Patch0 is no longer vulnerable to the following CVE References:
   - CVE-2023-28767
   - CVE-2023-33011
   - CVE-2023-33012

[AP Controller]

1. [ENHANCEMENT] Update AP version to V6.55(.1)
2. [ENHANCEMENT] Korea country code can support 6GHz for WAX620D-6E and WAX640S-6E
3. [ENHANCEMENT] DCS now enhancement
4. [ENHANCEMENT] APC now supports WAX300H new Access point
5. [ENHANCEMENT] APC now supports WAX655 wireless-bridge feature
6. [Feature Change] GUI warning message enhanced for Secure WiFi license expired
7. Common vulnerabilities and Exposures:
   ZLD5.37 Patch0 is no longer vulnerable to the following CVE References:
   - CVE-2023-34140
   - CVE-2023-34141

Features: V5.36(ABUJ.2)C0

Modifications in V5.36(ABUJ.2)C0 - 2023/05/24

[On Premises mode/On Cloud mode]

1. Common vulnerabilities and Exposures:

   ZLD5.36 Patch2 is no longer vulnerable to the following CVE References:

   - CVE-2023-33009
   - CVE-2023-33010

Features: V5.36(ABUJ.1)C0

Modifications in V5.36(ABUJ.1)C0 - 2023/05/09

[On Premises mode]

1. [Bug Fix] eITS#230401495
   Fix: If IKEv2 VPN with 2FA authentication is configured, it may cause device cease to function.
   a. Fix: IKEv2 initiator cause memory leak
2. [Bug Fix] eITS#230401438
   a. The device does not send 2FA by email for VPN connections when Two-factor Authentication > VPN Access > User/Group > Selected User/Group contains user object.

[On Cloud mode]

1. [Bug Fix] eITS# 230401284
   a. Fix: PPPoE failed to dial up if PPPoE account contains the character %.

Features: V5.36(ABUJ.0)C0

Modifications in V5.36(ABUJ.0)C0 - 2023/03/31

[On Premises mode]

1. [Feature Change] User Interface/Description change:
   a. GUI remove "Note 1 register and get firmware notification" for firmware management page
   b. GUI add "Note 2 try cloud-based Anti-Spam Cloud Email Security information" for service page
2. [Feature Change] Build-in WiFi APC initial wizard default radio profile change to 11ax
3. [Bug Fix] eITS#221000888
   a. Fix: The device stops sending SMS via a SMS gateway after several days and also becomes unresponsive.
4. [Bug Fix] eITS#221201004
   a. Fix: 2FA authorization mail receiver and mail content name are not identical.
5. [Bug Fix] eITS#221201009
   a. Fix: SNMP get incorrect value after the interface is disconnected.
6. [Bug Fix] eITS#221201374
   a. Fix: Customer can access port 8008 page even if 2FA for VPN access is not enabled.
7. [Bug Fix] eITS#230100962
   a. Fix: Lots of message “An IP address conflict is detected at MAC 00:00:00:00:00:00” appear in the log.
8. [Bug Fix] eITS#230101199
   a. Fix: The graph on dashboard and port statistics are not identical when the language is Russian.
9. [Bug Fix] eITS#230101534, 230101202
   a. Fix: Unable to open default-group in Configuration > Wireless > AP Management > AP Group.
10. [Bug Fix] eITS#230200237
    a. Fix: Nebula register QR code should be hidden when user uses limited-admin.
11. [Bug Fix] eITS#230201027
    a. Fix: Unable to see Remote AP VPN status in General > VPN Status on dashboard.

12. [Bug Fix] eITS#230201090
    a. Fix: Unable to replace any interface IP and subnet with 192.168.5.1/24 on USG FLEX 50.
13. [Bug Fix] eITS#230201128
    a. Fix: License sync failed in device HA Pro configuration sync process.
14. [Bug Fix] eITS#230201388
    a. Fix: The 'Enable Two-factor Authentication' checkbox in VPN gateway gets disabled upon every reboot.
15. [Bug Fix] eITS#230300352
    a. Fix: Password is transmitted in clear text in the trace log when HA is syncing.
16. [Bug Fix] eITS#230300393
    a. Fix: Unable to open the authentication page https://lan IP:8008/2FA-access.cgi when using 2FA with Google Authenticator.
17. [Bug Fix] eITS#230300453
    a. Fix: If a backup configuration file is encrypted using special characters such as '%' or '+', the ZIP archive cannot be opened.
18. [Bug Fix] eITS#230300467
    a. Fix: Getting error when trying to edit static DHCP table.
19. [Bug Fix] eITS#230300678
    a. Fix: Abnormal amount of DHCP IP table.
20. [Bug Fix] eITS#230300846
    b. Fix: Email security page displays red notification about license expired, but the email security service is already activated by bundle license.
21. Common vulnerabilities and Exposures:
    ZLD5.36 is no longer vulnerable to the following CVE References:
    - CVE-2023-22913
    - CVE-2023-22914
    - CVE-2023-22915
    - CVE-2023-22916
    - CVE-2023-22917
    - CVE-2023-22918
    - CVE-2023-27990
    - CVE-2023-27991
    - CVE-2023-28771

[On Cloud mode]

1. [Bug Fix] eITS#230300025
   a. Fix: SecuReporter stops working when the syslog server is set in NCC.
2. [Bug Fix] eITS#230300035
   a. Fix: VPN disconnects unexpectedly. (sdwan_interface issue)

Features: V5.35(ABUJ.0)C0

Modifications in V5.35(ABUJ.0)C0 - 2023/01/03

[On Premises mode]

1. [ENHANCEMENT] Configuration files download with password protection
2. [ENHANCEMENT] Custom DDNS support auto update when public IP changed
3. [ENHANCEMENT] Automatically update DDNS IP address at DDNS monitor page
4. [ENHANCEMENT] System Log support DHCP IP conflict detection
5. [ENHANCEMENT] Support traffic log rotate on USB storage
6. [ENHANCEMENT] Support Sensitive Data Protection to protect management password
7. [Feature Change] [eITS#220600529] Response Message remove customization page layout change to default block page design.
8. [Feature Change] The default radio profile under AP controller in Wireless setup wizard change from 11ac to 11ax
9. [Feature Change] Modify the wording at 5G Radio page:
   a. Change the wording "Enable 5 GHz DFS Aware" to "Avoid 5 GHz DFS Channel"
10. [Bug Fix] eITS#221000888 / 221200149
    a. Fix: The device stops sending SMS via a SMS gateway after several days and also becomes unresponsive.
11. [Bug Fix] eITS#221001336
    a. Fix: In the policy route rule, select interface/gateway as the next hop and enable connectivity check. After you change the next hop from interface/gateway to trunk, connectivity check becomes greyed out but the previous connectivity check settings are still applied to the policy route rule.
12. [Bug Fix] eITS#221100576
    a. Fix: USG FLEX 50 virtual device in the dashboard is incorrect
13. [Bug Fix] eITS# 221100935
    a. Fix: Support fast recovery
14. [Bug Fix] eITS# 221101130
    a. Fix: the boot up console warning message and SYS red light issue.
15. [Bug Fix] eITS# 221101139
    a. Fix: Security policy is not working when 2FA is enabled
16. [Bug Fix] eITS#221101280

a. Fix: NAT port forwarding data transfer rate is unstable

17. [Bug Fix] eITS#221101428
    a. Fix: Since the device is upgraded to firmware to V5.32, the warning message "Unverified Firmware Installed" pops up in the dashboard.
18. [Bug Fix] eITS#221101628 / 220301602
    a. Fix: USG FLEX unexpected reboot
19. [Bug Fix] eITS#221201009
    a. Fix: SNMP get incorrect value after the interface is disconnected.
20. Common vulnerabilities and Exposures:
    ZLD5.35 is no longer vulnerable to the following CVE References:
    - CVE-2022-38547
    - CVE-2022-40603

[On Cloud mode]

1. [ENHANCEMENT] Support captive portal logout via 6.6.6.6
2. [ENHANCEMENT] SecuReporter traffic log support client MAC address
3. [ENHANCEMENT] Event Log support DHCP IP conflict detection
4. [Bug Fix] eITS#221000144
    a. Fix: CPU and memory usage don't display in Monitor > Firewall > Status. Event log is also empty.
5. [Bug Fix] eITS#221000422
    a. Fix: WiFi clients have no internet access due to IPS customized signatures that are created in the previous on-premises mode.
6. [Bug Fix] eITS#221100122
    a. Fix: USG FLEX becomes offline on Nebula when the number of Firewall clients exceed 2048.
7. [Bug Fix] eITS#221200797
    a. Fix: In the Monitor > Clients > Firewall page only the clients connected to lan1 will be displayed and the clients connected to other ports such as SFP port will not be displayed.

[AP Controller]

1. [ENHANCEMENT] Update AP images V6.45(.0)
2. [ENHANCEMENT] DCS Client Aware default setting changed to disable.
3. [ENHANCEMENT] DFS channel behavior enhance for better UX.

4. [ENHANCEMENT] APC changed multicast to unicast default setting.
5. [ENHANCEMENT] Refine default AMPDU size.
6. [ENHANCEMENT] Support WiFi6E settings on APC.
7. [ENHANCEMENT] Support WAX655E Ethernet setting.
8. [ENHANCEMENT] Hostname supported in wireless station info.
9. [ENHANCEMENT] CAPWAP online/offline does not kick STA.
10. [ENHANCEMENT] Top-N supports 6GHz radio information.
11. [ENHANCEMENT] ZLD 5.3x APC fully support WiFi6E AP.
12. [ENHANCEMENT] ZyMesh support WiFi 6E (6GHz).

Features: V5.32(ABUJ.1)C0

Modifications in V5.32(ABUJ.1)C0 - 2022/11/10

[On Premises mode]

1. [Bug Fix] eITS#220900459 / 220901667: Fix:Potential device HA synchronization issue

Features: V5.32(ABUJ.0)C0

Modifications in V5.32(ABUJ.0)C0 - 2022/10/04

[On Premises mode]

1. [ENHANCEMENT] USG FLEX support DNS Threat Filter, IP Reputation and Sandboxing with Gold Security Pack
2. [ENHANCEMENT] Support System Protection and signature update
3. [ENHANCEMENT] ZLD firmware integrity
4. [ENHANCEMENT] [eITS#200700296, 220700648] When DNS TTL of FQDN object for destination IP timeout, the video stream will lag
5. [ENHANCEMENT] [eITS#220701026] 2FA window should pop up before password change window pops up
6. [ENHANCEMENT] User Interface/Description change:
   a. Refine SecuReporter Premium to standard license for consistency
   b. Adjust SecuReporter banner in device GUI more user friendly
   c. Update Note information in the bottom at Configuration service page
7. [Feature Change] Change CDR Malware detected default occurrence value from 2 to 5
8. [Bug Fix] eITS#220101543
   a. Fix: IKEv2 with pre-shared key on Samsung mobile phone (Android 12) cannot be connected.
9. [Bug Fix] eITS#220600781
   a. Fix: NAT forward to DMZ not working
10. [Bug Fix] eITS#220601116
    a. Fix: Multiple DH issue in IKEv2 connection
11. [Bug Fix] eITS#200601255 / 220700030
    a. Fix: After Device HA failover, clients in vlan subnet have no interface access
12. [Bug Fix] eITS#220700735
    a. Fix: Configuration in HTTPS Admin Service Control is not working.
13. [Bug Fix] eITS#220700760
    a. Fix: Specific object name causes device to roll back to lastgood configuration file.
14. [Bug Fix] eITS#220700981
    a. Fix: Second wan connection issue with wan trunk.
15. [Bug Fix] eITS#220700986
    a. Fix: Renaming object name causes object name display issue on web GUI

16. [Bug Fix] eITS#220701020
    a. Fix: SSL VPN client for macOS is not connected if HTTPS port and SSL VPN server port are not identical.
17. [Bug Fix] eITS#220701048
    a. Fix: Duplicate host name display issue on DHCP table
18. [Bug Fix] eITS#220701078
    a. Fix: URL threat filter signature is not updated to the latest version.
19. [Bug Fix] eITS#220701082
    a. Fix: 2FA authentication via mail is not working on AD users.
20. [Bug Fix] eITS#220800169
    a. Fix: DNS threat filter category query issue
21. [Bug Fix] eITS#220800428
    a. Fix: Schedule Backup doesn't work with complex password
22. [Bug Fix] eITS#220800881
    a. Fix: SSL VPN is not connected with LDAP authentication
23. [Bug Fix] eITS#220800994
    a. Fix: Device doesn't follow the schedule in Auto Update to update signature version.
24. [Bug Fix] eITS#220801346
    a. Fix: Unable to see Firewall's event log and topology on nebula
25. [Bug Fix] eITS#220900270
    a. Fix: When invalid NAT rule is configured (port mapping type: ports, start port 1 and end port 65535), the browser pops up weird message.
26. [Bug Fix] eITS#220900336
    a. Fix: The command "debug system show conntrack" is not allowed.
27. [Vulnerability Fix] Zyxel-SI-1430
    Fix XSS (Cross Site Scripting) vulnerability

[On Cloud mode]

1. [ENHANCEMENT] USG FLEX support DNS Threat Filter, IP Reputation and Sandboxing with Gold Security Pack
2. [ENHANCEMENT] In Hub and spoke VPN topology, the Hub VPN gateway will be a responder role during IKE negotiation
3. [ENHANCEMENT] Support DDNS peer address for non-Nebula Site2site VPN
4. [ENHANCEMENT] Live tool ping check support "Auto" interface
5. [ENHANCEMENT] Support TIML signature update

6. [ENHANCEMENT] Support System Protection and signature update
7. [Bug Fix] eITS#220700128
   b. Fix: The static route on nebula firewall to the peer site Microsoft Azure is not working anymore once the peer site Microsoft Azure VPN disconnects.

[AP Controller]

1. [ENHANCEMENT] Update AP images V6.40(.6)

Features: V5.31(ABUJ.0)C0

Modifications in V5.31(ABUJ.0)C0 - 2022/07/05

[On Premises mode]

1. [ENHANCEMENT] In the initial setup stage to detect LAN subnet if conflict with 192.168.1.1 then auto change to 192.168.10.1 redirect to myrouter.local
2. [ENHANCEMENT] Login Users table add Created Date column as same as User Object
3. [ENHANCEMENT] Device GUI add Astra cloud portal URL
4. [ENHANCEMENT] [eITS#211100981] Email Security Blocklist add i-note information
5. [ENHANCEMENT] [eITS#220101060, 220101420, 220200439] Enhanced the information in the CDR logs
6. [ENHANCEMENT] [eITS#220500069] Monitor > Log > View Log > "Email Log Now" error message is not clear to us
7. [Feature Change] USG FLEX100 and USG FLEX 100W max. VPN tunnels number upgrade to 50
8. [Feature Change] SSO feature enter maintenance mode and end of software service.
9. [Bug Fix] eITS#211200767
   a. Fix: Incorrect SSL VPN dashboard statistics information
10. [Bug Fix] eITS#220100656
    a. USG FLEX 200 / DNS Content filter functional Issue
11. [Bug Fix] eITS#220101259
    a. Fix: IP malfunctioning when the VLAN wan interface is configured with specific subnet mask
12. [Bug Fix] eITS#220200044
    a. Fix: Error message when visiting Sandboxing page.
13. [Bug Fix] eITS#220300054
    a. Fix: Virtual Server LB disconnected issue
14. [Bug Fix] eITS#220400122
    a. Fix: Address Object manipulation issue
15. [Bug Fix] eITS#220400688
    a. Fix: Malfunctioning on IPSec Connectivity check button
16. [Bug Fix] eITS#220400957
    a. Fix: Incorrect wireless monitoring data
17. [Bug Fix] eITS#220401137

a. Fix: DNSBL malfunctioning issue

18. [Bug Fix] eITS#220401321
    a. Fix: Wildcard FQDN object issue which may affect the system stability
19. [Bug Fix] eITS#220500188
    a. Fix: Packet forwarding issue on Trunk interface
20. [Bug Fix] eITS#220500690
    a. Fix: SSLVPN service port keeps using the original port after manually customized it
21. [Bug Fix] eITS#220500701
    a. Fix: GUI information correction
22. [Bug Fix] eITS#220500751
    a. Fix: SSLVPN connectivity issue
23. [Bug Fix] eITS#220500939
    a. Fix: DHCP service stability issue
24. [Bug Fix] eITS#220501025
    a. Fix: AAA radius COA will be turned on after firmware update to V5.30
25. [Bug Fix] eITS#220501052
    a. Fix: VPN connectivity issue between Nebula and Non-Nebula VPN gateways
26. [Bug Fix] eITS#220501182
    a. Fix: VPN wizard malfunctioning issue
27. [Bug Fix] eITS#220501267
    a. Fix: Incorrect dashboard Virtual device Rear Panel wlan led status
28. [Bug Fix] eITS#220501309
    a. Fix: Static DHCP table importing issue
29. [Bug Fix] eITS#220600336
    a. Fix: Device stability enhancement
30. [Bug Fix] eITS#220600447
    a. Fix: What's new notification in the GUI malfunctioning.
31. [Bug Fix] eITS#220600465
    a. Fix: DHCP service stability issue
32. Common vulnerabilities and Exposures:
    a. Local privilege escalation vulnerability fix (CVE-2022-30526)
    b. Authenticated directory traversal vulnerability fix (CVE-2022-2030)
    c. Security update of OpenSSL package (CVE-2022-0778)

[On Cloud mode]

1. [ENHANCEMENT] In the initial setup stage to detect LAN subnet if conflict with 192.168.1.1 then auto change to 192.168.10.1 redirect to myrouter.local
2. [ENHANCEMENT] Support access SNMP service from WAN interface
3. [Bug Fix] eITS#220200349
   a. Fix: Microsoft AD authentication not work
4. [Bug Fix] eITS#220301020
   a. Fix: BWM functional issue on USG FLEX 50(W) when the device is managed by NCC
5. [Bug Fix] eITS#220500277
   a. Fix: Google Authentication Bypass
6. [Bug Fix] eITS#220600408
   a. Fix: Nebula bwm cannot work on ftp active mode.

[AP Controller]

1. [ENHANCEMENT] Update AP images V6.30(.4)
2. [ENHANCEMENT] AP can connect to passive APC immediately

Features: V5.30(ABUJ.0)C0

Modifications in V5.30(ABUJ.0)C0 - 2022/04/20

[On Premises mode]

1. [ENHANCEMENT] Support DNS Threat Filter DoH and DoT blocking for ATP series.
2. [ENHANCEMENT] eITS#211101424
   Extends the maximum blocking periods of rate based IPS signatures.
3. [ENHANCEMENT] Remote Access VPN Wizard for SecuExtender IPsec VPN supports Multiple DH Group.
4. [ENHANCEMENT] Support Multi-Language update mechanism
5. [ENHANCEMENT] User Interface/Description enhancements:
   a. Fine tune reboot message at firmware upgrade page
   b. Add License transfer notification for Device HA scenario
   c. eITS#220101135: Fine tune Remote Access VPN Wizard descriptions
6. [ENHANCEMENT] eITS#211100100
   Prevent misconfiguration when enable mode configure in L2TP VPN rules.
7. [Bug Fix] eITS#211000711
   a. Fix: Abnormal memory usage issue
8. [Bug Fix] eITS#211101507
   a. Fix: Log information adjustment
9. [Bug Fix] eITS#211200301
   a. Fix: WeChat file transfer may be affected by Content Filter
10. [Bug Fix] eITS#211200520
    a. Fix: LAN interface subnet mask settings cannot be modified
11. [Bug Fix] eITS#211200767
    a. Fix: VPN dashboard statistics displaying issue
12. [Bug Fix] eITS#211201047
    a. Abnormal memory usage leads to firewall stability issue
13. [Bug Fix] eITS#211227250
    a. Fix: Throughput enhancement when URL Threat filter is enabled
14. [Bug Fix] eITS#220100445
    a. Fix: Logs to USB storage malfunctioning after device rebooting
15. [Bug Fix] eITS#220100448
    a. Fix: Device stability issue due to Wildcard FQDN group implementation
16. [Bug Fix] eITS#220100565
    a. Fix: Stability issue caused by device insight operations
17. [Bug Fix] eITS#220100644

a. Fix: Abnormal CPU usage

18. [Bug Fix] eITS#220101039
    a. Fix: Wording modification
19. [Bug Fix] eITS#220101098
    a. Fix: USG20(W)-VPN/USG FLEX 50(W) configuration backward compatibility issue
20. [Bug Fix] eITS#220200348
    a. Fix: 2FA mechanism
21. [Bug Fix] eITS#220200412
    a. Fix: Russian GUI issue
22. [Bug Fix] eITS#220200468
    a. Fix: In GUI displaying issue on VPN monitoring page
23. [Bug Fix] eITS#220200487
    a. Fix: When the admin limit was set to "1", the password can't be changed when it was expired
24. [Bug Fix] eITS#220200501
    a. Fix: Log category adjustment
25. [Bug Fix] eITS#220200553
    a. Fix: Can not ping via LAG IPv6 interface
26. [Bug Fix] eITS#220201162
    a. Fix: Wifi client layer 2 packets forwarding issue when deploying LAG+VLAN interface with managed AP running on tunnel mode
27. [Bug Fix] eITS#220301001
    a. Fix: Cloud Firmware update issue in device HA scenario
28. [Bug Fix] eITS#220301252
    a. Event log wording correction
29. [Bug Fix] eITS#220400118
    a. Fix: Device HA Pro synchronization issue with specific setting conditions.
30. [Bug Fix] eITS#220400247
    a. Incomplete 2FA SMS message issue
31. [Bug Fix] eITS#220201115
    a. Fix: Windows IKEv2 VPN connection issue.
32. [Bug Fix] eITS#211100603
    a. Fix: CNC reboot command can't trigger the device rebooting.
33. Common vulnerabilities and Exposures:
    ZLD5.21 is no longer vulnerable to the following CVE References:
    - CVE-2022-0342

[On Cloud mode]

1. [Bug Fix] eITS#211101707
   a. Fix: turn of unnecessary NCC query when the device is running in "on-premises" mode
2. [Bug Fix] eITS#220100087
   a. Fix: The diaginfo file cannot be opened from nebula debug local gui
3. [Bug Fix] eITS#220100357
   a. Fix: Incorrect WAN setting detection mechanism
4. [Bug Fix] eITS#220100368
   a. Fix: Device overload when users log into debug local gui.
5. [Bug Fix] eITS#220100519
   a. Fix: Captive Portal may overloading and delay when multiple users trying to login concurrently
6. [Bug Fix] eITS#220100817
   a. Fix: Some VPN tunnels may not be established automatically in large Hub-and-Spoke scale topology
7. [Bug Fix] eITS#220101549
   a. Fix: Traffic can't passthrough the established VPN tunnel occasionally due to applied incomplete VTI settings
8. [Bug Fix] eITS#220300971
   a. Fix: 1:1 NAT functional issue

[AP Controller]

N/A

Features: V5.21(ABUJ.1)C0

Modifications in V5.21(ABUJ.1)C0 - 2022/03/15

[On Premises mode]

1. [Bug Fix]
   a. Fix: A parsing error in Application signature v1.0.0.20220310.0 that may drive an error condition led to connective disruption.

[On Cloud mode]

1. [Bug Fix] eITS#220100368
   a. Fix CPU abnormal loading issue
2. [Bug Fix]
   a. Fix: A parsing error in Application signature v1.0.0.20220310.0 that may drive an error condition led to connective disruption.

[AP Controller]

N/A

Features: V5.21(ABUJ.0)C0

Modifications in V5.21(ABUJ.0)C0 - 2022/02/27

[On Premises mode]

1. [Vulnerability Fix]
   Fix an authentication bypass vulnerability in the CGI program
2. [Vulnerability Fix]
   Fix XSS (Cross Site Scripting) vulnerability

[On Cloud mode]

N/A

[AP Controller]

N/A

Features: V5.20(ABUJ.0)C0

Modifications in V5.20(ABUJ.0)C0 - 2022/01/05

[On Premises mode]

1. [ENHANCEMENT] Support CDR counter reset option.
2. [ENHANCEMENT] Application Objects in BWM add BitTorrent category.
3. [ENHANCEMENT] Support DNS over HTTPS in the Application Patrol.
4. [ENHANCEMENT] eITS#201201325
   a. Adjust the Content Filter Log Level of Blocked/Warned web sites.
5. [ENHANCEMENT] SSL-Inspection Exclude List add Advance function, support Web Categories option. Let user choose which categories can bypass the scan.
6. [ENHANCEMENT] Device Insight enhancement:
   a. Allows user remove selected device client in the table.
   b. Check and display SecuExtender IPSec VPN Client online status.
   c. Change "Download" button to "Feedback" and support online feedback the client device information.
7. [ENHANCEMENT] eITS#210101201
   a. IKEv2 and Active Directory Users setting update.
8. [ENHANCEMENT] eITS#180900304, 180801037
   a. Support VPN multiple Diffie Hellman groups.
9. [ENHANCEMENT] Support 2FA VPN access using Google Authenticator.
10. [ENHANCEMENT] Remote Access VPN Wizard of Zyxel SecuExtender VPN Client (IPSec VPN) supports configure provisioning of:
    a. Native iOS / MacOS IKEv2 client.
    b. Windows IKEv2 client.
    c. Android IKEv2 client. (StrongSwan)
11. [ENHANCEMENT] Support One-click change to Nebula Mode
    a. Configuration menu tree: Change "Cloud CNM" to "Mgmt. & Analytics"
    b. Add "Nebula" User Interface
12. [ENHANCEMENT] SNMP MIB support:
    a. Shutdown device and turn off SYS LED. (eITS#210200993)
    b. License Service remaining days read by SNMP. (eITS#190200257)
13. [ENHANCEMENT] USG20(W)-VPN rename to USG FLEX 50(W).
14. [Bug Fix] eITS#210701694
    a. Fix: Anti-Malware functional issue when scanning specific file format.
15. [Bug Fix] eITS#200900300

a. Fix: System stability issue
16. [Bug Fix] eITS#201101282
    a. Fix: BWM rules malfunction after device rebooting
17. [Bug Fix] eITS#201211231
    a. Fix: System stability issue
18. [Bug Fix] eITS#210700119
    a. Fix: IPv6 routing issue
19. [Bug Fix] eITS#210800257
    a. Fix: L2TP VPN connecting issue
20. [Bug Fix] eITS#210800467
    a. Fix: BWM functional issue
21. [Bug Fix] eITS#210900158
    a. Fix: Device HA synchronization issue in specific condition
22. [Bug Fix] eITS#210900208
    a. Fix: VPN may have connection issue after WAN trunk failover
23. [Bug Fix] eITS#210900589
    a. Fix: Routing trace functional issue
24. [Bug Fix] eITS#210800467
    a. Fix: BWM functional issue
25. [Bug Fix] eITS#210900805
    a. Fix: The ReadMe.txt included in the certificate package should be ignored when calculating the certificate.
26. [Bug Fix] eITS#210901135
    a. Fix: VApp Patrol display error message
27. [Bug Fix] eITS#210901142
    a. Fix: Config backup sends mail every day, but no configuration change
28. [Bug Fix] eITS#210901150
    a. Fix: SecuReporter connecting issue
29. [Bug Fix] eITS#210901248
    a. Fix: WAN interface will not restart process after receiving DHCP-NAK.
30. [Bug Fix] eITS#210901260
    a. Fix: Secure wifi feature may affect LAN users' network access
31. [Bug Fix] eITS#211000225
    a. Fix: Resetted device GUI won't go through the initial witzard when the it is located in specific regions
32. [Bug Fix] eITS#211000428
    a. Fix: ADP blocked specific traffic incorrectly

33. [Bug Fix] eITS#211000613
    a. Fix: Enhancement: Improved the security mechanism in token handling
34. [Bug Fix] eITS#211000656
    a. Fix: DDNS functional issue when multiple WAN are configured in specific way
35. [Bug Fix] eITS#211000763
    a. Fix: Device stability issue when IPS is enabled
36. [Bug Fix] eITS#211000798
    a. Fix: IDP static GUI displaying issue
37. [Bug Fix] eITS#211001019
    a. Fix: SSL VPN authentication issue when using numbers as username
38. [Bug Fix] eITS#211001461
    a. Fix: Reset button may malfunction occasionally
39. [Bug Fix] eITS#211100195
    a. Fix: Enhance: IP Reputation detection mechanism enhancement
40. [Bug Fix] eITS#211100198
    a. Fix: Device Insight table displaying issue
41. [Bug Fix] eITS#211000455 / 211000666
    a. Fix: When there's an account named "support", the config will rollback to default after upgrading the firmware to 5.10
42. [Bug Fix] eITS#211101344
    a. Fix: Improvement: CPU optimization
43. [Bug Fix] eITS#211100613
    a. Fix: L2TP VPN authentication issue
44. [Bug Fix] eITS#211100799
    a. Fix: App Patrol application name sorting issue
45. [Bug Fix] eITS#211000701
    a. Fix: MAC filter profile operation issue
46. [Bug Fix] eITS#211100512
    a. Fix: Device Insight incorrect license information issue
47. [Bug Fix] eITS#211100870
    a. Fix: Billing quota traffic displaying issue
48. [Bug Fix] eITS#211000455
    a. Fix: Configuration file applying issue when upgrading the firmware
49. [Bug Fix] eITS#211101148
    a. Fix: "IP/MAC Binding"
50. [Bug Fix] eITS#211100916

   a. Fix: L2TP VPN authentication issue
51. [Bug Fix] eITS#211101070
   a. Fix: Static DHCP table import issue

[On Cloud mode]

1. [ENHANCEMENT] Support MSChapv2 authentication for external Active Director Server.
2. [ENHANCEMENT] Nebula Portal and local GUI support to configure PPPoE Authentication Type, static IP, and MTU settings.
3. [ENHANCEMENT] Support Campus AP.
4. [ENHANCEMENT] Support "User group" in the Security Policy.
5. [ENHANCEMENT] Support sending traffic log to SecuReporter with Nebula Pro Pack License.
6. [ENHANCEMENT] Local GUI support QR code to register device to Nebula by Nebula Mobile app.
7. [ENHANCEMENT] Local GUI Device Information page enhance.
8. [ENHANCEMENT] Nebula Ticket#211000318
   a. Add the signature etag to detect signature version.
9. [Feature Change] Remove periodically system information log.
10. [Feature Change] Disable "Redirect HTTP to HTTPs" by default.
11. [Bug Fix] eITS#210900194
   a. Fix: A record malfunction when device running on cloud mode
12. [Bug Fix] eITS#211000191
   a. Fix: L2TP VPN connecting issue
13. [Bug Fix] eITS#211100218
   a. Fix: Device stability issue
14. [Bug Fix] eITS#211100628
   a. Fix: PPPoE connection issue when username has special character
15. [Bug Fix] eITS#211100502
   a. Fix: Captive Portal authentication issue

[AP Controller]

1. [ENHANCEMENT] Change the Button Confirmation Design for Renew Firmware.
2. [ENHANCEMENT] Airtime fairness on ax AP.
3. [ENHANCEMENT] Wireless health enhancement.

4. [ENHANCEMENT] Hash password in configuration.

Features: V5.10(ABUJ.0)C0

Modifications in V5.10(ABUJ.0)C0 - 2021/09/22

[On Premises mode]

1. [ENHANCEMENT] Support BWM setting in Remote Access IPsec VPN Configuration Provisioning with SecuExtender IPSec VPN Client.
2. [ENHANCEMENT] Remote Access VPN Wizard add bandwidth limit configuration.
3. [ENHANCEMENT] Support 2FA on IPsec per IKE rule.
4. [ENHANCEMENT] Remote Access VPN Log add user login/logout information.
5. [ENHANCEMENT] Add "user info" at IPsec Monitoring page.
6. [ENHANCEMENT] Add one more check address for VPN connectivity check.
7. [ENHANCEMENT] Initial Setup Wizard support Nebula mode choice.
8. [ENHANCEMENT] Device Insight support.
   a. Role-based Access Policy by user/device contextual.
   b. Device Insight monitoring.
9. [ENHANCEMENT] IPS packet logging.
10. [ENHANCEMENT] IPS enhancement for Brute-force attack.
11. [ENHANCEMENT] External Block List support URL full path.
12. [ENHANCEMENT] Black/White list rename to Block/Allow list.
13. [ENHANCEMENT] Add security policy name in Content Filter and Application patrol log.
14. [ENHANCEMENT] CDR allow the remote access to Quarantine VLAN.
15. [ENHANCEMENT] Content Filter command line support TTL configuration.
16. [ENHANCEMENT] Support CLI to disable weak cipher for SSH/HTTP service.
17. [ENHANCEMENT] Support advance option to prevent SNMP 'GETBULK' Reflection DDoS.
18. [ENHANCEMENT] eITS#210600320, 210701277
    a. FTP upgrade to TLSv1.2.
    b. Add option for Strict-Transport-Security http header.
    c. Add option for X-XSS-Protection http header.
19. [ENHANCEMENT] eITS#210100688 Strength password in web form mechanism.
20. [ENHANCEMENT] New DHCP table import and export.
21. [ENHANCEMENT] SSH support RADIUS with admin privilege login.
22. [ENHANCEMENT] SNMP management enhancement
    a. eITS#180400953, 191000280
       [Product Line: ATP200 above / VPN100 above / FLEX 200 above] SNMP

support CPU temperature (MIB file).

b. eITS#191000637

CPU average core usage and loading.

23. [ENHANCEMENT] Traffic log add NAT translated IP & Port information
24. [ENHANCEMENT] Web UI enhancement/ changes:
    a. Login page support multi-language selection.
    b. IDP rename to IPS.
    c. Warning Message when disable Device HA Pro.
    d. Add Cloud Email Security (CES) entry link at Email Security page.
    e. Captive portal mobile view add renew lease time button (eITS#210600516)
25. [ENHANCEMENT] eITS#210200687, 140101485
    a. Support special characters (+ symbol) in the E-mail field.
26. [Bug Fix] eITS#201000214
    a. Fix: IPv6 gateway may miss incidently.
27. [Bug Fix] eITS#201200826
    a. Fix: Configuration applying failed occasionally.
28. [Bug Fix] eITS# 210200627
    a. Fix: MSTP packet will be blocked incorrectly.
29. [Bug Fix] eITS# 210200863
    a. Enhance: HA Pro fail-over mechanism enhancement.
30. [Bug Fix] eITS# 210300954
    a. Enhance: Support "=" special character in the Anti-Spam tag header.
31. [Bug Fix] eITS# 210301092
    a. Fix: L2TP may not be able to connect in rarely case.
32. [Bug Fix] eITS#210301178
    a. Fix: When the Connectivity Check remote host was down, the Connectivity Check will keep probing on it and consumes the limited session.
33. [Bug Fix] eITS#210301272
    a. Fix: Can not add new interface into the bridge interface when there is a virtual interface in it.
34. [Bug Fix] eITS#210301305
    a. Fix: Wording correction.
35. [Bug Fix] eITS#210301528
    a. Fix: Facebook Wifi malfunctioning.
36. [Bug Fix] eITS#210301549

a. Fix: Session Monitor some field cannot sorting.

37. [Bug Fix] eITS#210400219
    a. Fix: Can not change from EZ mode to Expert mode when some attributes are included in the external RADIUS server.
38. [Bug Fix] eITS#210400228
    a. Fix: When adding the VLAN setting on LAG port, user needs to reboot the Devices to let this setting take effect
39. [Bug Fix] eITS#210400817
    a. Fix: Wrong file extension name on the exported certificate.
40. [Bug Fix] eITS#210400868
    a. Fix: Stability enhancement.
41. [Bug Fix] eITS#210401330
    a. Fix: IKE issue when using 3rd party authorized certificate.
42. [Bug Fix] eITS#210501373
    a. Fix: NAT mapping issue.
43. [Bug Fix] eITS#210600462
    a. Fix: Routing issue when interface goes down and recovered.
44. [Bug Fix] eITS# 210601917
    a. Fix: Windows built-in IKEv2 VPN connection issue.
45. [Bug Fix] eITS# 210700565
    a. Fix:2FA page did not change to the user assigned certificate.
46. [Bug Fix] eITS#210700587
    a. Change: Removed web ssl application to reduce the external surfing risk.
47. [Bug Fix] eITS#210700589
    a. Fix: HTTPS /SSLVPN service port changing issue.
48. [Bug Fix] eITS#210700708
    a. Fix: GUI display issue.
49. [Bug Fix] eITS#210700957
    a. Fix: SSH service malfunctioning.
50. [Bug Fix] eITS#210701634
    a. Fix: The direct traffic will be affected by policy route.
51. [Bug Fix] eITS#210701916
    a. Fix:Admin Service Control mechanism improvement.
52. [Bug Fix] eITS#210701928
    a. Fix: Limited Administrator Users Cannot Open Online Help by Clicking Help Button at Top of Web GUI Windows.
53. [Bug Fix] eITS#210800069

a. Fix: GUI display issue in Russian.

54. [Bug Fix] eITS#210800203
    a. Fix: Login password complexity issue
55. [Bug Fix] eITS#210800397
    a. Fix: 2FA VPN Authentication page vulnerability
56. [Bug Fix] eITS#210800854
    a. Fix: Support Username with "DOT" character in security policy filter
57. [Bug Fix] eITS#210801237
    a. Fix: USG FLEX series GUI display issue
58. [Bug Fix] eITS#190200518, 210200133
    a. Fix: LAN packets leaks to WAN interface and leads to SIP registration issue.
59. [Bug Fix] eITS#210200573, 210200579
    a. Fix: Video streaming packet dropping issue.
60. [Bug Fix] eITS#210500498, 210500611
    a. Fix: Stability issue.
61. [Bug Fix] eITS#210600320, 210701277
    a. Enhancement:
        1. Change TLSv1.0 to TLSv1.2 on FTP service
        2. X-Content-Type-Options supported
        3. DNS service enhancement to improve the security protection
        4. Support X-XSS-Protection.

[On Cloud mode]

1. [ENHANCEMENT] ATP series and USG20(W)-VPN Support Nebula management.
2. [ENHANCEMENT] DNS / URL Threat Filter and IP Reputation support External Block List.
3. [ENHANCEMENT] Remote Access IPSec VPN support email provision SecuExtender IPsec VPN Client IKEv2 configure and BWM setting.
4. [ENHANCEMENT] Support Nebula Native:
    a. Change site or change Organization without ZTP.
    b. Remove from site or changing site will reset device to default configure but keep the P2 WAN setting.
    c. Change Organization support reset device to default configure or reset but keep the P2 WAN setting.
5. [ENHANCEMENT] Local GUI support multi-language.

6. [Bug Fix] eITS#210400878
   a. VPN series can't complete ZTP.
7. [Bug Fix] eITS#210500633
   a. Enhance: Support special characters in the pre-shared key.
8. [Bug Fix] eITS#210900025
   a. Fix: Static DHCP assignment issue.
9. [Bug Fix] eITS#210600242, 210800245
   a. Fix: Hostname can't be displayed on the NCC portal.

[AP Controller]

1. [ENHANCEMENT] APC forward compatibility enhancement for AP management.
2. [Feature Change] AP firmware upgrade change to Manual mode
3. [ENHANCEMENT] Support Wireless health.
4. [ENHANCEMENT] Product spec enlarge AP Groups.

Model	WAS	IS
USG FLEX 500	8	16
USG FLEX 700	8	32
ATP500	8	16
ATP700	8	32
ATP800	8	32
VPN1000	16	32

Features: V5.02(ABUJ.1)C0

Modifications in V5.02(ABUJ.1)C0 - 2021/08/11

[On-Premises mode]

1. [ENHANCEMENT] User page enhancement.
   a. Separate Local Administrator and User in different tables.
   b. Local Administrator account table add Create Date, Password Last change and Password Expired Date information.
2. [ENHANCEMENT] Security Check enhancement.
   a. Security Policy page add warning message and button to popup Security Check configuration page when security risk detected.
3. [ENHANCEMENT] Limit SSLVPN port access.
4. [ENHANCEMENT] Isolate the service port of Zyxel SecuExtender IPSec VPN Client provisioning service.
5. [Vulnerability Fix] eITS#210800397
   a. Fix: 2FA VPN Authorization email link is vulnerable to XSS injection.
6. [Bug Fix] eITS#210700565
   a. Fix: 2FA page did not change to the customized certificate issue.
7. [Bug Fix] eITS#210700589
   a. Fix: SSLVPN Port changing malfunctioning.

[On-Cloud mode]

1. [Bug Fix] eITS#210601690
   a. Fix: Password is support symbols `~!@#$%&()_={}|;:'<,>./

[AP Controller]

N/A

Features: V5.02(ABUJ.0)C0

Modifications in V5.02(ABUJ.0)C0 - 2021/07/04

[On-Premises mode]

1. [Vulnerblilty Fix] Authentication bypass vulnerability (CVE-2021-35029).
2. [ENHANCEMENT] Privileged accounts password change reminder.
3. [ENHANCEMENT] Support configurable 2FA service port.
4. [ENHANCEMENT] Disable HTTP port automatically while allowing WAN management in security check wizard.
5. [ENHANCEMENT] Enhance admin-type user change logs to alert level.
6. [Bug Fix]
   a. Fix: Refine service port warning message in security check wizard.

[On-Cloud mode]

1. [ENHANCEMENT] Optimize the client usage monitor performance
2. [ENHANCEMENT] Support SIP ALG setting
3. [ENHANCEMENT] Support USG FLEX 100W built-in Wi-Fi
4. [BUG FIX] eITS#210500387
   Symptom: USG FLEX cannot establish VPN connection will show phase2 local policy mismatch log.
5. [BUG FIX] eITS#210401279
   Symptom: Configure NAT(Virtual server or 1:1NAT) rule will show unknown user with public IP address on client monitor page.
6. [BUG FIX] eITS#210500394
   Symptom: Client monitor page will show duplicate client.

[AP Controller]

N/A

Features: V5.01(ABUJ.0)C0

Modifications in V5.01(ABUJ.0)C0 - 2021/06/26

[On-Premises mode]

1. [ENHANCEMENT] The new Initial Setup Wizard will facilitate user to enforce security policies against access to the web management interface and SSL VPN service (from the Internet).
2. [ENHANCEMENT] Add Security Policy Check to spot out misconfiguration of security policies via pop-up window.
3. [ENHANCEMENT] Add configuration change log of user object.
4. [ENHANCEMENT] To strengthen security access under Covid19 pandemic, given GeoIP feature by default on all devices.

[On-Cloud mode]

N/A

[AP Controller]

N/A

Features: V5.00(ABUJ.2)C0

Modifications in V5.00(ABUJ.2)C0 - 2021/05/13

[On-Premises mode]

1. [ENHANCEMENT] IKEv2 EAP certificate provisioning support.
2. [ENHANCEMENT] Add switch option at login landing page to on-Cloud mode and ZTP demonstration video.
3. [Vulnerability FIX] A potential command execute vulnerability fix.
4. [BUG FIX] eITS#210400868
   a. USG40W / crash and reboot with system-default.

[On-Cloud mode]

1. [ENHANCEMENT] Add switch option at login landing page to on-Cloud mode and ZTP demonstration video.
2. [ENHANCEMENT] L2TP client information deliver to Cloud.

[AP Controller]

1. [ENHANCEMENT] Supported AP image upgrade to 6.20p0c0.

Features: V5.00(ABUJ.1)C0

Modifications in V5.00(ABUJ.1)C0 - 2021/04/12

[On-Premises mode]

1. [ENHANCEMENT] Support new feature: Collaborative Detection & Response (CDR).
2. [ENHANCEMENT] Support New Feature: DNS Content Filter.
3. [ENHANCEMENT] Support "Application object" option on BWM setting. (eITS #180900290)
4. [ENHANCEMENT] Support FQDN in IP Exception. (eITS#200400419)
5. [ENHANCEMENT] Support “space” character in signature search for IDP feature.
6. [ENHANCEMENT] Unified Block Page layout design and support customization for Web Content Filter and URL Threat Filter.
7. [ENHANCEMENT] Support IDP detection mode.
8. [ENHANCEMENT] Support ECDSA certificate.
9. [ENHANCEMENT] ADP is blocking VPN connections - ADP flood detection supports white list. (eITS#200801840)
10. [ENHANCEMENT] Display full Application name on device GUI.
11. [ENHANCEMENT] GUI usability enhance with suggesting setting when user click ‘Add’ at UTM features.
12. [ENHANCEMENT] Support secure tunnel for Remote AP (RAP).
13. [ENHANCEMENT] Web Authentication support managed AP 802.1x SSO and 2FA with Google Authenticator.
14. [ENHANCEMENT] Support SSL VPN service port configurable.
15. [ENHANCEMENT] Remote Access VPN Wizard support behind NAT scenario.
16. [ENHANCEMENT] Support IKEv2 configure provisioning for Zyxel VPN Client (SecuExtender IPsec).
17. [ENHANCEMENT] Support Auto SNAT for traffic from VPN client to Internet.
18. [ENHANCEMENT] Support CEF log format.
19. [ENHANCEMENT] Allow address object name with ‘.’ symbol.
20. [ENHANCEMENT] Support Notification Feature at Top Tool Bar.
21. [ENHANCEMENT] Support a policy route to do SNAT for local out traffic. (eITS#181200948 & 191000578)
22. [ENHANCEMENT] Support CIDR notation for IP object SUBNET. (eITS#200500332)

23. [ENHANCEMENT] CPU Temperature Information periodically to Syslog. (eITS#200700038)
24. [ENHANCEMENT] Add an option to allow NAT port forwarding rules on HTTP/HTTPs.
25. [Feature Change]
    a. Virtual Server Load Balance 'Source Hashing' change to 'Source IP'
    b. Remove VRRP and GRE from Default Service Group.
    c. Unified the statistic page layout.
26. [Vulnerability Fix] Security update of DNS Server Package. (CVE-2016-2776, CVE-2020-8616, CVE-2020-8617, CVE-2020-8622)
27. [Vulnerability Fix] Security update of OpenSSL package. (CVE-2020-1971)
28. [Vulnerability Fix] Add sanity check on CRLF to prevent cross-site scripting attack. (Acknowledgement Soter IT Security)
29. [BUG FIX] eITS#150300799, 150400336, 200900300
    a. Fix: SSO malfunctioning and leads to device reboot.
30. [BUG FIX] eITS#191100507, 210101016, 210100783
    a. Fix: Device FTP service can't be disabled.
31. [BUG FIX] eITS#200201380
    a. Fix: ADP blocks the traffic incorrectly.
32. [BUG FIX] eITS#200400514
    a. Fix: After editing the NAT virtual server rule, the modified rule didn't write to the system correctly.
33. [BUG FIX] eITS#200500708
    a. Fix: IKEv2 VPN connection stability issue.
34. [BUG FIX] eITS#200501370
    a. Fix: Improved the AD authentication speed.
35. [BUG FIX] eITS#200602920
    a. Fix: WAN trunk will not update the connection info when the DHCP client setting changes the gateway which will lead to routing issue.
36. [BUG FIX] eITS#200603933
    a. Enhance: CPU usage chart will now show the average usage of all cores.
37. [BUG FIX] eITS#200701085
    a. Fix: L2TP user connecting information incorrect.
38. [BUG FIX] eITS#200701366
    a. Fix: AD authentication issue.
39. [BUG FIX] eITS#200701414

a. Fix: Incorrect VLAN interface status when binding the VLAN to LAG interface.

40. [BUG FIX] eITS#200800978
    a. Fix: SSID becomes messy code after specific procedure.
41. [BUG FIX] eITS#200801004
    a. Fix: Content Filter website categories correction.
42. [BUG FIX] eITS#200801449, 210200280
    a. Fix: Content Filter malfunctioning issue.
43. [BUG FIX] eITS#200801553
    a. Fix: Initial wizard keep showing up.
44. [BUG FIX] eITS#200801720, 200900099, 200900082
    a. Fix: AP stability issue.
45. [BUG FIX] eITS#200801736
    a. Fix: IPv6 related settings affect the device stability.
46. [BUG FIX] eITS#200801857
    a. Fix: Cannot apply more than 100 security profiles.
47. [BUG FIX] eITS#200900147
    a. Fix: GUI search function in AP list page.
48. [BUG FIX] eITS#200900169
    a. Fix: GUI stop working after clicking on the preview button in the Billing profile page.
49. [BUG FIX] eITS#200900269
    a. Fix: Incorrect logged in user accounting.
50. [BUG FIX] eITS#200900300
    a. Fix: Stability issue when multiple users log in via web auth. concurrently.
51. [BUG FIX] eITS#200900655
    a. Fix: Special character support on DHCP option 60 setting.
52. [BUG FIX] eITS#200900997, 201000468
    a. Fix: Device stability improvement.
53. [BUG FIX] eITS#200901273
    a. Fix: Guest user cannot be deleted automatically nor manually.
54. [BUG FIX] eITS#201000150
    a. Fix: Iperf testing occupies the device memory and leads to reboot.
55. [BUG FIX] eITS#201000694, 201201311
    a. Fix: 2FA functional issue when implementing 2FA with AD server to establish SSL VPN tunnel.
56. [BUG FIX] eITS#201000881

a. Fix: Device Log adjustment.

57. [BUG FIX] eITS#201001082
    a. Fix: Security update of GUI Library for PCI compliance.
58. [BUG FIX] eITS#201001362
    a. Fix: Policy route malfunctioning in specific applications.
59. [BUG FIX] eITS#201100138
    a. Fix: Sandboxing statistics page display error in the GUI.
60. [BUG FIX] eITS#201100207
    a. Fix: GUI settings conflict leads to 2FA functional issue.
61. [BUG FIX] eITS#201100284
    a. Fix: VLAN editing issue on ZyWALL VPN series.
62. [BUG FIX] eITS#201100335
    a. Fix: IKEv2 Proposal mix not working (DH16, DH17, DH18).
63. [BUG FIX] eITS#201100338
    a. Fix: GUI information adjustment.
64. [BUG FIX] eITS#201100511
    a. Fix: DNS query cannot pass through VPN tunnel.
65. [BUG FIX] eITS#201100611
    a. Fix: Wrong virtual MAC address when deploying device HA with SPF as WAN interface.
66. [BUG FIX] eITS#201100642
    a. Fix: Wildcard certificate capability.
67. [BUG FIX] eITS#201100747, 210100862, 210101017
    a. Fix: Memory leakage issue.
68. [BUG FIX] eITS#201100901
    a. Fix: Dynamic-guest got incorrect time period.
69. [BUG FIX] eITS#201100916
    a. Fix: 2FA with SSH malfunctioning.
70. [BUG FIX] eITS#201101132
    a. Fix: Enhanced the configuration conflict prevention.
71. [BUG FIX] eITS#201101204, 201101472
    a. Fix: Log related settings can't be synchronized in HA Pro application.
72. [BUG FIX] eITS#201101209
    a. Fix: HA Pro mechanism improvement.
73. [BUG FIX] eITS#201101275
    a. Fix: GUI operation issue.
74. [BUG FIX] eITS#201101568

a. Fix: BWM malfunctioning.
b. Fix: Cannot apply the limitation on BWM function.

75. [BUG FIX] eITS#201200070
    a. Fix: In LACP + HA Pro scenario, the device will send packets with incorrect source(src) MAC address to the LAN hosts.
76. [BUG FIX] eITS#201200126
    a. Fix: Log message correction.
77. [BUG FIX] eITS#201200144
    a. Fix: Cannot set the SFP port to external in the wizard setting.
78. [BUG FIX] eITS#201200161
    a. Fix: Device generated CSR format can be recognized by specific CSR analyzer.
79. [BUG FIX] eITS#201200332
    a. Fix: Duplicated MAC on lag interface.
80. [BUG FIX] eITS#201200668
    a. Fix: USB log doesn't show IPv6 source and destination address information.
81. [BUG FIX] eITS#201200708
    a. Fix: Address object renaming may lead to unexpected configuration changing.
82. [BUG FIX] eITS#201200934
    a. Fix: Google Authenticator 2FA malfunctioning in specific condition.
83. [BUG FIX] eITS#201200935
    a. Fix: Certificate may be corrupted on HA Pro passive device.
84. [BUG FIX] eITS#201201413
    a. Fix: Content Filter functional issue.
85. [BUG FIX] eITS#210100098, 210100085
    a. Fix: Device stability issue.
86. [BUG FIX] eITS#210100144
    a. Fix: Daily report content correction.
87. [BUG FIX] eITS#210100281
    a. Fix: Log message correction.
88. [BUG FIX] eITS#210100397
    a. Fix: USG FLEX 100W capwap malfunctioning.
89. [BUG FIX] eITS#210100807
    a. Fix: [MAC Address] In User/Group->Mac Address page, when adding new MAC address profile, the GUI will show error.

90. [BUG FIX] eITS#210101205
    a. Fix: Cannot edit bridge interface.
91. [BUG FIX] eITS#210101331, 210200068
    a. Fix: Incorrect Remaining time for Login Users.
92. [BUG FIX] eITS#210101620
    a. Fix: Special character supported.
93. [BUG FIX] eITS#210101673
    a. Fix: Cannot set the lifetime value of 1 year on the self-generated certificates.
94. [BUG FIX] eITS#210200099
    a. Fix: Device GUI layout adjustment.
95. [BUG FIX] eITS#210200733
    a. Fix: Email Security service stability issue.

[On-Cloud mode]

1. [ENHANCEMENT] USG FLEX series support on cloud mode.

[AP Controller]

AP Controller Release Note

Supported AP Platforms

Zyxel WAX series
Zyxel WAC series
Zyxel NWA series

New Feature and Enhancements

[V6.20C0]

1. New Remote AP function providing secured L2 tunnel to office LAN providing same working experience for Work-From-Home users. Supported model: WAX650S, WAX610D, WAX510D, WAC500 and WAC500H.
2. Support Two factor authentication for WiFi connections. Supported model: WAX650S, WAX610D, WAX510D, WAC500 and WAC500H.
3. Strengthen office network security protection by new Collaborative Detection & Response (CDR) function on gateway and Access point.

Supported model: WAX650S, WAX610D, WAX510D, WAC500 and WAC500H.
4. Support zero-wait DFS on WAX650S to provide a non-stop Wi-Fi service to improve user experience.
5. Support Rate control to optimize Wi-Fi network.
6. Support IEEE802.11d configuration to minimize wireless client Interoperability issue.
7. Add Qatar country code.
8. Support 160MHz channel width for Russia(RU), Ukraine(UA) and Belarus(BY).
9. Support 80MHz channel width for Ukraine(UA).
10. Support channel 144 for Russia(RU) and Japan(JP).

[V6.10p10C0]

1. Enhance to allow Managed AP share secret configurable for RADIUS Authentication Server.

[V6.10p8C0]

1. Support new 11ax AP WAX610D.
2. WAX510D and NWA5123-AC HD support tunnel mode.
3. WAX650S, WAX610D, NWA210AX support 11ax 160MHz bandwidth.
4. Enhancement for configuration easy edit.

Bug Fix

[V6.20C0]

1. [BUG FIX] eITS#191201226
   a. Ping lost on MAC device.
2. [BUG FIX] eITS#200900762
   a. Macbook gets "conflicting country codes" errors.
3. [BUG FIX] eITS#201000502
   a. The OID: 1.3.6.1.4.1.890.1.15.3.5.2 stands for signal strength value will be "0" for a long time.
4. [BUG FIX] eITS#201000810
   a. The AP randomly reboot.
5. [BUG FIX] eITS#201100100
   a. Load balance daemon dead caused the CPU HIGH.
6. [BUG FIX] eITS#201100992
   a. AP keeps rebooting when multiple devices are connecting to it.

7. [BUG FIX] eITS#210100347
    a. The AP firmware version is shown incorrect in LLDP information.

[V6.10p10C0]

1. [BUG FIX] eITS#200911360
    a. The search function in AP list does not work.
2. [BUG FIX] eITS#201013064
    a. The AP can't upgrade the firmware because the capwap upgrade number is stuck.
3. [BUG FIX] eITS#201224515
    a. VPN 1000 can't find WAC500H in port setting of AP group.

[V6.10p8C0]

1. [BUG FIX] eITS#200300207
    a. The station has connection problem.
2. [BUG FIX] eITS#200602911
    a. MAC-address table of NWA1123-Acv2 with SNMP is incorrect.
3. [BUG FIX] eITS#200603705
    a. NWA5123AC-HD may happen data stuck in specific condition.
4. [BUG FIX] eITS#200900099, 200801720
    a. AP reboots randomly.

Features: V4.62(ABUJ.0)C0

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

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

Features: V4.60(ABUJ.1)C0

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

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

Features: V4.60(ABUJ.0)C0

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

1. [ENHANCEMENT] SSL Inspection enhancement
   a. Support TLS1.3
   b. Support ECDSA certificate generation
   c. Performance enhancement
2. [ENHANCEMENT] Support customized block page of Content Filtering and URL Threat Filter at Notification > Response Message.
3. [ENHANCEMENT] Move Content Filtering HTTPs Domain Filter port setting for Block/Warning page from System/WWW to Content Filtering/General settings.
4. [ENHANCEMENT] Support Content Filtering Black List and White List check after license expired.
5. [ENHANCEMENT] Support IDP and Application Patrol signature information query at OneSecurity Threat Intelligence web site.
6. [ENHANCEMENT] URL Threat Filter Log add 'Log-alert' type.
7. [ENHANCEMENT] Security services Log message format change.
8. [ENHANCEMENT] Cloud CNM SecuReporter new add Application Statistic category.
9. [ENHANCEMENT] [Secure Policy] CLI command support update firewall rule by rule name.
10. [ENHANCEMENT] System GUI HTTPs service security enhancement
    a. Support TLS 1.3
    b. TLS 1.0/1.1 disabled by default
    c. Weak chipper DES is deprecated
11. [ENHANCEMENT] System FTPs service security enhancement
    a. Weak cipher RC4/3DES disabled by default
    b. Support CLI to enable 3DES/RC4 cipher
12. [ENHANCEMENT] System SNMP service security enhancement
    a. SNMP service disable by default
    b. Remove default Get/Set Community string
    c. Support CLI to disable SNMPv1(eITS#190800258)

    Note:
    If you never change the default value of Get/Set Community string. After upgrade to 4.60, the value will be reset (as 4.60 default). You need to configure the Community string if you want to enable SNMP.

13. [ENHANCEMENT] Support Google Authenticator two-factor authentication for administrator access.
14. [ENHANCEMENT] Support send configuration by Email
15. [ENHANCEMENT] Support Scheduling Auto configuration backup and send via Email.
16. [ENHANCEMENT] Support Scheduling Reboot function.
17. [ENHANCEMENT] Support LAG feature for USG2200, ATP500 / 700 / 800, VPN300 / 1000, USG FLEX 500 / 700.
18. [ENHANCEMENT] Support Virtual Server Load Balancer (*on ATP/USG FLEX/VPN)
19. [ENHANCEMENT] Support Remote Access VPN Wizard for easy VPN client configuration.
20. [ENHANCEMENT][IPsec VPN] Support Diffie-Hellman Groups 19/20/21.
21. [ENHANCEMENT] Support Web-auth/VPN auth./wireless 8021.1X authenticate with Windows Server 2016 and 2019.
22. [ENHANCEMENT] APC upgrade to V3.60 support new features and 11ax AP.
    a. WPA3 enhancement.
    b. AP Log message enhance for Kick station enhancement of sticky clients
    c. Diagnostic enhancement for technical support.
    d. WAX510D and WAX650S AP support.
    e. Support wireless interface packet at Packet Capture on AP.
    f. Fully compatible configuration support for compatible AP
    g. Enhance Top N Stations traffic statistics from 24hour to 7days.
    h. Support Load-Balancing in AP Management.
    i. 802.11ax support.
    j. Tunnel SSID can chose Internal Ethernet interface not only VLAN support.
    k. Support Unicode SSID.
23. [ENHANCEMENT] GUI enhancement
    a. Support GUI grid tip content of objects
    b. Align the terms of Networking traffic indication
24. [Feature Change] Security service Black List behavior change, when Hit black list it will be blocked.
25. [Feature Change] [SMS] End of ViaNett support.
26. [Feature Change] [SSH] The GUI modification remove SSH Version 1.
27. [Feature Change] [Web Authentication] Default uncheck SSO when add new Web Auth. Policy.
28. [Feature Change] [ATP100W / USG FLEX 100W / USG40W / USG60W / USG20W-VPN] Default disable built-in Wi-Fi for Security purpose.

29. [BUG FIX][CVE-2015-5477] System DNS service vulnerability fix.
30. [BUG FIX][CVE-2020-3702] Cryptographic issues in WiFi driver(Kr00k) on USG40W, USG60W
31. [BUG FIX] eITS#200100755
    Fix: HA syncing issue when using FTPs to sync up the settings.
32. [BUG FIX] eITS#200301052
    Fix: Site to site VPN routing issue.
33. [BUG FIX] eITS#200301256
    Add L2TP VPN user login information on SecuReporter.
34. [BUG FIX] eITS#200400280
    Fix: FQDN malfunctioning when the cache is full.
35. [BUG FIX] eITS#200401028
    Debug log adjustment.
36. [BUG FIX] eITS#200401102
    Load-Balancing on VTI-Trunk enhancement.
37. [BUG FIX] eITS#200401499
    IP MAC binding malfunction issue.
38. [BUG FIX] eITS#200500114
    Fix: The syslog does not send out device HA role changed log.
39. [BUG FIX] eITS#200500789
    Enhancement: Disable TLS v1.0 for ddns service.
40. [BUG FIX] eITS#200525649
    SSL VPN connection issue.
41. [BUG FIX] eITS#200602927
    Fix: Direct router table isn't appearing at once in packet flow explore page.
42. [BUG FIX] eITS#200603039, 200603825
    IDP functional issue when the sessions over 20000.
43. [BUG FIX] eITS#200603050, 200603439
    Malfunction in user group when authenticating by 802.1x with external RADIUS server.
44. [BUG FIX] eITS#200603107
    Incorrect SSL VPN status information in dashboard.
45. [BUG FIX] eITS#200603276
    GUI time display issue.
46. [BUG FIX] eITS#200603297
    Object reference table display issue.
47. [BUG FIX] eITS#200603364

Incorrect 3G/LTE dongle warning message

48. [BUG FIX] eITS#200603806
    MAC address table display issue
49. [BUG FIX] eITS#200603855
    Email Security functional issue.
50. [BUG FIX] eITS#200700662
    Hyperlink redirect to incorrect page.
51. [BUG FIX] eITS#200603433
    Fix: Accounting packet issue for L2TP.
52. [BUG FIX] eITS#200700596
    Fix: Connectivity Check functional issue.
53. [BUG FIX] eITS#200700772
    Fix: Mail notification with invalid header error.
54. [BUG FIX] eITS#200701095
    Fix: Deactivated Interface IP address reply ICMP ping.
55. [BUG FIX] eITS#200701207
    Fix: L2TP User Group Issue.
56. [BUG FIX] eITS#200701291
    Device stability enhancement.
57. [BUG FIX] eITS#200800125
    Fix: OSPF routes will be reset after clicking "apply" on interfaces
58. [BUG FIX] eITS#201000416
    Fix: Port Zone changing issue.
59. [BUG FIX] eITS#201000593
    GUI wording fine-tuned.

Features: V4.55(ABUJ.0)C0

Modifications in V4.55(ABUJ.0)C0 - 2020/05/20

1. [ENHANCEMENT] GUI wording modification
   a. ATP100W Monitor > Wireless > AP information > Single AP page remove the decimal point in the axes of station count.
2. [ENHANCEMENT] Adopt new Technology from Security Partner: McAfee for Content Filtering, URL Threat Filter, and Email Security.
3. [ENHANCEMENT] IP Exception feature support on Anti-Malware (including sandboxing), URL Threat Filter, IDP, and IP Reputation.
4. [ENHANCEMENT] Support Advisory link for IDP log.
5. [FEATURE CHANGE] IP Reputation change the phishing category scan from "The Internet And Local Networks" to "The Internet" only.
6. [BUG FIX][CVE-2019-18991] Data injection to WPA-protected network vulnerability fix.
7. [BUG FIX] eITS#190900659
   a. Fix: IPSec VPN connection issue.
8. [BUG FIX] eITS#200201047
   a. Fix:The object reference of ip address cannot be displayed in NAT source.
9. [BUG FIX] eITS#191101378
   a. Fix: Widgets showing issue.
10. [BUG FIX] eITS#200200523
    a. Fix:The VPN connection status mismatch in Dashboard.
11. [BUG FIX] eITS#200201144
    a. Fix:No duration time in session monitor page.
12. [BUG FIX] eITS#200201403
    a. Fix: DNS domain query failed issue
13. [BUG FIX] eITS#200201344
    a. Fix:IKEv2 connection issue.
14. [BUG FIX] eITS#200201040
    a. Fix:The Traffic Usage on the Secureporter mismatch with the device's monitor page.
15. [BUG FIX] eITS#200300672
    a. Fix: SSL VPN user number incorrect issue.
16. [BUG FIX] eITS#200100755
    a. Fix: The Virtual Interface GUI does not show the interface description.
17. [BUG FIX] eITS#200300558

a. Fix: Schedule object displaying issue in security policy.

18. [BUG FIX] eITS#200107100
    a. Fix: CPU overloading issue when plugging in specific LTE dongle.
19. [BUG FIX] eITS#200300595
    a. Fix: Device does not send traffic log to SecuReporter.
20. [BUG FIX] eITS#200301428
    a. Fix: The count of "Managed AP Service" incorrect issue.
21. [BUG FIX] eITS#200105159
    a. Fix:App patrol can't block facebook and youtube.
22. [BUG FIX] eITS#200301256
    a. Fix: No logged-in logs on the SecuReporter for L2TP VPN users.
23. [BUG FIX] eITS#200300829, #200301264, #200301372
    a. Fix: 2 factor authentication issue when establishing the SSL VPN tunnel.
24. [BUG FIX] eITS#200200741
    a. Enhancement: Increase Lease time limit to 7200 for ext-user.
25. [BUG FIX] eITS#200301211
    a. Fix: Device HA failover issue in specific conditions.
26. [BUG FIX] eITS#200200523
    a. Fix:The VPN connection status mismatch in Dashboard.
27. [BUG FIX] eITS#200300148
    a. Fix: DHCP service down in specific conditions.
28. [BUG FIX] eITS#200400084
    a. Fix: 2FA mail content format.
29. [BUG FIX] eITS#200301052
    a. Fix: Policy route routing issue when deploying Site to site VPN with dynamic peer scenario.
30. [BUG FIX] eITS#200300371
    a. Fix: ZySH daemon stability improvement.

Features: V4.50(ABUJ.0)C0

Modifications in V4.50(ABUJ.0)C0 - 2020/03/31

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 Firewall 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, "539ABUJ0C0.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 Firewall 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 Firewall.
   - Router>**enable**
   - Router#**configure terminal**
   - Router(config)#**setenv-startup stop-on-error off**
   - Router(config)#**write**
   - Load the older firmware to ZyWALL Firewall using standard firmware upload procedure.
   - After system uploads and boot-up successfully, login into ZyWALL Firewall 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 Firewall.
   - Router>**enable**
   - Router#**configure terminal**
   - Router(config)#**setenv-startup stop-on-error off**
   - Router(config)#**write**
   - Load the older firmware to ZyWALL Firewall using standard firmware upload procedure.

- After system upload and boot-up successfully, login into ZyWALL Firewall via Console/Telnet/SSH.
- Router>**enable**
- Router#**write**

Now the system is successfully downgraded to older version.
Note: ZyWALL Firewall 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 Firewall platform status. If user wants to use this feature, you must prepare the following step:

1. Have ZyWALL Firewall mib files(ZYXEL-ZW-SMI.MIB, ZYXEL-ZW-COMMON.MIB) and install to your MIBs application (like MIB-browser).
2. ZyWALL Firewall SNMP is enabled.
3. Using your MIBs application connects to ZyWALL Firewall.
4. SNMPv2 private MIBs support three kinds of status in ZyWALL Firewall:
    1. CPU usage: Device CPU loading (%)
    2. Memory usage: Device RAM usage (%)
    3. VPN IPSec Total Throughput: The VPN total throughput (Bytes/s), Total means all packets(Tx + Rx) through VPN.

Appendix 3. Firmware Recovery

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

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 2

```
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 Firewall's IP addresses, your computer must use a static IP address in this range to recover the firmware.
- Connect your computer to the ZyWALL Firewall's port 2 (the only port that you can use for recovering the firmware).
- Use an FTP client on your computer to connect to the ZyWALL Firewall. This example uses the ftp command in the Windows command prompt. The ZyWALL Firewall'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 Firewall (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 Firewall 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 Firewall automatically restarts.

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

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

- The username prompt displays after the ZyWALL Firewall starts up successfully. The firmware recovery process is now complete and the ZyWALL Firewall 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!!