# 8.2.2 Release Notes

https://campus.barracuda.com/doc/96773466/

Before installing the new firmware version:

Do not manually reboot your system at any time while the update is in progress unless otherwise instructed by Barracuda Networks Technical Support. Upgrading can take up to 60 minutes.

**Changelog**

To keep our customers informed, the "Known Issues" list and the release of hotfixes resolving these known issues are now updated regularly. If there are intermediate updates to this release, the corresponding notes will be found in this info box.

- **9.2.2023 – Hotfix 1091** - OpenSSL - For more information, see https://dlportal.barracudanetworks.com/#/packages/5576/openssl-1091-8.2.2-175869125.tgz.

## Important Note for Users Wanting to Upgrade to Firmware Release 8.3.x at a Later Date

If your firewall is currently running firmware 8.2.1, and you plan to upgrade to release 8.3.x at a later date, you should consider switching to firmware 8.3.x now!

Because firmware 8.3.1 has been released after firmware 8.2.2, 8.3.1 does not include fixes contained in 8.2.2.

If you must switch to firmware 8.2.2, you can only upgrade to the upcoming releases 8.3.2 and 9.0.0 respectively.

## IMPORTANT NOTE

The list of solved issues below contains the ticket BNNGF-84038 and now provides a solution that requires special attention:

If you are operating a reverse proxy and traffic is transmitted both for HTTP and HTTPS through

that proxy, the performance might decrease.

As a workaround, and to avoid performance decreases, it is recommended to configure different ports for both protocols.

In the upcoming release(s), the ports will be enforced to be different if you want to transmit both HTTP and HTTPS over the reverse proxy.

## Use the Appropriate Firewall Admin Release

Generally, Barracuda Networks recommends using the latest version of Firewall Admin for a new firmware release.

As of the public availability of this firmware release 8.2.2, Barracuda Networks recommends using at least the Firewall Admin version https://dlportal.barracudanetworks.com/#/packages/5479/FirewallAdmin_8.2.2-62.exe.

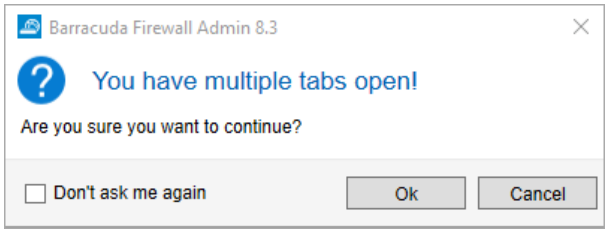
In case of upcoming hotfixes that solve known issues for Barracuda Firewall Admin, you can find the respective notes for the updated version(s) in this info box.

## What's New in Version 8.2.2

Version 8.2.2 is a minor update firmware release.

#### Barracuda Firewall Admin

If multiple tabs are open in Barracuda Firewall Admin and the main window will be closed by clicking the 'X' symbol in the upper right corner of the window, a dialog will be displayed giving the user the choice to cancel the closing of all tabs or to keep Firewall Admin's window open. The option of displaying the dialog window can be turned off via a checkbox.



## What has been Carried On from Version 8.2.1 to 8.2.2

#### HA Auto-Pairing

You can activate the HA auto-pairing feature to turn two separate firewalls into an HA pair with a minimum effort in configuration.

For more information, see HA Auto-Pairing.

#### Consolidated Menu for Importing Certificates

All UI buttons with a context menu for importing certificates with the file ending .cer, .crt, and .pem have been consolidated into a single, common context menu item. The format conversions will be handled automatically in the background by Firewall Admin.

## Improvements Included in Version 8.2.2

#### Appliances

- The LCD now works as expected on the F1000B. [BNNGF-83659]

#### Authentication

- Domain join with SMBv2 now works as expected. [BNNGF-76010]
- SAML authentication metadata is now generated correctly for a managed box. [BNNGF-76521]
- RADIUS no longer gets spammed with authentication requests when C2S/NAC has UDP chosen as transport. [BNNGF-80365]
- The confirmation page is now forwarding as expected. [BNNGF-80885]
- When group caching is enabled, authentication now works as expected. [BNNGF-81127]

#### Barracuda Firewall Admin

- The length of the service name has been increased to 40 characters. [BNNGF-79461]
- Tabs in the ribbon bar now also display the name of the firewall and its associated MIP. [BNNGF-79931]
- When switching from the **FIREWALL > Forwarding Rules** tab to the **Firewall > local** tab, the **Refresh** button no longer vanishes. [BNNGF-79937]
- It is now possible to find, edit, and replace information in the **ConfTemplate Editor**. [BNNGF-79966]
- While a subnode is open and modified in the configuration tree, a cluster migration is not possible. [BNNGF-80277]

- For importing a certificate or a certificate chain, a password query has been implemented that displays a dialog window in the following three cases: 1. When the file to be imported is encrypted. 2. When parsing the file is not possible, e.g., due to faulty file content. 3. When the file to be imported has a different file extension, e.g., 'p12'. [BNNGF-80435]
- If multiple tabs are present in the ribbon bar, clicking on the 'X' symbol of Firewall Admin's window in the upper-right corner causes a dialog window to be displayed that must be confirmed by the user. [BNNGF-80811]
- Limiting traffic in the default shaping tree now works as expected when a PC is located in the US. [BNNGF-81245]
- The list for additional VPN transport networks no longer displays additional GTI networks. [BNNGF-82939]
- Connecting to the SSH now works as expected when connecting to the configuration with a public key and without entering the username into the AltName field. [BNNGF-83119]
- When using IPsec settings for client-to-site configurations, Firewall Admin no longer crashes in certain situations. [BNNGF-83373]

**Barracuda OS**

- The **Model** label on the **CONTROL > Services** page is now displayed as expected. [BNNGF-78300]
- Two boxes as part of an HA pair no longer crash simultaneously in certain situations. [BNNGF-78380]
- The LTE modem is now enabled by default to be used by zero-touch via the mobile network. [BNNGF-79206]
- When SCADA detection is enabled and PLC is accessed via client-to-site VPN, the connection to PLC S7 now works as expected. [BNNGF-79273]
- Routes are now introduced after restarting the VPN service. [BNNGF-79770]
- The DHCP client now introduces the default gateway route as expected. [BNNGF-79948]
- In rare cases, calculations caused blocked sessions that now no longer occur. [BNNGF-80007]
- Application Control for AnyDesk now works as expected. [BNNGF-80329]
- After moving the FTP plugin into the kernel space, a pair of HA firewalls no longer crashes in certain situations. [BNNGF-80493]
- TLS Inspection now works as expected in the HTTP proxy. [BNNGF-80500]
- Host routes with MTU 1500 now work as expected on interfaces with MTU 9000. [BNNGF-80501]
- The firewall no longer crashes in certain situations. [BNNGF-80562]
- The firewall no longer freezes in certain situations. [BNNGF-80576]
- HTTPS sites now load at expected speeds when certificates are validated. [BNNGF-80589]
- VLANs / Interfaces with the name "vlan" do not affect the activation or functionality of the unit. [BNNGF-81075]
- The processing of statistics no longer causes the hard disk to be filled. [BNNGF-81167]
- RIP now works as expected. [BNNGF-81977]
- The server node is now correctly removed from the configuration tree after migrating the old 3-layer service architecture to the new 2-layer one. [BNNGF-82070]
- An update of the Firewall Insight license now works as expected if the license name was previously changed. [BNNGF-82088]

- Security measures have been taken for CVE-2022-0778. [BNNGF-83054]

**Cloud Azure**

- A managed box now connects to an Azure VWAN as expected. [BNNGF-80901]
- Service IPs of additional IPs are now used in an HA pair as expected. [BNNGF-81951]

**Control Center**

- On an 8.2.0 Control Center, the update package for 8.x to 8.2.0 now appears as expected. [BNNGF-77667]
- Control Centers with IPv4 and IPv6 enabled now work as expected after an update. [BNNGF-79934]
- In the Control Center, the SC editor now updates the VPN configuration as expected. [BNNGF-80407]
- After configuration changes, a bogus "defaultbox" is no longer displayed in the CC status map. [BNNGF-81019]

**DHCP**

- **BOOTREPLY** messages are now processed as expected after the DHCP relay service is restarted following a complete configuration update. [BNNGF-81966]

**DNS**

- The BIND system has been updated to version 9.16.x. [BNNGF-74788]
- If multiple DNS services are configured, DNS no longer causes issues with using incorrect source-IP addresses. [BNNGF-78289]
- The DNS system BIND has been updated to version 9.16.27. [BNNGF-83078]

**Firewall**

- The Control Center no longer crashes in certain situations after reporting the error message "skb_warn_bad_offload". [BNNGF-73804]
- The **Firewall Authentication Client** no longer logs out automatically after approximately 30 seconds. [BNNGF-80694]

**HTTP Proxy**

- The HTTP proxy no longer experiences memory leaks in certain situations. [BNNGF-80387]
- The proxy service no longer causes segmentation faults after transforming a box to operate the new 2-layer service architecture (Assigned Services). [BNNGF-83509]
- If you are operating a reverse proxy and traffic is transmitted both for HTTP and HTTPS through that proxy, the performance might decrease.
  As a workaround, and to avoid performance decreases, it is recommended to configure different ports for both protocols. In the upcoming release(s), the ports will be enforced to be different if you want to transmit both HTTP and HTTPS over the reverse proxy. [BNNGF-84038]

**VPN**

- If **HA Tunnel Sync** is enabled in **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN > VPN Settings**, a VPN tunnel now works as expected when an HA-failover is initiated. [BNNGF-54419]
- The VPN status page now correctly displays IKEv2 tunnels. [BNNGF-56468]
- If pre-authentication failed, logging in with a username in the VPN client will display an error message. [BNNGF-67672]
- Client-to-Site connection no longer fails with capital letters in the certificate. [BNNGF-75138]
- Using MSAD + RSAACE for personal licenses no longer causes authentication errors. [BNNGF-76332]
- Using special characters in the **Group Pattern** field of the **Group Policy Condition** no longer causes an issue when logging in. [BNNGF-76804]
- A VPN tunnel with DNS now starts as expected. [BNNGF-79154]
- Client-to-site IPSec connections for Android now work correctly when the used server certificate does not have a subAltName. [BNNGF-80260]
- Downloading the CRL file now works as expected. [BNNGF-80823]
- IKEv2 memory leaks no longer occur when establishing VPN tunnels/transports. [BNNGF-81077]
- Default route and DNS server (IKEv1 C2S with IOS 15.2) now work as expected. [BNNGF-81513]
- Bandwidth probing for SD-WAN now displays the effective throughput between the two endpoints of the connection. [BNNGF-82160]

## Known Issues

- **Azure** – OMS is currently not supported on CC-managed boxes.
- Currently, no RCS information is logged for **Named Networks**. [BNNGF-47097]
- **Barracuda Firewall Admin** – FW Admin 8.x fails to configure DNS 7.x correctly. [BNNGF-77636]
- **Configuration Templates** – FscVpn ConfUnit - Updating management net does not work in 8.2.2 [BNNGF-81328]
- The learn-only mode for OSPF is not working as expected. [BNNGF-65299]
- **Firewall** – Inspecting traffic for QUIC / UDP 443 is currently not supported. [BNNGF-74540]

## Figures

1. dialog_window_multiple_tabs_open.png