FSC 2.x Release Notes

https://campus.barracuda.com/doc/99620324/

Do not manually reboot your system while the update is running. For assistance, contact Barracuda Networks Technical Support.

FSC 2.0.x firmware supports Firewall Secure Connectors 2.x only. Installation on FSC1 appliances is not possible.

FSC 2.0.5 or higher requires a Barracuda Firewall Control Center 7.2.3 + HF898 or higher.

Installing Firewall Secure Connector firmware version 2.0.5 requires migration of the Control Center Secure Connector Editor AFTER updating the Firewall Secure Connectors. This operation cannot be reverted.

- After migration to SC Release 2.0, the editor only supports Secure Connectors 1.x with firmware versions 1.1.5 or higher.
- After migration to SC Release 2.0, the editor only supports Secure Connectors 2.x with firmware versions 2.0.5 or higher.

To migrate the editor, lock the editor configuration on your Firewall Control Center and click **Migrate SC Release**

The Secure Connector deployment needs a Secure Access Controller and a Control Center. See the CloudGen Firewall Release and Migration Notes for additional information.

What´s New in FSC Version 2.0.10

Barracuda Secure Connector version 2.0.10 is the direct successor to Barracuda Secure Connector version 2.0.9 and contains all features delivered with version 2.0.9. In addition to numerous improvements, v2.0.10 offers the following new features:

- Support for TOBY-L201 modem, models SC28 (LTE North America, Verizon) and SC29 (Wi-Fi + LTE North America, Verizon), which support LTE frequency bands B2, B4, B5, B13, and B17 (Verizon) for America.

What´s New in FSC Version 2.0.9

Barracuda Secure Connector version 2.0.9 is the direct successor to Barracuda Secure Connector version 2.0.8 and contains all features delivered with version 2.0.8. In addition to numerous improvements, v2.0.9 offers the following new features:

- Support for Azure IoT Edge and Docker has been implemented for SC containers. [BNNGF-64022], [BNNGF-64023]
- SIM/PUK functionality has been improved. [BNNGF-64428]

Improvements Included in FSC Version 2.0.8

- This update fixes an issue where incorrect SIM PIN did not get recognized and triggered a PUK request. [BNNGF-64428]
- Container Engine selection and configuration has been implemented in container settings. [BNNGF-64025]
- DHCP offset is now disabled at the SC and template configuration when "Automatically" mode is not selected. [BNNGF-64077]

What´s New in FSC Version 2.0.8

Barracuda Secure Connector version 2.0.8 is the direct successor to Barracuda Secure Connector version 2.0.7 and contains all features delivered with version 2.0.7. In addition to numerous improvements, v2.0.8 offers the following new features:

- Support for broadcast traffic forwarding to LAN has been implemented and is now configurable on the Control Center. [BNNGF-61047], [BNNGF-61796]
- Barracuda Secure Connector version 2.0.8 provides a new web interface. For more information, see Secure Connector Web Interface.
- A password change is now enforced during first login and after reset when no custom configuration has been applied. [BNNGF-63735], [BNNGF-63457], [BNNGF-63696]

Improvements Included in FSC Version 2.0.8

- This update fixes an issue where DHCP relay was not working after disconnecting from the VPN server. [BNNGF-61057], [BNNGF-61959]
- Log indexer has been fixed. Multiple improvements and bug fixes were applied. [BNNGF-59658], [BNNGF-63273], [BNNGF-63290], [BNNGF-63253]
- 3G/4G modem status is now displayed in the web interface. [BNNGF-62000]

- When operating in ‘host-mode’ (= WLAN router), clients can now also access the SC without encryption. [BNNGF-61751]
- Execution of custom user scripts is now configurable on the Control Center. [BNNGF-61803], [BNNGF-61792]
- A password change is no longer enforced when the backup file gets restored. [BNNGF-63697]
- Additional IP addresses are now configurable on the WAN interface. [BNNGF-61931], [BNNGF-61930], [BNNGF-62744]
- The web interface has been reworked. Multiple improvements and bug fixes were applied. [BNNGF-62981], [BNNGF-62982], [BNNGF-62982], [BNNGF-62980], [BNNGF-63212], [BNNGF-62987], [BNNGF-63048]
- ZTD no longer fails due to incorrect time settings. [BNNGF-61742]
- Link Selection now points to the correct routing table. [BNNGF-60972]
- A WWAN online probing IP can now be set in the configuration. [BNNGF-61875]
- Rollback no longer gets activated after successful connection to the Control Center. [BNNGF-63647]
- scactl now uses rollback configuration if no fallback is available. [BNNGF-63320]
- When the Wi-Fi SSID name is changed in Access Point mode, the change is now correctly uploaded. [BNNGF-61784]
- All messages sent to the CC now contain a SCA unique box name identifier. [BNNGF-61884]
- Uninitialized variable issue has been fixed in sca-system/src/libscatools/NetHelper.cpp. [BNNGF-63729]
- Configuration is no longer locked after using Reset button. [BNNGF-63789]
- Additional IP addresses can now be entered with correct subnet. [BNNGF-63639], [BNNGF-62815]

What´s New in FSC Version 2.0.7

In addition to numerous stability and performance improvements, v2.0.7 offers the following new features:

- Container can now be reset to factory defaults before update packages are installed. This is done when a "resetcontainer" file is in the container update package.
- An iptables firewall implementation has replaced Shorewall.
- Automatic rollback for faulty configuration. When no connection to the CC can be established after 2 hours of configuration change, a rollback is done to the last-known working configuration.
- DHCP Relay now works on startup. (It no longer needs a manual restart after reboot.)
- Monitoring for 3G/LTE connections.
- UMTS.log has been added to syslog streaming.

What´s New in FSC Version 2.0.6

Local Breakout IP Addresses

- You can now configure up to 10 local breakout IPs in the WAN zone that are accessible from the LAN zone to exclude certain IP addresses from network traffic backhauling. Local breakout IP addresses can be configured to reach the Internet through the WAN or Wi-Fi zone and can be covered by the Link Selection feature.

What´s New in FSC Version 2.0.5.1

- Default network routes are now correctly introduced if primary and secondary uplinks with enabled link selection are present. [BNNGF-57713]

What´s New in FSC Version 2.0.5

Additional LAN Modes

It is now possible to choose from three different LAN modes for the Secure Connector.

- **Switch mode** - Combines all available LAN ports to a network switch group.
- **2 Port Mode** - Combines LAN2 and LAN3 to a network switch group. LAN1 can be configured individually.
- **3 Port Mode** - All available LAN ports can be configured individually.

Passive Link Probing for Link Selection

- It is now possible to configure passive link probing as an additional option of the Link Selection feature. Enabling Passive Probing enables probing of the first configured VPN IP address and disables probing of explicit probing targets. Passive Probing does not support UDP Mode of VPN tunnels.

New WAN Probing Options

- It is now possible to configure additional WAN Probing options via ICMP, DNS, or both.

What´s New in FSC Version 2.0.3

- It is now possible to perform firmware updates via the web user interface. [BNNGF-53742]
- Additional advanced DHCP options are now available on CloudGen Control Centers 7.2.2 and

higher. [BNNGF-53946]
- The DHCP Relay agent now starts correctly when the Secure Connector is booting. [BNNGF-54802]
- The VPN Mode configuration has been removed from the web user interface. [BNNGF-53032]
- The log viewer of the web user interface now works as expected. [BNNGF-50051]
- The Wi-Fi client configuration on the web user interface was consolidated with the available settings via Firewall Admin SC Editor to allow IP address assignment only via DHCP. [BNNGF-55001]
- It is now possible to configure a Control Center so that the LAN IP address of a Secure Connector is reachable via the VPN tunnel. [BNNGF-54024]
- It is now possible to configure the modem of the Secure Connector via the web user interface. [BNNGF-54781]
- The MTU of VPN interfaces of the Access Concentrator and the Secure Connector are consolidated to prevent fragmentation of packets. [BNNGF-48839]
- Secure Connector configuration files can now have a user-defined file name when uploaded to the Secure Connector via USB thumb drives.

What´s New in FSC Version 2.0.1

Wi-Fi and 3G Support

- Certain FSC2 models now support Wi-Fi and 3G. For more information, see Firewall Secure Connectors.

DHCP Relay Support

- All FSC2 models now support DHCP relaying in combination with a CloudGen Firewall Control Center version 7.2.1 or higher.

Other Improvements

- Firewall Secure Connector configuration files are now accepted as <name>*.conf* files. *sca.conf* is no longer required. Please note that after successful activation all configuration files are removed from the mass-storage device on the FSC unit.
- Several stability and performance improvements.