NGAF

NGAF 8.0.23 Version Release Notes

Version 8.0.23

Change Log

Date	Change Description
September 4, 2019	Quick Start Guide release.

Contents

Chapter 1 What is New

[New] IPsec VPN Supports IKEv2 Protocol

IPSec VPN supports IKEv2 protocol and makes NGAF suitable for more deployment scenarios.

[Enhanced] UI Reconstruction of Third-Party Connection in IPSec VPN

The third-party connection UI is reconstructed to enhance user experience.

[Enhanced] Enhanced Security Capability

It supports high-risk vulnerability detection in key modules of HTTP and provides effective security protection.

It enhances parsing capability of bypass methods and engine detection capability to prevent attacks through bypassing.

[Enhanced] Enhanced Security Protection

It enhances error check against multipart header, chunk, etc.

It enhances decoding capability to improve BASE64 error check.

It adds specialized engines and whitelist to protect against WebShell upload, code injection and command injection to improve detection capability.

[Enhanced] Enhanced SSL VPN

It transplants the latest SSL VPN version into this NGAF version to improve usability, adaptation and stability.

SSL VPN becomes compatible with major browsers, such as Google Chrome, Firefox, Microsoft Edge, Internet Explorer, etc.

SSL VPN client becomes compatible with major operating systems, such as Android, iOS, ubuntu, Kylin, etc.

It improves authentication methods of SSL VPN and adds authentication through LDAP to improve usability.

Upgrade Instructions for Customer Service or Distributors

Confirmation Before Upgrade

For Chinese version of NGAF, it supports upgrade from the following earlier versions by loading the upgrade package AF8.0.23(20200511).ssu:

NGAF7.1 official version, NGAF7.2 official version, NGAF7.3 official version, NGAF7.3.0R1 official version, NGAF7.4 official version, NGAF7.5.0 official version, NGAF7.5.1 official version, NGAF8.0.2 official version, NGAF8.0.5 official version, NGAF8.0.6 official version, NGAF8.0.6 R1 beta version, NGAF8.0.7 official version, NGAF8.0.7R2 official version, NGAF8.0.8 official version, NGAF8.0.9 official version, NGAF8.0.10 official version, NGAF8.0.13 official version, NGAF8.0.17 official version, NGAF8.0.18 beta version, NGAF8.0.19 official version, NGAF8.0.20 beta version, NGAF 8.0.22 beta version and NGAF 8.0.23 beta version.

For English version of NGAF, it supports upgrade from the following earlier versions by loading the upgrade package AF8.0.23(20200511).ssu:

NGAF7.1 official version, NGAF7.1 R1 official version, NGAF7.2 official version, NGAF7.3 official version, NGAF7.3.0 R1 official version, NGAF7.4 official version, NGAF7.5.1 official version, NGAF8.0.2 official version, NGAF8.0.5 official version, NGAF8.0.6 official version, NGAF8.0.7 official version, NGAF8.0.7 R2 official version, NGAF8.0.8 official version, NGAF8.0.9 official version, NGAF8.0.10 official version, NGAF8.0.13 official version, NGAF8.0.17 official version, NGAF8.0.18 beta version, NGAF8.0.19 official version, NGAF8.0.20 beta version, NGAF 8.0.22 beta version and NGAF 8.0.23 beta version.

For Chinese version of vNGAF in aCloud, it supports upgrade from vNGAF7.1 R3 official version, vNGAF8.0.8 official version, vNGAF8.0.9 official version, vNGAF8.0.13 official version and vNGAF8.0.17 official version, vNGAF8.0.18 beta version, vNGAF8.0.19 official version, vNGAF8.0.20 beta version, vNGAF8.0.22 beta version and vNGAF8.0.23 beta version to vNGAF8.0.23 official version by loading the upgrade package AF8.0.23(20200511).ssu.

For English version of vNGAF in HCI, it supports upgrade from vNGAF7.1 R3 and vNGAF 8.0.8 official version, vNGAF8.0.9 official version, vNGAF8.0.13 official version, vNGAF8.0.17 official version, vNGAF8.0.18 beta version, vNGAF8.0.19 official version, vNGAF8.0.20 beta version, vNGAF8.0.22 beta version, vNGAF8.0.23 beta version to vNGAF8.0.23 official version by loading the upgrade package AF8.0.23(20200511).ssu.

For Chinese version of vNGAF in aBOS, it supports upgrade from vNGAF7.5.3 official version, vNGAF8.0.8 official version, vNGAF8.0.9 official version, vNGAF8.0.13 official version, vNGAF8.0.17 official version, vNGAF8.0.18 beta version, vNGAF8.0.19 official version, vNGAF8.0.20 beta version, vNGAF8.0.22 beta version and vNGAF8.0.23 beta version to vNGAF8.0.23 official version by loading the upgrade package AF8.0.23(20200511).ssu.

For English version of vNGAF in aBOS, it supports upgrade from vNGAF8.0.8 official version, vNGAF8.0.9 official version, vNGAF8.0.13 official version and vNGAF 8.0.17 official version, vNGAF8.0.18 beta version, vNGAF8.0.19 official version, vNGAF8.0.20 beta version, vNGAF8.0.22 beta version and vNGAF8.0.23 beta version to vNGAF8.0.23 official version by loading the upgrade package AF8.0.23(20200511).ssu.

Upgrade Limitations

Not support upgrade from custom version.

Not support upgrade from version installed KB package.

If "Always detect data packets that traverse repeatedly" is enabled, immediate upgrade is not supported. You need to disable it manually first and upgrade. After upgrading, you may go to System > General > System > Second-passthrough Traffic to enable it.

For upgrade from earlier version, high availability and configuration sync should be disabled first.

Earlier NGAF device cannot be upgraded to version 8.0.23 and its configurations cannot be imported to the device (version 8.0.23) if it has any of the following configurations:

Mobile user or virtual IP pool is configured.

Solution: Delete mobile user(s) or virtual IP pool(s).

Dynamic routing is configured for VPN.

Solution: Disable routing information protocol (RIP) in Network > IPSec VPN > Advanced >

Dynamic Routing.

Default user is configured with local password-based authentication method enabled.

Solution: Disable the default user in Network > IPSec VPN > Local Users.

Multicast or broadcast is enabled for VPN.

Solution: Disable multicast and broadcast in Network > IPSec VPN > Basics > Advanced.

MTU in Basic settings under Sangfor VPN is not within the range 576-1500.

Solution: Change MTU in Network > IPSec VPN > Basics.

IPSec VPN is used in earlier versions but its lines have not been added in multiple lines.

Solution: Enable multiline (gateway) and add a line for IPSec VPN connection in Network > IPSec VPN > Multiline Options.

IPSec VPN is used in earlier versions and there are lines, but multiline is not enabled.

Solution: Enable multiline (gateway) in Network > IPSec VPN > Multiline Options.

Indirect Internet connection is chosen for IPSec VPN basic settings.

Solution: Choose direct Internet connection for IPSec VPN basic settings

Indirect Internet connection is chosen for IPSec VPN multiline options.

Solution: Choose direct Internet connection for IPSec VPN multiline options in Network > IPSec VPN > Multiline Options.

For earlier versions, IPSec VPN outgoing line option is not selected for WAN interface of Sangfor VPN (in single line scenario)

Solution: Follow instructions to fix it.

When the product number between local IP address and peer IP address is over 64 in third-party connection of IPSec VPN, please merge or delete the addresses of local or peer device. You may add them back after upgrade.

Solution: Follow the tips on the manager.

Phase I or Phase II is disabled or unassociated settings when connecting to third-party device in lower NGAF versions.

Solution: Delete or enable the settings and make them corresponding to Phase I or Phase II separately and then upgrade the device.

Not support upgrading devices to this version from earlier versions with memory size smaller than 2 GB (not inclusive of 2 GB) and SSL VPN is activated.

Solution: Remove the SSL VPN license and then upgrade the device to this version.

Not support upgrading devices to this version for vNGAF (vAF-100) with 1 core and 2 GB memory.

Solution: Shut down the vNGAF device and edit its settings to 2 cores and 4 GB memory or higher settings. Restart the device and then upgrade to this version.

Not support upgrade for devices with External Report Center enabled. If you have any problems, please contact Sangfor Customer Service.

Upgrade is not allowed if database service encountered error. In this case, please check the status of database service.

Not support upgrading devices to this version from earlier versions with memory size smaller than 2 GB (not inclusive of 2 GB) and with Engine Model Update activated and valid.

Note: For NGAF devices with 2 GB memory size, Engine Zero Model update has been transferred to the cloud and will be available after Neural-X service is subscribed.

Solution:

If users have subscribed to Neural-X Unknown Threat Update, it is suggested to remove the Engine Model Update license.

2. If users have not subscribed to Neural-X Unknown Threat Update, it is suggested that users subscribe to it.

3. If NGAF devices is inaccessible to the Internet, users can only upgrade NGAF to 8.0.17 or earlier versions.

Immediate Upgrade of Configurations, Logs and Data

Yes

Impacts on Functions After Upgrade

1. The port detection of Web application protection and intrusion prevention is enabled by default after upgrade.

2. PHP code injection prevention, Java code injection prevention, command injection prevention and WebShell upload prevention are added in all templates of Web application prevention after upgrade.

Reboot Required After Upgrade

Yes. Device will restart automatically upon upgrade completion.

Time Taken

Upgrade process may take about 10 minutes under normal circumstance (at least 40% of the total CPU and memory are available, and network is connected).

Upgrade Recommendations

Back up configurations before upgrade.

Before upgrade, make sure network connection is OK.

After upgrade completes, make sure network is not impacted and NGAF manager can be accessed.

If you encounter any problem, contact Customer Service to turn to developer for help.

Upgrade Procedure

To upgrade standalone device, do the following:

Check whether the current version is a custom version, since upgrade from custom version is not supported. Check whether that version has been installed KB package. If KB package has been installed, contact developer to confirm whether the issues brought about by the KB package can be fixed. Check whether that version is an official version. If it is a Beta version (Labeled B), upgrade it to its corresponding official version first. Make sure free space is sufficient.

Get update package and the corresponding MD5 file, and make sure that the MD5 is correct.

Back up configurations and import configuration files.

4. For upgrade from NGAF7.1 or above, launch Sangfor Firmware Updater and load the update package AF8.0.23(20200511).ssu.

After upgrade completion, check network connection and whether NGAF manager can be accessed properly.

To upgrade device in high availability environment, do the following:

Disable high availability and configuration sync, and then follow the upgrade steps (step 1-5 illustrated for standalone device).

After active and standby devices are upgraded, enable HA.

Handling of Upgrade Failure

Scenario 1: Memory is insufficient.

Solution: If memory is insufficient but customer insists on upgrading, contact Customer Service to turn to developer for help.

Scenario 2: Error parsing update package.

Solution: Get update package and MD5 hash file and make sure the MD5 is correct.

Scenario 3: apppre execution failed message occurs, prompting that upgrade from the current version is not supported.

Solution: Check whether the current version is a custom version, since upgrade from custom version is not supported. If it is a Beta version (Labeled B), upgrade it to its corresponding official version first.

Scenario 4: appsh execution failed message occurs, prompting that upgrade is not supported in high availability environment.

Solution: Disable HA and configuration sync before upgrade and then perform upgrade again.

Scenario 5: Other error occurs.

Solution: Contact Customer Service to turn to developers for help.

Precaution

Support upgrade with Sangfor Firmware Updater 6.0 only.

Internal Database

Databases can be updated online. Please log in to NGAF manager and go to System > Security Capability Update to update databases.

Obtain update package from database servers for offline update.

Central management (CM) is not supported, but Sangfor BBC is supported.

Support pass-through. Enabling pass-through does not require a restart of device.

HA module update: Disable HA and configuration sync before upgrading earlier version to this version.

Downgrade is not supported.

SANGFOR

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc