SANGFOR

NGAF

NGAF 8.0.13 Version Release Notes

Version 8.0.13

Change Log

Date	Change Description
Oct 24, 2019	NGAF 8.0.13 Version release notes.

CONTENT

Chapter 1 What is New?

[New]

1. This version integrates new features from NGAF 8.0.10, NGAF8.0.12, C3000 and requirements of Multi-Level Protection System 2.0.

[Scenarios]

1. Support correlation to X-Central and Endpoint Secure and displaying security values on NGAF manager. It helps customers find out security risks and issues by correlating to endpoint and network devices to provide a lightweight, one-stop and closed-loop security solution.
2. Support five new C3000 modules to enhance cost/performance of mid-low end NGAF devices.
3. Support requirements of Multi-Level Protection System 2.0 (MLPS 2.0) to help customers meet its requirements, since MLPS 2.0 will take effect in 1 December, 2019.

Chapter 2 Resolved Issues

[Fixed] Https Decryption

This special scenario also supports SSL decryption： the SSL handshake packet and the data content are in the same package.

[Fixed] WebUI

Optimize related software processes to make WebUI more stable.

[Fixed]SSL VPN

SSL users are often disconnected after logging in, and no virtual IP is obtained.

Chapter 3 Upgrade Instruction

2.1 Confirmation before Upgrade

For Chinese version of NGAF, it supports upgrade from the following earlier versions by loading the upgrade package AF8.0.13(20191020).ssu: NGAF6.5 official version, NGAF6.6 official version, NGAF6.7 official version, NGAF6.8 official version, NGAF7.0 official version, 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, NGAF8.0.7 R2 official version, NGAF8.0.7 R5 beta version, NGAF8.0.8 official version, NGAF8.0.9 official version, NGAF8.0.9 R2 beta version, NGAF8.0.10 official version, NGAF8.0.12 beta version, .

For English version of NGAF, it supports upgrade from the following earlier versions by loading the upgrade package AF8.0.13(20191020).ssu:
NGAF7.0 official version, 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, NGAF8.0.9 R2 beta version and NGAF8.0.10 official version.

2.2 Upgrade Limitations

1. Not support upgrade from custom version.
2. Not support upgrade from version installed KB package.
3. 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.
4. For upgrade from earlier version, high availability and configuration sync should be disabled first.
5. Earlier NGAF device cannot be upgraded to version 8.0.13 and its configurations cannot be imported to the device (version 8.0.13) if it has any of the following configurations:

a) Mobile user or virtual IP pool is configured.
Solution: Delete mobile user(s) or virtual IP pool(s).

b) Dynamic routing is configured for VPN.
Solution: Disable routing information protocol (RIP) in Network > IPSec VPN > Advanced > Dynamic Routing.

c) Default user is configured with local password-based authentication method enabled.
Solution: Disable the default user in Network > IPSec VPN > Local Users.

d) Multicast or broadcast is enabled for VPN.
Solution: Disable mulicast and broadcast in Network > IPSec VPN > Basics > Advanced.

e) MTU in Basic settings under Sangfor VPN is not within the range 576-1500.
Solution: Change MTU in Network > IPSec VPN > Basics.

f) 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.

g) 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.

h) Indirect Internet connection is chosen for IPSec VPN basic settings.
Solution: Choose direct Internet connection for IPSec VPN basic settings

i) 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.

j) 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.

2.3 Upgrade Recommendations

1. Back up configurations before upgrade.
2. Before upgrade, make sure network connection is OK.
3. After upgrade completes, make sure network is not impacted and NGAF manager can be accessed.
4. If you encounter any problem, contact Customer Service to turn to developer for help.

2.4 Upgrade Procedure

- **To upgrade standalone device, do the following:**

1. 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.
2. Get update package and the corresponding MD5 file, and make sure that the MD5 is correct.
3. Back up configurations and import configuration files.
4. Check the version first. For upgrade from NGAF6.5, NGAF6.6 or NGAF6.7 version, launch Sangfor Firmware Updater and load the update package AF_Pre(for 8.0.13).ssu**.** Reboot is not required after upgrade. Then load the update package AF8.0.13(20191020).ssu with Sangfor Firmware Updater. For upgrade from other versions, launch Sangfor Firmware Updater and load the update package AF8.0.13(20191020).ssu**.**
5. After upgrade completion, check network connection and whether NGAF GUI can be accessed properly.

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

1. Disable high availability and configuration sync, and then follow the upgrade steps (step 1-5 illustrated for standalone device).
2. After active and standby devices are upgraded, enable HA.

2.5 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.

Chapter 4 Precautions

1) For versions earlier than NGAF8.0.7 (inclusive of NGAF8.0.7), when IPSec VPN connection is established but multiline options are not specified:
   IPSec VPN will be disconnected but upgrade will succeed if your device is upgraded to NGAF8.0.7 first and then to NGAF8.0.13 (solution: enable multiline and add a IPSec VPN line to multiple line).
2) For earlier versions, IPSec VPN outgoing line is not selected for all WAN interfaces for Sangfor VPN (in multiple line scenario):
   VPN will be disconnected for those IPSec VPN outgoing line is not selected after upgrade to NGAF8.0.13.
3) Support upgrade with Sangfor Firmware Updater 6.0 only.
4) Internal Database
   a) Database can be updated online. Please log in to NGAF manager and go to System > Security Capability Update to udate databases.
   b) Obtain update package from database servers for offline update.
5) Central management (CM) is not supported, but Sangfor BBC is supported.
6) Support pass-through. Enabling pass-through does not require a restart of device.
7) HA module update: Disable HA and configuration sync before upgrading earlier version to this version.
8) 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