www.zyxel.com

ZYXEL
NETWORKS

Release Note

USG FLEX H Series

Zyxel Security Firewall

Version V1.35 Patch 2

September 1, 2025

PDF
Adobe

Contents

Supported Platforms

Zyxel USG FLEX H Series

USG FLEX 50H / USG FLEX 50HP / USG FLEX 100H / USG FLEX 100HP / USG FLEX 200H / USG FLEX 200HP / USG FLEX 500H / USG FLEX 700H

Versions

USG FLEX 50H

uOS Version	V1.35(ACLO.2) | 2025-08-22 11:50:00
Firmware Image File name	135ACLO2C0.bin
Recovery Image File name	135ACLO2C0.ri

USG FLEX 50HP

uOS Version	V1.35(ACLP.2) | 2025-08-22 11:50:52
Firmware Image File name	135ACLP2C0.bin
Recovery Image File name	135ACLP2C0.ri

USG FLEX 100H

uOS Version	V1.35(ABXF.2) | 2025-08-22 10:49:19
Firmware Image File name	135ABXF2C0.bin
Recovery Image File name	135ABXF2C0.ri

USG FLEX 100HP

uOS Version	V1.35(ACII.2) | 2025-08-22 10:51:56
Firmware Image File name	135ACII2C0.bin
Recovery Image File name	135ACII2C0.ri

USG FLEX 200H

uOS Version	V1.35(ABWV.2) | 2025-08-22 11:47:28
Firmware Image File name	135ABWV2C0.bin
Recovery Image File name	135ABWV2C0.ri

USG FLEX 200HP

uOS Version	V1.35(ABXE.2) | 2025-08-22 11:48:16
Firmware Image File name	135ABXE2C0.bin
Recovery Image File name	135ABXE2C0.ri

USG FLEX 500H

uOS Version	V1.35(ABZH.2)	2025-08-22 11:47:36
Firmware Image File name	135ABZH2C0.bin
Recovery Image File name	135ABZH2C0.ri

USG FLEX 700H

uOS Version	V1.35(ABZI.2)	2025-08-22 11:49:43
Firmware Image File name	135ABZI2C0.bin
Recovery Image File name	135ABZI2C0.ri

Files lists contain in the Release ZIP file

*Note: Please refer to the version table for the following file names mapping.

Firmware Image File name: 135A__2C0.bin
Purpose: This binary firmware image file is for normal system update.
Note: The firmware update may take five or more minutes depending on the scale of device configuration. The more complex the configuration, the longer the update time. Do not turn off or reset the Security Appliance while the firmware update is in progress. The firmware might get damaged, if the device loses power or you reset the device during the firmware upload.

File name: 135A__2C0.conf
Purpose: This ASCII file contains default system configuration commands.

File name: 135A__2C0.pdf
Purpose: This release file.

Recovery Image File name: 135A__2C0.ri
Purpose: This binary firmware recovery image file is for emergent system firmware damage recovery only.
Note: The Security Appliance firmware could be damaged, for example by the power going off or pressing Reset button during a firmware update.

Read Me First

This is the uOS1.35 Patch2 firmware release for USG FLEX H series.

1. The system default configuration is summarized as below:

   - The default device administration username is "admin", password is "1234" or see the Device label.

   - The default LAN interface is ge3, which are port 3 (P3)/ port 4 (P4). The default IP address of lan1 is 192.168.168.1/24.

   - By default, WWW/SSH service can only be accessed from LAN subnet.

   - The default WAN interface is ge1, and the secondary WAN interface is ge2. These two interfaces will automatically get IP address using DHCP by default.

   - For the first setup, it requires connecting to the Internet with your Zyxel account to complete device registration and activation.

2. Please **DO NOT turn off** the power during the firmware upgrade. Please wait until the device reboots and the PWR/SYS LED stays solid.

3. It is recommended that the user backs up "startup-config.conf" file first before upgrading firmware.

4. When getting troubles in configuring via GUI, it is recommended to clear browser's cache first and try to configure again.

5. To reset device to system default configuration, user could press **RESET** button for 7 seconds and the device would reset itself to system default configuration and then reboot.

   > **Note:** After resetting, the original configuration will be removed. It is recommended to back up the configuration before this operation.

Special notices

- Do not utilize the ports allocated to internal services or system services. Assigning a port that is already used by another service, or an internal service can lead to the failure of the service to launch successfully.

  Internal Services port (Reserved):

  53/67-68/179/500/546-547/694/830/953/1812-1813/2601-2605/2616/3799/4500/5246-5247/5432/7681-7682/18121/49058

  Built-in System Services Port:

  You can add or change default ports.

System Services	Port
HTTP	80
HTTPS	443
Captive Portal HTTP	1080
Captive Portal HTTPS	1443
SSH	22
SNMP	161
FTP	21
Remote SSL VPN	10443
Tailscale VPN	41641

- Generate self-signed certificate or certificate request obsolete SHA-1.
- **ZON Utility** does **not support H series** models.
- The following table lists the functions/features that are **not yet** supported by uOS products:

Category	Function/ Feature
Wireless	- Data tunneling - Remote AP - WiFi 7 MLO (Default supported but not configurable) - SSID scheduling - Airtime fairness - WMM - Rogue AP detection - Load balance - AP frame capture - Collect AP diagnostic info - WiFi Aid - Top N report
Network	- IGMP Proxy - Proxy ARP - IPv6

	• IPv6-in-IPv4 Tunnel • 6to4 Tunnel • GRE Tunnel • DNS Load Balancing
Routing	• Policy Route Next Hop VPN Tunnel • Dynamic Route (RIP/OSPF/BGP)
VPN	● Secondary peer gateway for VPN failover and fallback ● Supports LAG interface in IPsec S2S and IPsec Remote Access VPN
Bandwidth Management (BWM)	● BWM for Transparent Bridge interface
Authentication	● Cloud Authentication ● Customize and Click-to-continue Captive Portal ● Zyxel Single Sign-On (with SSO Agent)
Security UTM	● Collaborative Detection & Response (CDR) ● ADP–Protocol anomaly rules (specific scenarios use only)
Management	● Nebula Summary Report ● Nebula Remote Access VPN
Hospitality	● Hotspot Management
Maintenance	● Shell script ● Firmware upgrade by USB

Product integration and support

The following table lists uOS1.35 Patch2 product integration and support information:

Web Browser:

Other browser versions have not been tested but may fully function.

Other web browsers may function correctly but are not supported by Zyxel.

Operating System	Web Browser
Windows 11(64-bit)	Microsoft Edge Google Chrome Mozilla Firefox
Windows 10 (64-bit)	Microsoft Edge Google Chrome Mozilla Firefox
Linux OS (Ubuntu)	Mozilla Firefox
macOS Ventura 13	Safari Google Chrome Mozilla Firefox
macOS Monterey 12	Safari Google Chrome Mozilla Firefox

Language support

The following table lists language support information.

Language	GUI
English	Yes
Chinese (Simplified)	Yes
Chinese (Traditional)	Yes
French	Yes
German	Yes
Spanish	Yes
Portuguese (Brazil)	Yes
Polish	Yes
Turkish	Yes
Russian	Yes

IKEv2/SSL Remote Access VPN support

Following is the list for IKEv2/SSL Remote Access VPN supporting applications and operating systems:

VPN Client	Operating System
Zyxel SecuExtender VPN Client	• Microsoft Windows 10 and 11 (64bit) • macOS versions Big Sur, Monterey, and Ventura

Transceivers Support List

Only USG FLEX 700H supports SFP/SFP+.

Other transceivers have not been tested but may fully function.

Other transceivers may function correctly but are not officially supported by Zyxel.

Type	Transceiver Model
10GbE Transceiver Modules	• SFP10G-T [1] • SFP10G-SR [2] • SFP10G-SR-E [2] • SFP10G-LR [2] • SFP10G-LR-E [2]
GbE Transceiver Modules	• SFP-1000T • SFP-SX-D [2] • SFP-SX-E [2] • SFP-LX-10-D [2] • SFP-LX-10-E [2]

* Please note that Direct Attach Copper (DAC) cables are not supported. For optimal performance, use compatible SFP+ optical modules.

[1]: Works with Cat6a/7 Cable up to 30 m. Switch fan speed will speed up to dissipate the addition heat generated by 10G BASE-T transceiver. The maximum

number of 10G copper transceivers a switch can support depends on its thermal design.

[2]: Only connections with patch cords with PC or UPC connectors are supported.

AP Controller Supported Managed AP List

Below is the list of APs that the H Series can manage when functioning as an AP Controller.

● After upgrading to 1.35 Patch2, if you are using 802.1x WPA-Enterprise with the built-in internal authentication server, please **MUST forget or delete the existing SSID profile on wireless client devices** to prevent potential Wi-Fi authentication issues.

uOS version	Support AP model
1.35 P2	WAC500H
	WAX300H
	WAX510D
	WAX610D
	WAX620D-6E
	WAX630S
	WAX640S-6E
	WAX650S
	WAX655E
	WBE510D
	WBE530
	WBE630S
	WBE660S

Features: V1.35(A__.2)C0

Modifications in V1.35(A__.2)C0 -- 2025/09/01

Bug Fix

1. [eITS#250800776]

    Fix the behavior issue when Nebula is selected without network connectivity and without completing the initial setup wizard.

Features: V1.35(A___.1)C0

Modifications in V1.35(A___.1)C0 -- 2025/08/12

Bug Fix

1. [eITS#250501586]

    RADIUS logs cause memory issues, leading to unexpected reboots.
2. [eITS#250701932]

    Security policy cannot detect the user or user group.
3. [eITS#250701854]

    IKEv2 login with AD user is not working when ext-group-user is selected in Remote
    Access VPN > Authentication > User.

Features: V1.35(A__.0)C0

Modifications in V1.35(A__.0)C0 -- 2025/07/22

Feature

1. [Enhancement] Support Pre-configure Settings in Nebula- Set up your firewall even before it's online
2. [Enhancement] Support DNS Content Filter Safe Search. [eITS#240501656, 241000432]
3. [Enhancement] IP Reputation allow/block list supports on local-in traffic. [eITS#240900032]
4. [Enhancement] Integration with Avast SMB- Endpoint Management with Avast Business Hub
5. [Enhancement] Support Microsoft Exchange SMTP OAuth 2.0 [eITS#241100638]
6. [Enhancement] Support IPsec VPN Connectivity Check
7. [Enhancement] Support added for external user groups in Remote Access VPN authentication privileges. [eITS#241000271]
8. [Enhancement] Support scheduled backup rotation for configuration files. [eITS#240901439]
9. [Enhancement] Increased the maximum configuration file upload limit to 65 (including the default 3).
10. [Enhancement] Added support for logging SNAT/DNAT details in CEF traffic logs.
11. [Enhancement] Enhanced WAN Trunk Fallback with automatic connection termination on passive interface during failover for seamless transition. [eITS#250302339]
12. [Enhancement] Support for "BaseDN" and "BindDN" configuration settings for AD authentication. [eITS#250200416, 250300826]
13. [Enhancement] Packet Flow Explorer > Routing Status: Add Tailscale packet flow static route information
14. [Feature Change] Authed IP sets are now separated for Management GUI and Captive Portal.
15. [Enhancement] Separate the SSH port from Device HA and other usage.
16. [Enhancement] Device HA enhancements:
    a. Synchronize UAM events to the passive device
    b. The passive device will always upgrade the firmware on the standby partition.
    c. Supports an automatic full synchronization operation to ensure seamless updates in the following situations:
       i. Device reboot

      ii.   Firmware upgrade

      iii.   Disabling or pausing HA

      iv.   Heartbeat interface reconnection or heartbeat conflict

    d.   Enhanced "Show State" functionality to include failover-count information

17. [Enhancement] GUI and User experience enhancements

    a.   IPsec VPN displays DES decryption for Russia country

    b.   Log filter now supports space characters in keyword filtering.

    c.   Stronger color contrast and bolder text for improved readability. [eITS#250301509]

    d.   Display all interface references –Shows where each interface is used or referenced across settings.

    e.   When the DHCP pool size is set incorrectly, a warning message will pop up. [eITS#250401121]

    f.   Add a hyperlink on the Tailscale configuration page to redirect users to the Tailscale Portal.

    g.   Replaced "Logout" with "Revoke" on the Tailscale configuration page, and updated the associated iNote accordingly.

    h.   Support for the Nebula pre-configuration scenario by enabling the device to process the conversion of the "support" account name and password

    i.   Added the "External Group User" option to the Default Authentication Timeout Settings

    j.   Change the inline editing style to default in editing mode

    k.   Network > Interface table add "MAC Address" column/information

    l.   Added an iNote to inform users that 2FA for VPN access is not supported when accessed directly from the WAN interface. [eITS#240901645]

18. [Enhancement] Updated the Web Help and User's Guide to include VLAN interface notifications in the Interface chapter for better clarity and guidance. [eITS#250601363]

19. [Feature Change] WAN Trunk can only support 1 passive interface.

[AP Controller]

1. [Enhancement] Support MAC authentication with local database
2. [Enhancement] Support UTF-8 SSID
3. [Enhancement] Support LED suppress (Override/Group Setting)
4. [Enhancement] LAN Provision (Override Setting)
5. [Enhancement] Wireless bridge (Override Setting)

Bug Fix

1. [eITS#240501768, 240700730]

   The automatic MAC address assignment for interface is assigning wrong MAC addresses, leading to abnormal behavior in network traffic transfer.

2. [eITS#240901725, 250401491]

   Resolved issues in the traffic flow process that could cause system instability during spoofing prevention and anti-malware operations.

3. [eITS#250200887]

   After PPPoE is reconnected, policy routing cannot be automatically enabled.

4. [eITS#250201234]

   Resolved an issue where USG FLEX H users were unable to configure remote access VPN due to a missing provision CLI in the Convert Tool.

5. [eITS#250201553]

   Creating multiple IPSec VPN Phase policies with user-defined Local/Remote policies continuously causes error message.

6. [eITS#250400138]

   Resolved two issues in device HA scenarios:
   - (1) the Syslog server could stop functioning unexpectedly.
   - (2) Addressed a problem where the HA passive device encountered errors due to applying an incomplete configuration file.

7. [eITS#250400363]

   USG FLEX H keeps send ARP broadcast that is not triggered by ping-check.

8. [eITS#250400596]

   The password of the DDNS profile cannot be set to '_' underscore character.

9. [eITS#250400848]

   Adjust the following logs to debug level:

   (1) abnormal tcp traffic detected, source port is zero, DROP.

   (2) abnormal tcp traffic detected, destination port is zero, DROP.

   (3) abnormal udp traffic detected, source port is zero, DROP.

   (4) abnormal udp traffic detected, destination port is zero, DROP.

10. [eITS#250401058]

    Modifying VPN settings causes PPPoE to keep redialing.

11. [eITS#250401127, 250401228]

    Firewall offline due to PPPoE is changed.

12. [eITS#250401204]

    Translation issues in the user interface. Improved accuracy and clarity of translations,

especially in German.

13. [eITS#250401353]

PPPoE Interface did not request DNS IP after dial up the connection.

14. [eITS#250401416, 250600069]

GUI doesn't allow interface IP/network overlaps with Secondary IP.

15. [eITS#250401513]

Translation issues in the user interface. Improved accuracy and clarity of translations, especially in Traditional Chinese translation of Virtual Server Port(s).

16. [eITS#250401516]

The certificate was not generated when switching from Manual to Auto with NAT Traversal not empty.

17. [eITS#250401534, 250401613, 250501069]

The firewall is unable to get correct license status from MZC server after working for a while, and caused firewall is unable to send data to SecuReporter.

18. [eITS#250401557]

Device is unable to start up due to an internal system error during boot.

19. [eITS#250401917, 250500833]

PPPoE Interface connection is unstable, and caused firewall online/offline from NCC.

20. [eITS#250500077]

When the certificate list is empty, the manual selection field is marked in red to indicate a missing certificate.

21. [eITS#250500308]

Resolved an issue related to user account queries that caused inefficient memory usage.

22. [eITS#250500336]

Translation issues in the user interface. Improved accuracy and clarity of translations.

23. [eITS#250501361]

Unable to use "-" in Content filter redirect URL issue.

24. [eITS#250501496]

MacBook is not able to get configuration from server with SecuExtender VPN client.

25. [eITS#250600290]

The DHCP Option code 43 cannot be configured on the web GUI.

26. [eITS#250600376]

Admin login fail event is not correct.

27. [eITS#250600378]

The Mail Alert feature did not support multiple selections.

28. [eITS#250600733]

The client did not appear in the NCC client list as expected.

29. [eITS#250601347]

GUI Note for email: valid character does not show [0-9].

30. [eITS#250601674, 250700954]

SSL VPN is not able to be connected.

31. [eITS#250700034]

Revise the VPN configuration saving method to prevent user errors.

[AP Controller]

1. [eITS #250400906]

SSID Settings Page Stuck in Continuous Loading Loop

2. [eITS #250701103, eITS #250701190]

WPA-Enterprise Default Authentication Certificate Expired

● Upgrade your devices to uOS1.35 for enhanced protection against the CVE references listed, as uOS1.35 is no longer vulnerable to them.

• CVE-2024-8176

ZYXEL
NETWORKS

Features: V1.32(A__.0)C0

Modifications in V1.32(A__.0)C0 -- 2025/04/09

Feature

1. [Enhancement] Support DoT/DoH Blocking.
2. [Enhancement] Support Application Patrol allow list to allow only specified applications. [eITS#240900222].
3. [Enhancement] Support Sign-on Captive Portal (Web authentication policy). Behavior change notice: Since uOS 1.32, only users listed in the Captive Portal authentication policy can log in and access the Internet through the device.
   Parameter:

Maximum Authentication Policy	10
Maximum Exempt List per Policy	50
Maximum Walled Garden per Policy	30

4. [Enhancement] Support Tailscale VPN.
5. [Enhancement] IPsec VPN support Bridge interface.
6. [Enhancement] Support LAG (Link Aggregation) interface.
7. [Enhancement] Support external user group.
8. [Enhancement] Bandwidth Management support schedule, rule type per-user and per-source-ip.
9. [Enhancement] Support AP Controller with Secure WiFi service.
   Special Notice: Remote AP and Tunnel AP are not supported yet; support is planned for the July 2026 release.
   a. Managed AP Numbers:

Model Name	Default Manageable AP Numbers	Maximum Manageable AP Numbers
USG FLEX 50H/50HP	8	12
USG FLEX 100H/100HP	8	24
USG FLEX 200H/200HP	8	40
USG FLEX 500H	8	72
USG FLEX 700H	8	520

   b. Wireless configuration for AP Controller and AP management.
   c. Support AP Controller and AP Log settings and events.
   d. Support AP Controller SNMP.

e. Unmask SSID pre-shared key. [eITS#220200760, 230101321]

f. Gold Security Pack add Secure WiFi service and Support a-la-carte Secure WiFi license.

g. Support IEEE 802.1x authentication.

h. Support APC smart mesh.

10. [Enhancement] Support Route Trace. [eITS#230900984]

11. [Enhancement] Device HA enhancement:

a. Device SYS LED to display Device HA pairing status.

b. Support virtual MAC algorithm.

c. Device HA status display full sync. information config/file lists.

d. Support Pause Device HA function for troubleshooting.

e. For a better user experience, a prompt will appear when uploading firmware via the GUI on a Device-HA setup.

12. [Enhancement] Support Smart Sync.: Nebula and Device local configuration synchronization.

13. [Enhancement] Support Nebula Auto-link VPN (non-nebula VPN).

14. [Enhancement] Support Nebula NAT, Routing, Security Policy and Firewall settings.

15. [Enhancement] Support Nebula Application/Client usage monitoring.

16. [Enhancement] User experience enhancements:

a. Add "Renew" button in Network status > Interface when wan is DHCP client. [eITS#250100625]

b. Update the "Release" icon at Network Status > DHCP Table.

c. On the Interface Configuration page, add a mechanism to check for Static IP and subnet overlap.

d. Update the i-note at Remote Access IPsec and SSL VPN, to make it more clearly.

e. Device reboot event email content fine tune and more information.

17. [Feature Change] "My Certificates" and "Trust Certificates" are each limited to a maximum of 10 certificates.

18. [Feature Change] The GUI will no longer auto-generate Ethernet interfaces upon removal, instead prompting a warning; "eth" interfaces will now be displayed in the Interface Summary, auto-removal behavior is removed, and a new warning will appear if a VLAN interface exists without a corresponding Ethernet interface. [eITS#250200421]

19. [Feature Change] System > Settings Remove the 'HTTP/HTTPS Auth Server' section.

Bug Fix

1. [eITS#160200757]

   HA Certificate sync. Issue.
2. [eITS#210800986]

   Enhancement: Auto whitelisting source IP in backend when VPN tunnels   phase 1 is done.
3. [eITS#221200441]

   When Slave device becomes Active, then in the top icon bar   SecuReporter icon is missing.
4. [eITS#240500400]

   SNMP query is not responding.
5. [eITS#240601358]

   Missing service group member after device reboots.
6. [eITS#241001254, 241200549]

   VPN Pre-shared key is not working when the character " is included.
7. [eITS#241200131]

   Sending the email report takes over 15 minutes.
8. [eITS#241200756, 250100985]

   Windows Server 2025 with AD authentication integration.
   https://support.zyxel.eu/hc/en-us/articles/27386297086610-Zyxel-Firewall-Windows-Server-2025-Active-Directory-and-Zyxel-Firewall-ZLD-5-40-uOS-1-32
9. [eITS#241200902]

   SSL/TLS DoS vulnerabilities (disable DHE).
10. [eITS#241200916]

    Enhancement: Support consumption mode by default and support   multiple PoE devices.
11. [eITS#250100196]

    Enhancement: When using Nebula mode to upgrade firmware, the   firmware will be updated in the standby partition.
12. [eITS#250100275]

    Security Policy User filter does not work for OpenVPN SSL user account.
13. [eITS#250100382]

    The sandboxing feature causes the firewall reboot unexpectedly.
14. [eITS#250100489]

    Remove the unused DOMPurify package.
15. [eITS#250100640, 250201503]

    Need to remove unsupported settings before using converter.
16. [eITS#250201503, 250300781]

Need to remove unsupported settings before using converter.

17. [eITS#250100845, 250101359]

After logging to firewall, the dashboard is not loading and an error   message pops up.

18. [eITS#250100862]

The file still exists on the page of System Log Archives in USB Storage unless   you refresh the page.

19. [eITS#250101171]

Test Web Site Category feature is not working.

20. [eITS#250101226]

After updating the PFS in Phase2 and saving it, the VPN script does not   update the new PFS value (DH5).

21. [eITS#250101289]

When User "Any" is selected, it is not able to authenticate RADIUS users in   IKEv2 Remote Access VPN.

22. [eITS#250101306]

The event log shows multiple "Category query fail-open" messages.

23. [eITS#250101367]

Once the console speed is set to 9600 in PuTTY, the firewall generates noise characters in the console output.

24. [eITS#250101511]

Port 13 and port 14 LED light are not working on USG FLEX 700H.

25. [eITS#250101598]

After logging to firewall, the dashboard is not loading and an error   message pops up.

26. [eITS#250101643]

The event log shows multiple "Category query fail-open" messages.

27. [eITS#250101686]

Test Web Site Category feature not working.

28. [eITS#250101765]

Get config fail message when edit config.

29. [eITS#250101835]

The size of Nebula certificate on firewall is 0 (Null) that causes firewall not   able to get license status.

30. [eITS#250200057]

DNS Content Filter and DNS Threat Filter services cause device reboot.

31. [eITS#250200097]

The event log shows multiple "Category query fail-open" messages.

32. [eITS#250200141]

    The DNS filter feature causes the firewall reboot unexpectedly.

33. [eITS#250200161]

    DNS Content Filter and DNS Threat Filter services cause network slow.

34. [eITS#250200309]

    The DNS content filter feature causes the firewall to unexpectedly reboot.

35. [eITS#250200344]

    Receiving empty alert content when using Office 365 as SMTP server.

36. [eITS#250200466]

    The routing status incorrectly displays the local and remote policies by
    swapping them around.

37. [eITS#250200608]

    Bridge interface and member disappear.

38. [eITS#250201019]

    GUI shows unable to save/write the startup configuration.

39. [eITS#250201655]

    USG FLEX 700H reboots randomly.

40. [eITS#250301115]

    USG Flex 700H rebooted unexpectedly.

41. [eITS#250301533]

    Login User show "-1".

● Upgrade your devices to uOS1.32 for enhanced protection against the CVE references
  listed, as uOS1.32 is no longer vulnerable to them.
    • CVE-2025-1731
    • CVE-2025-1732

ZYXEL
NETWORKS

Features: V1.31(A___.0)C0

Modifications in V1.31(A___.0)C0 -- 2025/01/07

Feature

1. [Enhancement] Support Device HA (Active-Passive mode)
2. [Enhancement] Support Event Notification, sending emails for event and alert logs.
3. [Enhancement] Support Packet Flow Explore
4. [Enhancement] Support SIP ALG
5. [Enhancement] Support Policy-based Site to Site VPN with NAT (NAT over IPsec)
6. [Enhancement] Support Nebula VPN
7. [Enhancement] Support Device and Nebula seamless configuration synchronization.
8. [Enhancement] Support Nebula Firewall Interface settings.
9. [Enhancement] Support Nebula Firewall Object settings.
10. [Enhancement] Support Nebula Auto Rollback WAN function for ISP (Change to a different ISP).
11. [Enhancement] Support Lockout user list that allows admins perform unlock actions.
12. [Enhancement] IPsec VPN Phase 2 now supports Address object selection.
13. [Enhancement] Add USB storage disk full warning.
14. [Enhancement] Support Recovery Manager, one-click backup for configurations and certificates.
15. [Enhancement] Usability enhancements:
    a. Added ""Nebula Status"" to System Dashboard > System.
    b. Added Cloud Firmware download icon to System Dashboard > System when new firmware is available.
    c. Added disconnected legend to System Dashboard > Port.
    d. Added search field to Address and Service Object.
    e. Improved GUI usability, including scroll bar adjustments, DHCP Extended Option reminders, and interface table refinements."
16. [Feature Change] Update Reset button behavior by pressing the Reset button for more than 7 seconds will now retain certificates and user configurations.
17. [Feature Change] The default payload size for "Drop SYN with Payload Pkt" has been modified to 1 byte. [eITS#240901862]
18. [Feature Change] No License Required for Application Usage/Traffic
19. [Feature Change] Updated the Mail Server layout, including the default sender and receiver email addresses

Bug Fix

1. [eITS#240600109]
    NAT rule affects VPN traffic when the NAT destination setting is Any

2. [eITS#240801135]
    CPU usage of core0 and core1 is high even if just a few clients are connected   in LAN.

3. [eITS#240801153]
    If the firewall runs for a few days, the memory usage will gradually increase.

4. [eITS#240801231]
    The CF service will perform additional scanning, which may increase memory
    usage and lead to system reboots.

5. [eITS#240801470]
    Local out traffic failure if WAN(Static IP) isn't in Trunk member

6. [eITS#240801545]
    External block list can't update if HTTP no content-length header

7. [eITS#240801656]
    When accessing the device dashboard, it remains in a loading state, and the   security
policy is missing from the web GUI.

8. [eITS#240801699]
    The syslog daemon dead and leads firewall is unable to send out the syslog to
    server.

9. [eITS#240801798]
    No settings are displayed in the web GUI when the device has been running   for around 5
to 10 days.

10. [eITS#240900150]
    Sometime USG FLEX 100H becomes unresponsive.

11. [eITS#240900509]
    Network is very slow and GUI can't load

12. [eITS#240900523]
    Apply config failed after the device is upgraded to 1.30 version.

13. [eITS#240901455]
    Firewall will keep CF query until the server reply to firewall. If server stops   replying or
replies slow, it will affect firewall memory high and may lead reboot.

14. [eITS#240901725]
    Stability issue when DNS Domain scan is enabled.

15. [eITS#240901822]
    Can't remove group of user profile

16. [eITS#241000324]
    Multiple entries in the DHCP list are missing MAC addresses.

17. [eITS#241000471]

Unable to delete an empty user group; the GUI becomes unresponsive and   freezes.

18. [eITS#241000768]

CPU usage becomes high when ZSDN sync

19. [eITS#241000983]

An error message pops up when creating a VLAN or Ethernet interface.

20. [eITS#241001089]

In DDNS settings, DDNS update status is "Update Failed" when the primary   address is "Public IP".

21. [eITS#241001229]

The device failed to apply configuration file after upgraded from 1.21WK40 to   1.30. It will roll back to the original firmware partition 1.21WK40.

22. [eITS#241001300]

DHCP service stops for no reason, and LAN hosts cannot obtain an IP address   from the firewall.

23. [eITS#241001397]

Unable to delete multiple "*.log" files at once.

24. [eITS#241001550]

Display of Security Policy jumps randomly

25. [eITS#241001778]

GUI should stop duplicated MAC for reserved DHCP client

26. [eITS#241100097]

DHCP table becomes empty after firmware upgrade

27. [eITS#241100219, 241100331]

LAN and VLAN clients experience ping timeouts to 8.8.8.8 and slow internet access/download speeds.

28. [eITS#241100235, 241200863]

The WAN trunk WRR algorithm is not working as expected; all traffic is routed through a specific WAN interface.

29. [eITS#241100473]

The " character in VPN PSK setting causes VPN tunnel doesn't work and system   is unable to delete completely from system.

30. [eITS#241100480]

The VPN service is affected by the NAT service, causing data traffic to be   unable to pass through.

31. [eITS#241100518]

Improve USG FLEX 700 FAN noises

32. [eITS#241100535]

The firewall reboots unexpectedly due to a memory leak caused by VPN rekey failures

33. [eITS#241100601]

The PoE port stops working after the firmware update to 1.30, and both ports cannot operate simultaneously.

34. [eITS#241101398]

  (1)The firewall stopped sending syslogs to the syslog server.

  (2) The syslogs show a UTC+0 timestamp instead of the corresponding   timestamp for the configured time zone.

35. [eITS#241101415]

  Google MFA binding fails, and no backup codes are displayed in the web GUI.

36. [eITS#241101660]

  If user defined "any" as External IP in NAT rules, it affects VPN traffic matches the rule even if the Incoming interface is configured as "WAN" interface but not VTI interface.

37. [eITS#241200162]

  Unable to delete a user in User Authentication > User/Group > User. The button "Remove" is greyed out.

38. [eITS#241200665]

  SSLVPN provision is not working

Features: V1.30(A__.1)C0

Modifications in V1.30(A__.1)C0 -- 2024/11/06

Bug Fix

1. [Bug Fix][eITS#241001229, 241001349, 241001408, 241001709]
   Unable to upgrade the device from 1.21 to 1.30. It failed to apply configuration file and roll back to the original partition 1.21.
2. [Bug Fix][eITS#241001734]
   Upgrade firmware to 1.21 to 1.30 firmware the system will going as expected. But after reboot firewall manually, the configuration will become to system default.
3. [Bug Fix][eITS#241001817]
   Geo DB back to default signature after rebooted.

ZYXEL
NETWORKS

Features: V1.30(A__.0)C0

Modifications in V1.30(A__.0)C0 -- 2024/10/16

Feature

1. [Enhancement] Support Nebula Topology.
2. [Enhancement] Support Nebula Security Profile Sync.
3. [Enhancement] Support Nebula Site-wide management Device Status feature for comprehensive network oversight.
4. [Enhancement] Support Nebula site-wide management Event Log.
5. [Enhancement] The USG FLEX H series now supports the Entry Defense Pack license, which includes Reputation Filter, SecuReporter, and Priority Support features.
6. [Enhancement] Support Source IP Spoofing Prevention (IP/MAC binding). [eITS#240300026, 210300781]
7. [Enhancement] Support FQDN Address Object. [eITS#230800339, 230900214, 221001833, 221200385, 230600766, 240500098]
8. [Enhancement] BWM support Bridge (Routing mode), PPPoE and VTI interface.
9. [Enhancement] Support Web Console.
10. [Enhancement] Remote Access IPsec VPN support behind NAT scenario.
11. [Enhancement] Support Password complexity for Local user and admin.
12. [Enhancement] Support Scheduling Reboot.
13. [Enhancement] Support PoE power reset at Dashboard > Port Status.
14. [Enhancement] Support sending of scheduled backup configuration via email.
15. [Enhancement] Support "Drop Invalid TCP Flags Packet" at System > Advanced.
16. [Enhancement] Support "Drop TCP SYN Packet" with abnormal payload at System > Advanced.
17. [Enhancement] Support Proton VPN to the APP patrol category "Tunneling". [eITS#221000252]
18. [Enhancement] Support email configuration file with Encryption function. [eITS#240500775]
19. [Enhancement] Support Bridge-Routing mode scenarios. [eITS#230700789]
20. [Enhancement] Support 802.1P Priority on VLAN interface. [eITS#240501460, 240500746]
21. [Enhancement] Support USB Storage log rotate function. [eITS#160301602]
22. [Enhancement] Support more troubleshooting diagnostic files at Diagnostic > System log: apply-config-error, boot-config-error, ipsecvpn.

23. [Enhancement] Diagnostic > Network Tool add IPsec Trace Log for IPsec VPN troubleshooting.

24. [Enhancement] Diagnostic > Network Tool add Nebula Connection Status check.

25. [Enhancement] Support firmware automatic fallback mechanism.

26. [Enhancement] Add Priority Support at Tool Bar > Help, that user can open support tickets for prioritized assistance with Licenses.

27. [Enhancement] Add VLAN ID information in the DHCP Table. [eITS#231101504]

28. [Enhancement] Improve the IPS signature searching efficiency. [eITS#230900165]

29. [Enhancement] Change Dashboard Virtual Device style and add the link speed by colors.

30. [Enhancement] Support USB Storage status at Dashboard. [eITS#230800268, 231201382]

31. [Enhancement] Usability enhancements:
    a. Add check and validation of the Reserved IP Hostname at DHCP Table.
    b. Add Security Profile Sync reminding message when use edit or remove Security services at local GUI.
    c. The Tx and Rx values should be displayed at the same time point in the flowchart. [eITS#231000421]
    d. The log settings display a minus circle, indicating that some log categories are selected.

32. [Feature Change] change the "myZyxel.com" log category name to "License".

33. [Feature Change] Change the default enabled log categories.

34. [Feature Change] Default enable the LLDP function (System > Advanced).

35. [Feature Change] move myZyxel.com log to cloud-helper category.

Bug Fix

1. [Bug Fix][eITS#230500151]
   Once too many objects are configured in App Patrol profile, it will cause the device to get stuck.

2. [Bug Fix][eITS#230701453]
   Duplicate packets when capturing ICMP packets.

3. [Bug Fix][eITS#231201131]
   When users login to device with 2FA, event logs shows "0.0.0.0" in both source and destination IP address. There is no destination IP in the log of Administrator login.

4. [Bug Fix][eITS#240400191]
   It takes a long time for the interface to get the IP.

5. [Bug Fix][eITS#240400563]

High memory usage.

6. [Bug Fix][eITS#240500400]

    SNMP query is not responding.

7. [Bug Fix][eITS#240500775]

    Unable to e-mail the configuration backup from the H series firewall. The sender field in the configuration backup mail is root, not the email address.

8. [Bug Fix][eITS#240600660]

    If connecting the Zyxel SFP 10G-T (RJ45), P13 or P14 of USG FLEX 700H become port down.

9. [Bug Fix][eITS#240601179]

    The dashboard memory usage and SNMP query do not match.

10. [Bug Fix][eITS#240601626]

    Deleting default Security Policy for SSL VPN will be re-created after a reboot.

11. [Bug Fix][eITS#240700792]

    Device hang up

12. [Bug Fix][eITS#240700915]

    In Network status > DHCP table > Click Add, the Host name shows the remind message as "The value in this field is duplicate"" even there is no duplicated host name.

13. [Bug Fix][eITS#240700919]

    If specific characters is configured in DHCP IP reservation, it causes DHCP function stop to work.

14. [Bug Fix][eITS#240701396]

    2FA doesn't work after the power cord is removed and reconnected.

15. [Bug Fix][eITS#240701628]

    (Sweep) UDP Sweep should be in uppercase.

16. [Bug Fix][eITS#240701749]

    Change IPS signature GUI style.

17. [Bug Fix][eITS#240701765]

    Virtual server is not working after firewall reboot.

18. [Bug Fix][eITS#240701793]

    DHCP process stop to work if specific HOST character in reserved hosts.

19. [Bug Fix][eITS#240701946]

    Fail to capture ICMP packet when split threshold value is not the default.

20. [Bug Fix][eITS#240800592]

    It takes a long time for the interface to get the IP.

21. [Bug Fix][eITS#240800778]

ZYXEL
NETWORKS

If specific characters are configured in DHCP IP reservation, it will cause DHCP function stop to work.

22. [Bug Fix][eITS#240800822]

In VPN Status > SSL VPN, there is "Disconnect" button but it is always greyed out.

23. [Bug Fix][eITS#240800866]

The memory usage on the USG FLEX 700H reached 91% after running for 9 days.

24. [Bug Fix][eITS#240801054]

Static DHCP entries cannot be edited.

25. [Bug Fix][eITS#240801364]

If the referenced IP address group includes any "empty" address object, the policy control rule will behave unexpectedly.

26. [Bug Fix][eITS#240801540, 240801470]

Main Route should involve Active interface regardless static IP or DHCP and even if not the trunk member.

27. [Bug Fix][eITS#240801732]

Network is instable when MTU lower 1500.

28. [Bug Fix][eITS#240801834]

On dashboard CPU% chart, it shows core1 to core4. However, in diagnostics > CPU/Memory Status, it shows CPU0 to CPU3.

29. [Bug Fix][eITS#240801834]

On dashboard CPU% chart, it shows core1 to core4. However, in diagnostics > CPU/Memory Status, it shows CPU0 to CPU3.

30. [Bug Fix][eITS#240900132]

When you download multiple VPN profiles on iOS, a new file removes the existing profile.

31. [Bug Fix][eITS#240900141]

The SSL VPN connection cannot be blocked from accessing the defined Local Network by the security policy's default rule.

32. [Bug Fix][eITS#240900292]

Cannot join the domain because the NetBIOS domain name starts with a number, such as 123zyxel.com.

33. [Bug Fix][eITS#240901043]

There are many "Two-factor Auth. daemon: uam_read_event error, ret = -1" logs on the collected USB log file.

34. [Bug Fix][eITS#240901052]

Unable to change DNS order.

35. [Bug Fix][eITS#240901130]

Device rebooted unexpectedly since lock incorrect parameters.

36. [Bug Fix][eITS#240901316]

Unable to add VLAN to the port interface.

37. [Bug Fix][eITS#240901822, 241000471]

Unable to delete an empty user group; the GUI becomes unresponsive and freezes.

38. [Bug Fix][eITS#241000008]

DHCP reservation keeps loading continuously when clicking the ""Reserve"" button. The issue can be seen in remote site.

39. [Bug Fix][ZNGA-5381]

Disable Force change password will reset the Default Authentication Timeout Settings.

40. [Bug Fix][ZNGA-5378]

From tooltip to edit Zone will not show any Interface in the selection list.

41. [Bug Fix][ZNGA-5458]

The display of what's new content will run into auto refresh loop if opened from the dashboard.

● Upgrade your devices to uOS1.30 for enhanced protection against the CVE references listed, as uOS1.30 is no longer vulnerable to them.
  • CVE-2024-6387
  • CVE-2024-9677

ZYXEL
NETWORKS

Features: V1.21(A___.0)C0

Modifications in V1.21(A___.0)C0 -- 2024/07/16

Feature

1. [Enhancement] Content Filter/SSL Inspection support inspect TLS 1.3 hybridized Kyber session. [eITS#240401693, 240401220, 240401350][ZNGA-4890, 4960, 5005]

2. [Enhancement] Support modify Zone in IPsec/SSL Remote Access VPN. [ZNGA-5018, 5020]

3. [Enhancement] Newly supported applications include: Zoom, Webex, Google Meet, Skype, WeChat, Yandex Stream for Bandwidth Management. [eITS#210800391, 220200469][ZNGA-4906, 4907]

4. [Enhancement] Usability enhancements:

    a. Add License Service expiration notification. [ZNGA-4830, 4833, 4834]

    b. A memory check mechanism has been added for firmware upgrades, with a pop-up reminder message. [ZNGA-4732, 4775, 4777, 4778, 4779]

    c. Tooltips can be clicked to redirect and edit the objects. [eITS#230900100] [ZNGA-3681]

    d. Add a redirect link to SecuReporter at security statistics page, allowing users to easily check historical data. [ZNGA-4824]

    e. Add SecuReporter tutorial video. [ZNGA-4825]

    f. Unify the Timestamp format for statistic graphics. [ZNGA-4887]

    g. Display or hide settings for table columns can be saved. [ZNGA-4392]

    h. Enhance the user interface entry fields to be wider for better key-in visibility. [eITS#230701262][ZNGA-4911]

    i. Add pattern validation for the subject of certificate. [ZNGA-4695]

    j. Fine tune the hint message to make it more precise. [ZNGA-4807]

    k. Support scan statistics of sandboxing on SecuReporter. [eITS#240501652] [ZNGA-5289]

5. [Feature Change] Hidden the PKCS#12 password for security. [eITS#231200194][ZNGA-4909]

6. [Feature Change] Stop Cloud firmware updates if the current firmware is Project/ITS firmware to avoid losing ITS-specific bug fixes. [ZNGA-4989, 4990]

7. [Feature Change] Change FTP ALG default settings: [eITS#231201239][ZNGA-4908]

    a. Enable FTP ATG from Disable to Enable.

    b. Enable FTP Transformation from Disable to Enable.

Bug Fix

1. [Bug Fix][eITS#231100879][ZNGA-4071]

    Open another website will redirect to uOS after logout.

2. [Bug Fix][eITS#231200398][ZNGA-4269]

    The device becomes unresponsive and stop processing traffic.

3. [Bug Fix][eITS#240100668][ZNGA-4539]

    Remote access VPN cannot be established.

4. [Bug Fix][eITS#240201429][ZNGA-4753]

    The device becomes unresponsive.

5. [Bug Fix][eITS#240301616][ZNGA-4782]

    Unable to establish SSL VPN using OpenVPN on mobile phone.

6. [Bug Fix][eITS#240400076][ZNGA-4836]

    iOS OpenVPN traffic cannot go through VPN tunnel to Internet in full tunnel mode.

7. [Bug Fix][eITS#240400192][ZNGA-4847]

    The device rebooted unexpectedly.

8. [Bug Fix][eITS#240400989][ZNGA-4874]

    Incorrect IPS and Sandboxing statistical data on SecuReporter.

9. [Bug Fix][eITS#240401060, 240600483][ZNGA-4882]

    USG FLEX 200H works properly but it is always offline on Nebula.

10. [Bug Fix][eITS#240401303][ZNGA-4894]

    Error message: "Unable to save/write the startup config ..." appears when moving policy route order.

11. [Bug Fix][eITS#240401280][ZNGA-4895]

    VPN configuration page gets stuck on loading when setup.

12. [Bug Fix][eITS#240500136][ZNGA-4955]

    Use CLI to create "Configuration backup schedule". If the minute value is '00', it is not displayed in the GUI, only the hour.

13. [Bug Fix][eITS#240500140][ZNGA-4988]

    Search Base in Active Directory is not working.

14. [Bug Fix][eITS#240401531][ZNGA-4991]

    Site-to-site VPN traffic goes to the wrong zone for security policy management.

15. [Bug Fix][eITS#240500438][ZNGA-5069]

    Security policy is not working after modify the action from allow to deny in bridge mode.

16. [Bug Fix][eITS#240500522][ZNGA-5004]

Unable to apply imported configuration file.

17. [Bug Fix][eITS#240501331][ZNGA-5056]

Typo on USG FLEX H.

18. [Bug Fix][eITS#240501546][ZNGA-5098]

Network Status -> DHCP Table sorting order works incorrectly.

19. [Bug Fix][eITS#240600115][ZNGA-5115]

If 00 is configured as minute in Configure Backup schedule > Enable Auto Backup > Daily, it becomes empty after the settings are saved.

20. [Bug Fix][eITS#240600764][ZNGA-5258]

NAT rule cannot be applied properly.

21. [Bug Fix][eITS#240600735][ZNGA-5259]

On Site to Site VPN monitor page, it shows all VPN tunnels are disconnected even they are properly connected.

22. [Bug Fix][eITS#240601117][ZNGA-5271]

NAT rule does not take effect after object type "interface IP" is used.

23. [Bug Fix][eITS#240501404][ZNGA-5286]

USG FLEX 100H works properly but it is always offline on Nebula.

24. [Bug Fix][eITS#240600305][ZNGA-5287]

Policy route health check does not work as expected. It is always "down" even wan link is up and ping check is successful.

25. [Bug Fix][eITS#240500726][ZNGA-5382]

SSL VPN tunnel disconnects after 60 minutes.

26. [Bug Fix][eITS#240600938][ZNGA-5383]

DDNS is unable to be updated.

27. [Bug Fix][eITS#240601358][ZNGA-5386]

Service disappear from service group after device reboots.

28. [Bug Fix][ZNGA-3402, 3314]

Malfunction when set banner via CLI command.

29. [Bug Fix][ZNGA-4754]

IPSec VPN VTI interface ping check cannot trigger IKE negotiation.

30. [Bug Fix][ZNGA-4762]

[GUI/Policy Route] Change browser to Firefox then move rule will appear error undefined.

31. [Bug Fix][ZNGA-4768]

[File Manager] DUT will not reboot when apply system-default.conf.

32. [Bug Fix][ZNGA-4846]

VTI interface in user defined Trunk is not working.

33. [Bug Fix][ZNGA-4883]

[Remote Access IPsec VPN] Add admin user type into Remote Access VPN results in failure to provision the Remote Access IPsec VPN configuration to local user.

34. [Bug Fix][ZNGA-5036]

Users may encounter issues where the DHCP Relay retains outdated IP addresses and upstream interface configurations.

35. [Bug Fix][ZNGA-5042]

An unexpected behavior occurs in the DHCP Relay functionality when the upstream interface setting is left empty or set to any other interface.

36. [Bug Fix][ZNGA-5045]

When the PPPoE interface is active, other VLANs cannot obtain IP addresses.

37. [Bug Fix][ZNGA-5091]

[Interface/GUI] Remove port from port group that GUI will keep loading

38. [Bug Fix][ZNGA-5094]

DHCP option 46 is not working.

39. [Bug Fix][ZNGA-5102]

DHCP Relay interface is same as upstream interface, then the DHCP Relay will not work.

- Upgrade your devices to uOS1.21 for enhanced protection against the CVE references listed, as uOS1.21 is no longer vulnerable to them.
  - CVE-2024-3596

Features: V1.20(A__.2)C0

Modifications in V1.20(A__.2)C0 -- 2024/06/04

Bug Fix

1. [Bug Fix] [eITS#240501707, 240501747]
    DHCP server doesn't work on VLAN interface.

ZYXEL
NETWORKS

Features: V1.20(A___.1)C0

Modifications in V1.20(A___.1)C0 -- 2024/05/21

Bug Fix

1. [Bug Fix][eITS#240400401][ZNGA-4854]

    Where DHCP relay traffic was not being sent over the tunnel.

2. [Bug Fix][eITS#240401226][ZNGA-4891]

    CF profile reference display issue.

3. [Bug Fix][eITS#240401237][ZNGA-4892]

    Devices became unresponsive when modifying bandwidth management rules.

4. [Bug Fix][eITS#240401564][ZNGA-4926, 4965]

    Unclear service port conflict messages prevented configuration changes.

5. [Bug Fix][eITS#240500137][ZNGA-4971]

    The site-to-site tunnel could not connect when the pre-shared key included ' or ".

Features: V1.20(A__.0)C0

Modifications in V1.20(A__.0)C0 -- 2024/04/18

Feature

1. [Enhancement][eITS#230701372] Support External Block List for Reputation Filter. (ZNGA-1125,1126,1127,4023)
2. [Enhancement] Support ARP Spoofing Protection.
3. [Enhancement] Reputation Filter supports the Allow List push from SecuReporter portal. (ZNGA-3267, 3268, 3269)
4. [Enhancement] Support VPN failover. (ZNGA-3456,2883,2819,1700,532)
5. [Enhancement] Support Bandwidth Management (BWM). (ZNGA-3705, 4548, 4366)
6. [Enhancement] Add Copy function for Security Policy. (ZNGA-3723)
7. [Enhancement] Support Microsoft AD Authentication for IPsec/SSL Remote Access VPN. (ZNGA-1134,3163,3272,4373)
8. [Enhancement] Support LDAP external Authentication for SSL Remote Access VPN. (ZNGA-1565)
9. [Enhancement] Allow conversion from Wizard-type to Custom-type on the VPN Wizard edit page.
10. [Enhancement] VPN Wizard edit page: add 'Go to Static Route' link when edit route-based rule. (ZNGA-4660)
11. [Enhancement] Support SSL VPN add to Zone. (ZNGA-4138,4492)
12. [Enhancement] Support two-factor authentication for VPN access using Google/Microsoft Authenticator. (ZNGA-4162,442)
13. [Enhancement] Site-to-Site VPN Wizard and Custom type add Routes conflict check.
14. [Enhancement] Support failover for Static Route and Policy Route through ping-check. (ZNGA-1705)
15. [Enhancement] [eITS#230801176] Support VTI in Policy Route. (ZNGA-2393,3445,3456,3678)
16. [Enhancement] [eITS#230801177] Support policy route health check. (ZNGA-3744,4186)
17. [Enhancement] Implement rule-based hit count information for Security Policy and Policy Route. (ZNGA-3142,3487)
18. [Enhancement][eITS#230700790] Add disable option for Global Zone Forwarder. (ZNGA-3680)

19. [Enhancement][eITS#240101556] Add Services Port conflict check and message. (ZNGA-4612,4712,4487)
20. [Enhancement] Add status column and Routes conflict check in Static Router page. (ZNGA-4614)
21. [Enhancement][eITS#230700934] Support modify MAC address for Ethernet Interface & VLAN Interface. (ZNGA-3291, 923)
22. [Enhancement] DHCP enhancement:
    a. DHCP Table add Edit action and Description column. (ZNGA-3695)
    b. DHCP Table add Host Name duplicated check in Static IP.
    c. [eITS#230800272, 231200626] Support DHCP extended options to internal interfaces. (ZNGA-3740,4793)
    d. On the Network > Interface page, automatically fill in the Start IP field in the DHCP Server section when editing or adding LAN settings. (ZNGA-3702)
23. [Enhancement] [eITS#230800732] DDNS supports behind NAT scenario that will update the public IP. (ZNGA-3743)
24. [Enhancement] Implement DDNS failover based on the connection status of the interface. (ZNGA-4176)
25. [Enhancement] Support Session Control function. (ZNGA-419)
26. [Enhancement] Bridge interface add "Role" setting (ZNGA-4338)
27. [Enhancement] add "VLAN ID" column in the Interface page. (ZNGA-4009)
28. [Enhancement] Implement automatic update functionality for the GeoIP database and Certificates. (ZNGA-3790,4670)
29. [Enhancement] Support CIDR Notation. (ZNGA-3396, Seeding#1278)
30. [Enhancement] Add GeoIP country information in the Log/Events page. (ZNGA-3520)
31. [Enhancement] Add address object range hint message at Address Object. (ZNGA-4377)
32. [Enhancement] New Add Traffic Statistics > Application Usage. (ZNGA-22,4183)
33. [Enhancement] Device Insight enhancement:
    a. Add Astra data source to Device Insight. (ZNGA-3266, 3965, 4285)
    b. Gray out the 'Remove' button when a Blocked client is selected. (ZNGA-4734)
34. [Enhancement] [eITS#230701224] Stop username from being capitalized when Login. (ZNGA-3359)
35. [Enhancement] Display boot up status at System Dashboard. (ZNGA-3538)
36. [Enhancement] [eITS#230800348] Double-click to enter Edit mode. (ZNGA-3540)
37. [Enhancement] Display session duration in the format of hh:mm:ss in the Session Monitor. (ZNGA-3691)
38. [Enhancement] Add Export function at Log page (Export to Excel file). (ZNGA-2971)

ZYXEL
NETWORKS

39. [Enhancement] Enhance the configuration backup feature to only perform a backup when there are changes to the configuration. (ZNGA-3734)

40. [Enhancement][eITS#230800053] Add description field to Allow/Block list for the security services. (ZNGA-3738)

41. [Enhancement] [eITS#230800351] Revise the GUI grid table resizing behavior,

42. introducing a new 'Fit View' functionality. (ZNGA-3741)

43. [Enhancement] [eITS#230801252] Add the system language setting to the top right corner. (ZNGA-3745)

44. [Enhancement] Add an 'Advanced' page within the System category. This 'Advanced' page allows users to adjust System Parameters, such as UDP/ICMP timeout, and includes toggles for enabling or disabling Additional Features. (ZNGA-3941)

45. [Enhancement] Log event add Src. Port (Source Port) and Dst. Port (Destination Port) information. (ZNGA-4003)

46. [Enhancement] Implement hover effects on action icons. (ZNGA-4087)

47. [Enhancement] Initial Setup Wizard refine the Nebula onboarding flow. (ZNGA-4093)

48. [Enhancement] Support Configuration File test/verify function. (ZNGA-4337)

49. [Enhancement] Troubleshooting enhancement:
    a. Display error message at Console when apply configuration failed. (ZNGA-3797)
    b. Display boot up status and message at Console. (ZNGA-3799)
    c. Allow copying the configuration to a USB drive using the command-line interface (CLI). (ZNGA-3892)
    d. Diagnostic content add a file of Boot & Apply process logs. (ZNGA-4165)
    e. Add file header to the configuration file. (ZNGA-4364)

50. [Enhancement] Click "The latest log" title in System Dashboard will redirect to the Log/Event page. (ZNGA-4250)

51. [Enhancement] Implement the new filter style on the Log page and Session Monitor. (ZNGA-4355,4542)

52. [Enhancement] Change address object type 'CIDR' to 'SUBNET' (ZNGA-4375)

53. [Enhancement] Object pages to add 'Description' column. (ZNGA-4376)

54. [Enhancement] Add URL report link at Content Filter General and URL Threat Filter General page. (ZNGA-4552)

55. [Enhancement] Email Daily Report add Application Usage. (ZNGA-4554,4591)

56. [Feature Change] DoS Prevention is turned off by default. (ZNGA-4444)

57. [Feature Change] Default enable the "Auto Reboot" function when doing Firmware Auto Update and Remove the on/off from GUI (ZNGA-4751)

58. [Feature Change] By default, PoE power is disabled on Port 3 and Port 4 for USG FLEX 700H. (ZNGA-4360)

59. [Feature Change] Menu Tree adjustment (ZNGA-4371):
    a. Change 'System Statistics' to 'Traffic Statistics'
    b. Move out "Session Monitor" to 'Traffic Statistics'
    c. Remove "Resource" from 'Traffic Statistics'. Resource data can be read at System Dashboard.
    d. New add "Application Usage" to 'Traffic Statistics'
    e. Move Device Insight on/off to "Advanced" page

Bug Fix

1. [Bug Fix][eITS#230700936][ZNGA-3339]
   Interface setting is ineffective after interface type is changed.
2. [Bug Fix][eITS#230701023][ZNGA-3309]
   NAT rule is not working.
3. [Bug Fix][eITS#230701149][ZNGA-3333]
   Add static DHCP reservation entries in Network > Interface.
4. [Bug Fix][eITS#230800882][ZNGA-3478]
   Devices should not respond to DNS queries originating from the WAN interface when a security policy with content filtering is applied between the WAN and WAN interfaces.
5. [Bug Fix][eITS#230801575][ZNGA-3593]
   Firewall local-out SNAT does not work.
6. [Bug Fix][eITS#230900765][ZNGA-3755]
   Firewall do Destination NAT even if TCP first packet is not SYN.
7. [Bug Fix][eITS#230900864][ZNGA-3776]
   Unable to disable DHCP server of all interfaces.
8. [Bug Fix][eITS#230901363][ZNGA-3862]
   Under the EEE feature, the AP may encounter compatibility issues with certain devices.
9. [Bug Fix][eITS#230901052][ZNGA-3812]
   DNAT cannot work.
10. [Bug Fix][eITS#231000138][ZNGA-3872]
    With AES128/SHA256 with DH14/DH2 groups, IPSec VPN on iPhone cannot be established.
11. [Bug Fix][eITS#231000224][ZNGA-3889,3890]
    Inactivate VPN profile but the status still shows connected.
12. [Bug Fix][eITS#231000238][ZNGA-3883]

If the VPN profile name exceeds 19 characters, it always in loading status when clicking "connect" button.

13. [Bug Fix][eITS#231000350][ZNGA-3894]

In PPPoE, the settings should not be saved when the retype password field of is empty.

14. [Bug Fix][eITS#231000557][ZNGA-3915]

The extension .conf should be added automatically while users backup configuration.

15. [Bug Fix][eITS#231000599][ZNGA-3918]

Unable to edit Default Trunk.

16. [Bug Fix][eITS#231000601][ZNGA-3919]

In the Initial Wizard, it should not allow users to configure different subnets in WAN IP and default gateway.

17. [Bug Fix][eITS#231000868][ZNGA-3940]

Unable to set the static DHCP IP in the DHCP server option. Users need to navigate to Network Status > DHCP Table to configure.

18. [Bug Fix][eITS#231001044][ZNGA-3957]

Anti-malware causes network slowness.

19. [Bug Fix][eITS#231001922][ZNGA-4005]

Skip the second connection test when the device passes the first connection test.

20. [Bug Fix][eITS#231001962][ZNGA-4010]

Unable to access the internet the device becomes unresponsive.

21. [Bug Fix][eITS#231001978][ZNGA-3994]

USG Flex 700H is experiencing unexpected reboots when a USB flash drive is plugged in.

22. [Bug Fix][eITS#231001989][ZNGA-4060]

The connection port statistics traffic graph displays abnormally.

23. [Bug Fix][eITS#231001990][ZNGA-3989]

Graph of the same port are duplicated in System Statistics > Port > Monitor Port.

24. [Bug Fix][eITS#231002035][ZNGA-4011]

Unable to assign the DHCP IP because the device becomes unresponsive.

25. [Bug Fix][eITS#231002151][ZNGA-4027]

Poor SSL Inspection performance and Teams is not usable.

26. [Bug Fix][eITS#231100108][ZNGA-4014]

Firewall does not assign IP address to the connected host, and even cannot be connected with static IP.

27. [Bug Fix][eITS#231100792][ZNGA-4065]

NAT rule doesn't work if one of wan connections is lost.

28. [Bug Fix][eITS#231101152][ZNGA-4114]

    The page for Trunk is stuck in loading.

29. [Bug Fix][eITS#231101272][ZNGA-4090]

    Sometimes the NAT and routing settings disappear.

30. [Bug Fix][eITS#231101418][ZNGA-4151]

    When enabling/disabling remote access VPN function, an error message pops up on GUI.

31. [Bug Fix][eITS#231200178][ZNGA-4161]

    Once the firewall rule applied user profile, the rule cannot detect VPN related session.

32. [Bug Fix][eITS#231200349][ZNGA-4170]

    When disabling DHCP server on GE3, you cannot make any changes in the GE4.

33. [Bug Fix][eITS#231200357][ZNGA-4168]

    SNAT entry in policy route becomes "none" after IP address is configured and saved.

34. [Bug Fix][eITS#231200715][ZNGA-4206]

    The firewall rule cannot detect the SSL VPN connection established from the OpenVPN Connect with user ID.

35. [Bug Fix][eITS#231200716][ZNGA-4196]

    Network > Interface > Trunk fails to load.

36. [Bug Fix][eITS#231200802][ZNGA-4198]

    Unable to control user by remote VPN by firewall rule

37. [Bug Fix][eITS#231200991][ZNGA-4317]

    After firewall reboots, you need to inactivate/activate the NAT profile again to make NAT work again.

38. [Bug Fix][eITS#231201025][ZNGA-4233]

    If you create more continent GeoIP objects, some Geo IP addresses are not correctly assigned. After these continent GeoIP objects are removed, these Geo IP addresses can be correctly assigned.

39. [Bug Fix][eITS#231201089][ZNGA-4259]

    The device doesn't generate sys log into USB storage immediately.

40. [Bug Fix][eITS#231201247][ZNGA-4256]

    IKEv2 remote VPN connection cannot access internet.

41. [Bug Fix][eITS#231201457][ZNGA-4255]

    Firewall cannot obtain IP in specific condition

42. [Bug Fix][eITS#231201467][ZNGA-4281]

    Incorrect limitation for the IPSec VPN zone

43. [Bug Fix][eITS#240100145][ZNGA-4276]
     The nslookup tool cannot resolve the longer TLD domain name. The field should support the TLD length of 63 characters.
44. [Bug Fix][eITS#240100206][ZNGA-4453]
     NAT is not working.
45. [Bug Fix][eITS#240100211][ZNGA-4307]
     When a new user is created, GUI pops up an error message.
46. [Bug Fix][eITS#240100321][ZNGA-4339]
     Sometimes NAT rule and policy disappear. User needs to reboot device to recover it.
47. [Bug Fix][eITS#240100480][ZNGA-4320]
     Create several GeoIP in a address group and apply the group object to a security policy rule. Only the 1st entry is working. It does not go to the 2nd entry but jumps to the next security policy rule.
48. [Bug Fix][eITS#240100590][ZNGA-4343]
     On Dashboard > Security, the area of the threat filter is always loading.
49. [Bug Fix][eITS#240100647][ZNGA-4346]
     When trying to adjust the settings for ge1_PPP, an error pops out. But after clicking OK, the page shows the adjusted settings.
50. [Bug Fix][eITS#240100728][ZNGA-4347]
     Device reboots unexpectedly.
51. [Bug Fix][eITS#240100813][ZNGA-4409]
     The page of Log event is always loading.
52. [Bug Fix][eITS#240100875][ZNGA-4365]
     Relay server settings disappear after you click "Save".
53. [Bug Fix][eITS#240100884][ZNGA-4399]
     When disabling DHCP server on GE3, you cannot make any changes in the GE4.
54. [Bug Fix][eITS#240100980][ZNGA-4451]
     USG Flex H doesn't support IP in IP tunnel routing.
55. [Bug Fix][eITS#240101119][ZNGA-4397]
     All settings on web GUI are empty.
56. [Bug Fix][eITS#240101125][ZNGA-4452]
     The error message "Command failed: CHILD_SA config 'sec_policy1_VPN-HOME' not found" pops up when you connect site-to-site VPN.
57. [Bug Fix][eITS#240101192][ZNGA-4567,4685]
     The PPTP(TCP 1723 port) traffic cannot be NAT forwarded from WAN to LAN normally.
58. [Bug Fix][eITS#240101242][ZNGA-4517]

An error message pops up when dialing PPPoE connection.

59. [Bug Fix][eITS#240101258][ZNGA-4446]

The error "WebSocket KeepAlive failed." appears on Dashboard > System and Network > Interface.

60. [Bug Fix][eITS#240101639][ZNGA-4474]

IKEv2 with Windows native client cannot be connected.

61. [Bug Fix][eITS#240200217][ZNGA-4541]

The device becomes unresponsive.

62. [Bug Fix][eITS#240200307][ZNGA-4514]

When WAN1 connectivity check is fail, the DDNS does not update to WAN2 automatically.

63. [Bug Fix][eITS#240201202][ZNGA-4561]

Firewall rule is not working due to false address-object settings.

64. [Bug Fix][eITS#240201528][ZNGA-4655]

PPTP VPN can't build up when initialed from LAN side..

65. [Bug Fix][eITS#240300253][ZNGA-4616]

The reserved DHCP IP is unable to release from DHCP table after changing the interface IP segment.

66. [Bug Fix][eITS#240300390][ZNGA-4765]

NAT is not working.

67. [Bug Fix][ZNGA-2819, 3817]

After manual disconnect tunnel the IPsec VPN with Nailed-up setting will not auto reconnect.

- Upgrade your devices to uOS1.20 for enhanced protection against the CVE references listed, as uOS1.20 is no longer vulnerable to them.
   - CVE-2023-6398, CVE-2023-6399

Features: V1.10(A__.1)C0

Modifications in V1.10(A__.1)C0 -- 2023/11/21

1. [Enhancement] GUI enhancement
    a. [eITS#231001856] fine tune the wording for Firmware upgrade.
    b. Refine the Menu Tree item "File Manager" to "Firmware/File Manager".
    c. [eITS#230900275] The wording "Diffie-Hellman Groups" in phase 2 is changed to "PFS".
2. [Enhancement] Support CLI to change ICMP timeout value.
3. [Bug Fix] GUI bugs fix:
    a. Change the "Description" field on Device Insight > Edit page from mandatory to optional.
    b. Add a checking mechanism in SSL VPN settings page. When the combination of the incoming interface and DNS name fields is incorrect, the configuration download button will be gray out.
    c. Fix the Query display inconsistent issue at Reputation Filter page.
    d. Fix the System Dashboard loading issue.
4. [Bug Fix] The traffic of established session goes to new next-hop interface but with previous SNAT.
5. [Bug Fix] eITS#230900089
    a. Fixed the problem of incorrect zone name issue.
6. [Bug Fix] eITS#230901003
    a. Fix the problem of Network loop issue when port 1(with vlan configured) and port 2 are connected to a same dummy switch.
7. [Bug Fix] eITS#231000637
    a. Failed to send scheduled daily report.
8. [Bug Fix] eITS#231000957
    a. Failed to add object and object group by policy tooltip.
9. [Bug Fix] eITS#231001098
    a. The VLAN's DHCP Relay setting is disabled unexpectedly when new VLAN DHCP Relays are added.
10. [Bug Fix] eITS#231001941
    a. When changing to different LAN ports, the DHCP IP address cannot be obtained.
11. [Bug Fix] eITS#231001962
    a. The USG Flex 700H reboots unexpectedly and there is no internet due to a fast path CPU deadlock.

12. [Bug Fix] eITS#231002035
    a. LAN clients cannot get DHCP IP.
13. [Bug Fix] eITS#231100687
    a. Sometimes the clients in VLAN interface failed to query DNS after the device reboots.

Features: V1.10(A__.0)C0

Modifications in V1.10(A__.0)C0 -- 2023/10/16

First release.

1. Internet Protocol Version: IPv4 only
2. Firewall Function Supports:
   - Routing and transparent (bridge) modes
   - Stateful packet inspection
   - Dos Prevention (Preventing Flooding and Sweep Attacks)
   - FTP NAT traversal
   - Security Policy
     - Unified policy management interface
     - Policy control criteria by IP/GeoIP/CIDR/ Service
     - Policy control criteria by User
     - Schedule
3. VPN Function Support:
   - IPsec VPN
     - Site-to-Site VPN
     - Remote Access VPN (IKEv2)
     - Native Windows, iOS/macOS and Android (StrongSwan) client provision
   - SSL VPN
     - Client remote access (compatible with OpenVPN Connect)
   - SecuExtender VPN client provision for both IPsec and SSL VPN
4. Security Features and Services Support:
   * Services that requires Gold Security Pack
   - Application Patrol*
   - Intrusion Prevention System (IPS)*
   - Anti-Malware (Cloud Query only) *
   - Web Filtering*
   - Reputation Filter*
     - IP Reputation
     - DNS Threat Filter
     - URL Threat Filter
   - Sandboxing*
   - Device Insight*

- SSL Inspection
- IP Exception

5. Networking Support:
   - Port Grouping
   - Routing mode
     - Policy Route criteria by IP/GeoIP/CIDR/Service
     - Policy Route criteria by user
     - Policy Route criteria by DSCP code
     - Policy Route Schedule
     - Policy Route DSCP Marking
     - Policy Route SNAT
     - Static Route
   - External Interface
     - Types: DHCP, Static, and PPPoE
     - MTU setting
     - VLAN setting
     - MAC address setting
     - DHCP Option 60
   - Internal Interface
     - MTU setting
     - VLAN setting
     - DHCP relay/ server role
     - DHCP Options
     - Static DHCP IP/MAC mapping
   - Bridge Interface -transparent mode only
   - WAN Load Balancing support Weight Round Robin only
   - WAN Failover
   - Dynamic DNS (DDNS)
   - NAT
     - Virtual Server
     - 1:1 NAT
     - Many 1:1 NAT
   - ALG: FTP ALG only

6. Management Support:
   - Nebula Centralized Management
     - Monitor device on/off status
     - Firmware upgrade operation

- o Access remote GUI (requires Nebula Professional Pack)
  - o Backup and restore firewall configurations (requires Nebula Professional Pack)
- Authentication:
  - o Local user database
  - o RADIUS
  - o 2FA Authentication Google Authenticator (Admin only)
  - o IKEv2 with EAP-MSCHAPv2 VPN authentication
- System Management
  - o Firmware upgrade via FTP, FTP-TLS, Web GUI
  - o Multi-lingual Web GUI
  - o Command line interface (Console, SSH and Telnet)
  - o SNMP v1, v2c, v3
- Logging and Monitoring
  - o SecuReporter supported (requires Gold Security Pack)
  - o Syslog Server
  - o Email daily report

7. Maintenance Support:
- Configuration File management
- Firmware upgrade management
- Firmware upgrade schedule
- Diagnostics collection
- Packet Capture
- Network Tools

Limitations

General

1. Not support rename function for following features:
    (1) Interface name
    (2) Policy Route rule name
    (3) Static Route rule name
    (4) Security Policy rule name
    (5) NAT rule name
    (6) IPsec Site-to-Site Rule name
    (7) Security Services Profile name

Network

1. [Port Group]
    (1) Port 1 and Port 2 of the USG FLEX 500H and USG FLEX 700H cannot perform Port Group with other ports.
    (2) Port 13 and Port 14 of the USG FLEX 700H cannot perform Port Group with other ports.
2. [ZNGA-1649] [Interface] Not support multiple interfaces connect on the same Network. Different interface cannot configure IP in the same IP subnet that the ARP Flux problem will cause unexpected traffic forward behavior.
    For example, you configure the interface as following:
    Ge1 interface set or get IP: 192.168.254.10/24
    Ge2 interface set or get IP: 192.168.254.11/24
    This means ge1 and ge2 are on the same IP subnet 192.168.254.0/24
3. [ZNGA-6405][Interface] If a VLAN is bound to an Ethernet physical port, it will only function when the Ethernet is enabled.

IPsec VPN

1. [ZNGA-3935] [Remote Access VPN] For native iOS/macOS design, the lifetime minimum value is 10 minutes. If you set the lifetime less than 10mins, then it cannot connect to iOS/macOS VPN client correctly.
    see reference of the iOS/macOS parameters:
    https://developer.apple.com/documentation/devicemanagement/vpn/ikev2/ikesecurityassociationparameters
2. Device needs to have at least one default route for IPsec VPN traffic forward.

Tailscale

1. [ZNGA-7437] Dual WAN traffic from the device is not supported in Tailscale configurations.

Known Issue

The following issues have been identified in version 1.35P2. To inquire about a particular bug or report a bug, please contact Customer Service & Support.

Nebula

1. [ZNGA-5846] [Reverse Tunnel] User cannot access web console page when login by Nebula Remote Configurator.
   .

System

1. [ZNGA-7192] Diagnostics Collect takes too long time to complete the collection.

Network

1. [ZNGA-4442] [eITS#240100505] NAT is not working after works for hours.
2. [ZNGA-4037] [eITS#231000192] INTERFACE type should contain the status of physical link (layer1), Layer 2 link and connectivity check.
3. [ZNGA-5044] The upstream interface of DHCP Relay does not support PPPoE interface (GUI selection list still show the PPPoE interface).
4. [ZNGA-5988] [DHCP Table] Certain data may be lost if unsupported hostname data is modified and reserved. Users are advised to ensure hostname data complies with supported formats before making changes.
5. [ZNGA-6109] [Bridge][NAT] If NAT loopback is enabled, devices on the same bridged LAN cannot be accessed.
6. [eITS#250701327] The DHCP reserved table may not display correctly. To resolve this, switch to another tab and then return to the DHCP table tab to refresh the status.

IPsec VPN

1. Remote access IPsec VPN does not support two external authentication server.
2. When there are more than 300 VPN tunnels, the device may sometimes not respond and not display status.
3. [ZNGA-5688] Policy-based IPSec VPN doesn't bypass the direct route to other subnets.
4. [ZNGA-7997] The pre-shared key for IPsec Site-to-Site VPN on uOS 1.32 does not support special characters such as ' (single quote), " (double quote), or \ (backslash). However, uOS 1.35 supports these characters. Therefore, for Site-to-Site VPN connections between uOS 1.32C0 and 1.35C0, avoid using these special characters in the pre-shared key.

User & Authentication
1. 2FA valid time does not support the character "+".
2. RADIUS user login with Admin role will pop-up change password message.
3. [ZNGA-4518] [AAA] The joining status is "Not join AD Domain yet." after reboot.
4.

GUI
1. System Dashboard widget will be loading for a while. Please wait till dashboard widget data displays before switching to other GUI pages.
2. [ZNGA-4999] The error messages on the change password page are not precise.
3. [ZNGA-6552] [Device Insight] The Device Insight function remains operational even when a license expired message is displayed.

Log
1. [ZNGA-4447] [eITS#240101503] The syslog format doesn't comply RFC.

Device-HA
1. The SSH service under System > SSH must be enabled on both Zyxel devices, to enable synchronization for Device HA.

Packet Flow Explore
1. [ZNGA-6768, ZNGA-6749] The tooltip for users displays blank when the user is an AD/LDAP/Radius user or when the user's setting is "group" and all members are logged in.

UTM
1. [ZNGA-7240] It will be loading for a long time and there have two rules after edit full category app rules.

APC
1. When enabling the Smart Mesh feature for the first time, a reboot of the access points is required to ensure the feature is properly activated.
2. There is a malfunction with WPA2-Enterprise authentication using EAP-TLS or EAP-TTLS (MSCHAPv2).

3. [SPR: #250307114] When the number of managed APs reaches the system limit, no error message is displayed when attempting to add or manage a new AP.

SSL VPN

1. [ZNGA-8190] SSL VPN works properly when using an AD server as the Secondary authentication server and allowing External Group Users, but ext-group-users are not shown on the **Login User** page.

Appendix 1. Firmware upgrade procedure
The following is the firmware **upgrade** procedure:
- Use Browser to login into ZyWALL Security Gateway as administrator.
- Go firmware upgrade wizard step3 (Firmware Upgrade and Reboot) to auto download and upgrade to the latest firmware.
- After several minutes, the system is successfully boot up with the newest version.