7.0.2 Release Notes

https://campus.barracuda.com/doc/71862312/

Barracuda Networks recommends to always install the latest firmware release of the major version to benefit from the latest security and stability improvements.

This firmware version includes a critical security issue resolved by installing Hotfix 834. If Hotfix 825 is already installed use Hotfix 839 instead. For more information, see Hotfix 834 - Security Issue and Hotfix 839 - Security Issue.

Before installing or upgrading to the new firmware version:

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

Changelog

To keep our customers informed, the Known Issues list and the release of hotfixes resolving these known issues are now updated regularly.

- 16.03.2017 – Firmware version 7.0.2 released.
- 24.03.2017 – Added information about the automatic license update daemon.
- 19.10.2017 – Release Hotfix 848 KRACK Attack.

- Back up your configuration.
- The following upgrade path applies – **5.2 > 5.4 > 6.0 > 6.1 (optional) > 6.2 (optional) > 7.0.2**
- Before updating, read and complete the migration instructions.

For more information, see Migrating to 7.0.

As of January 31, 2019, the first-generation ATP cloud services used by default with firmware versions 6.2.x, 7.0.x, 7.1.0, 7.1.1, and 7.2.0 will be discontinued. Firewalls using ATP must switch to the second-generation ATP cloud service, which is known as Barracuda Advanced Threat Protection (BATP).

For more information, see 7.0 Migration Notes.

What´s New in Version 7.0.2

Migrating to a New Hardware Model Wizard

A new wizard now helps you to migrate PAR files created on hardware firewall models either to the next larger model or to a different revision of the same model. The PAR file migration wizard automatically changes default values to fit the new model unless the settings have been changed by the admin. The migration is available for both stand-alone and managed firewalls.

For more information, see Migrating to a New Hardware Model and How to Migrate Managed Hardware Firewalls to a New Model.

NextGen Firewall available in Google Cloud

The F-Series Firewall can be deployed to the Google Cloud Platform to secure and connect your cloud resources. The NextGen Firewall can be deployed either by uploading the disk image available from the Barracuda download portal, or by using the marketplace image in Google Launcher.

For more information, see Google Cloud Deployment.

Integrated Barracuda DSL Modem

This release provides firmware support for upcoming NextGen Firewall F82 DSL model with integrated xDSL modem. Some NextGen Firewall models now feature a built-in DSL modem supporting ADSL and VDSL connections.

For more information, see xDSL WAN Connections and How to Configure an xDSL WAN Connection with an Internal DSL Modem in Bridge Mode.

Automatic License Updates on Stand-Alone Firewalls

New firewalls now continuously check and, if necessary, update their licenses with the newest version available from the Barracuda licensing servers. The Box Activation Daemon is disabled by default for managed firewalls and firewall updated to 7.0.2. If the box activation daemon is disabled, licenses must be downloaded and updated via NextGen Admin for standalone firewalls, or through the Control Center for managed firewalls.

For more information, see Migrating to 7.0.

Improvements Included in Version 7.0.2

NextGen Admin

- Deleting a firewall while it is still referenced by a virtual server now displays an error message. BNNGF-40378
- NextGen Admin automatic session reconnection improvements. BNNGF-43601
- NextGen Admin dashboard stability improvements. BNNGF-42232
- IPv6 ICMP traffic no longer shows the ICMP identifier as the port on the **FIREWALL > Live** and **FIREWALL > History** pages. BNNGF-31417
- The **Max Entries** setting on the **FIREWALL > History** page is now honored immediately without a manual refresh. BNNGF-41383
- NextGen Admin no longer cuts off the Phase 2 lifetimes in the site-to-site IPsec configuration dialog. BNNGF-42321
- NextGen Admin now uses the **Organisation** on the **CC Identity** page as the label for the connection tab. BNNGF-38642
- The refresh tabs icon in NextGen Admin now added the option to reconnect to the session with or without entering the password. BNNGF-37663
- The serial number displayed on the Control Center **Status Map** is now fetched directly from the managed firewall. BNNGF-43819
- On the **Authentication Service > Certificate Validation** page, the **Ignore OCSP** setting is now in **Advanced View**. BNNGF-44776
- Sorting the list of protected IPs on the **FIREWALL > Dynamic > Protected IPs** page now works as expected. BNNGF-42089
- Long network object names are no longer cut off in the connection object **Network Object** drop-down menu. BNNGF-42599
- Updated the icon for the URL Filter policy action **alert**. BNNGF-43320
- **Networks** in the **GTI Editor** are no longer shown in phion notation. BNNGF-41357
- In the TINA VPN tunnel configuration dialog, the drop-down menu for the **Compression** parameter is now displayed correctly. BNNGF-41793
- The throughput of the network interfaces on **CONTROL > Network** is now shown in MBit instead of bps10. BNNGF-42329
- The time stamp for the last successful IPS update is now displayed correctly. BNNGF-42374
- Sorting the application's browser by risk now works as expected. BNNGF-42377
- Sorting the user column in Grouped By User mode on the **FIREWALL > User** page now works as expected. BNNGF-39618
- If the user information is available, usernames are now displayed for firewall connection cache entries on the **FIREWALL > History** page. BNNGF-39617
- For access rules matching on the VPN username, the user is now displayed in the **FIREWALL > Live** and **History** pages as well as in the firewall logs. BNNGF-29581
- The label of the **VPN Clients Downloads** column is now changed to **Description** to match the **Upload** dialog. BNNGF-43206
- Locking CC admins now automatically locks all instances of the user. Locking single instances of a CC admin is no longer possible. BNNGF-42286
- NextGen Admin now shows more informative error messages if the files for the firmware update elements could not be downloaded. BNNGF-44095

- NextGen Admin session reconnect message boxes improvements. BNNGF-42977
- Expiration dates are now also visible for subscription licenses. BNNGF-37049
- The DNS Suffix parameter no longer accepts multiple comma separated values. BNNGF-43488
- Displaying File Content policy information in the Firewall monitor now works as expected. BNNGF-43001
- Favorites can be configured via the left menu in NextGen Admin again. BNNGF-39160
- Entering email addresses in the CC Wizard now works as expected. BNNGF-44288

Barracuda OS

- Firewalls and Control Centers using legacy phion licenses no longer receive IPS patterns. BNNGF-42195
- Updated bind to version 9.9.9-p5 to mitigate security vulnerabilities CVE-2016-8864, CVE-2016-9131, CVE-2016-9147, and CVE-2016-9444. BNNGF-43714
- Resolved a rare case where the authentication service causes a system crash. BNNGF-43285
- It is now possible to use stub zones in combination with the caching DNS server. BNNGF-43470
- It is no longer required to restart the authentication service when configuring DC agent / DC client authentication. BNNGF-41689
- Corrected the portmapping for the Barracuda NextGen Firewall F1000. BNNGF-42285
- **Copy From Default** now restores factory default settings based on the platform and firewall model. BNNGF-41514
- IPsec tunnel states are now correct in the box level SNMP service. BNNGF-40965
- Sensor mappings for the F800 Rev C and F900 Rev B now show correct data for all versions. BNNGF-42408
- Hardware firewalls using flash storage no longer write core files, as these would fill up the limited storage on the firewall. BNNGF-44597
- Migrating managed firewalls using global firewall objects in a repository linked Network configuration node, now works as expected. BNNGF-42841
- It is now possible to configure the threshold of the license expiration warning. BNNGF-42839
- Corrected time zone for Europe/Istanbul. BNNGF-44151
- Using an Explicit CC IP address in Box Properties no longer breaks syslog streaming to the Control Center. BNNGF-34556

Firewall

- Custom block pages no longer cause package flooding when blocking services that reuse the same source and port for multiple destinations. BNNGF-42472
- Memory consumption improvements in the Firewall service request handler. BNNGF-36793
- Handling and matching for user objects containing users in many different groups improved. This no longer causes the access rule to not match. BNNGF-43511
- It is now possible to use numbers in the name of a **Trusted Root Certificate** in the **SSL Interception** configuration. BNNGF-32428
- Firewall loopback traffic on port 9023 is no longer sent out on a different interface. BNNGF-40381
- Block page delivery improvements. BNNGF-41440
- It is now possible to detect Facebook file transfers using Application Control. BNNGF-38975

- Using IPS in **Report Only** mode for IPv6 traffic now works as expected. BNNGF-23520
- Trend Micro AV updates are now detected correctly by Application Control. BNNGF-41169
- Firewall statistics for UDP traffic now work as expected. BNNGF-42153
- **Broad-Multicast** rules no longer use Application Control. BNNGF-29188
- Hostname network objects are now resolved reliably in the Forwarding Firewall ruleset. BNNGF-42694
- The DNS sinkhole can no longer cause the firewall service to crash. BNNGF-4137
- Various firewall service stability improvements. BNNGF-42260
- Fixed an race condition causing the firewall service to crash. BNNGF-41753
- It is now possible to detect the TOR browser 6.5 using Application Control. BNNGF-44075
- Solved deadlock in Firewall service occurring in rare cases in combination with the URL Filter service. BNNGF-42249
- Changing the subnet mask of a network object now works as expected. BNNGF-43207

Distributed Firewall

- Improved resolving hostname network objects in the Distributed Firewall service. BNNGF-41059
- Pattern updates for ranges where all managed firewalls use the distributed firewall service now work as expected. BNNGF-42907

Virus Scanner and ATD

- SMTP users are now exempt from the ATD blacklisting policy. BNNGF-43481
- It is now possible to add exceptions to the virus-scanned MIME types by entering the exempted MIME type with a prepended '!' in the **Scanned MIME Types** on the **Security Policy** page. E.g: !application/mapi-http BNNGF-43070
- ClamAV freshclam fallback update method is now disabled by default. Legacy licensed firewalls must enable freshclam updates manually. BNNGF-42234
- Added option for legacy phion customers to enable **ClamAV Freshclam Fallback** in the **Advanced View** of the **Virus Scanner Settings > Update Handling** page. BNNGF-41289
- It is now possible to log SMTP virus scanning to a dedicated logfile by enabling the option in the **Virus Scanner Advanced Settings** of the **Security Policy** page. BNNGF-41374
- It is no longer possible to manually quarantine mail attachments scanned by ATD to avoid the mail server IP address from being placed in quarantine. BNNGF-39476
- ATD scan first, then deliver web page, now allows both HTTP And HTTPS redirects. BNNGF-42647
- ZIP or RAR files are no longer trickled to avoid errors when redirecting to the scan first, then deliver page. BNNGF-42308
- Files with no content length are now handled correctly by the virus scanner and ATD. BNNGF-43103
- Solved rare issue that caused asp files to be recognized as a PDF file. BNNGF-41755
- Virus Scanner service improvements to fix several issues causing the firewall to lock up. BNNGF-42958
- Retransmissions from the server no longer cause some websites to not load, when virus scanning is enabled. BNNGF-44273

VPN

- The ESP lifetime is now enforced if the CHILD_SA rekeying fails for IPsec IKEv2 VPN tunnels. BNNGF-43137
- Updated libCURL to fix several security vulnerabilities. BNNGF-42747
- It is now possible to enter hostnames as the **Remote Gateway** for IKEv2 IPsec site-to-site tunnels. BNNGF-34681
- Renamed **Server Key** to **Service key** in the client-to-site personal license configuration dialog. BNNGF-42419
- It is now possible to click **Send Changes** without a dummy change when importing client-to-site profiles. BNNGF-42278
- Stability improvements for Site-to-site IKEv2 tunnels to the Azure VPN gateway. BNNGF-37569
- Removing a IKEv2 site-to-site VPN tunnel no longer now also deleted the VPN routes. BNNGF-43153
- Upgraded strongSwan to version 5.4.0 to fix various IKEv2 issues. BNNGF-39850
- it is now possible to establish IKEv2 IPSec tunnels with multiple SPIs. BNNGF-37167
- Solved issue with the IKEv1 daemon causing the VPN service to fail. BNNGF-40960

Control Center

- Improved error handling for file and pattern updates of managed firewalls. BNNGF-42756
- Updating patterns and definitions for a large number of managed firewalls no longer overloads the Control Center. BNNGF-42828
- CC VPN service memory consumption improvements. BNNGF-43392
- CC-Data-Receiver (mdist2) service stability improvements. BNNGF-37964
- Control Center HA sync no longer fails if files are missing while creating the PAR file. BNNGF-23115
- The CC Syslog service now works as expected when UDP is configured as the **Supported Protocol**. BNNGF-44632
- GTI tunnels using Explicit IPs set to 0.0.0.0 now work as expected. BNNGF-42588
- Using link-override for repository linked default boxes in a cluster, now keeps this information when firewall configuration are created from the default box. BNNGF-40444

OSPF/RIP/BGP

- Multipath BGP routes handling improvements. BNNGF-43378
- The split-horizon parameter is now written to the RIP configuration file correctly. BNNGF-42843
- Added missing POINT2MULTIPOINT parameter for OSPF. BNNGF-43927

HTTP Proxy

- Updated HTTP Proxy to fix connection error handling. BNNGF-41846
- Kerberos authentication now works as expected with the HTTP Proxy service. BNNGF-41625
- ATD quarantine now works as expected for the HTTP proxy. BNNGF-41777
- Updated squid to version 3.5.23 to fix security vulnerability SQUID-2016:10-11. BNNGF-43434
- ATD in scan first, then deliver mode now works as expected with the HTTP Proxy service. BNNGF-44551

- Added parameter to allow TLSv1, TLSv1.1 and TLSv1.2 for the HTTP Proxy service in reverse proxy mode. BNNGF-42996

DHCP Server

- The BOOTP lease time is now handled correctly in the DHCP server configuration files. BNNGF-33394

FSC Series

- Attempting to create an invalid S-Series VIP network no longer results in a disconnect. BNNGF-41208
- Adding multiple pool licenses to an Access Concentrator now works as expected. BNNGF-42774,BNNGF-39627

Wi-Fi Service

- Running multiple Wi-Fi services on Wi-Fi-enabled firewall models now works as expected. BNNGF-40173

Public Cloud

- XML parsing errors for IP Forward protection in Azure no longer occur. BNNGF-42117

Report Creator

- In some cases, Report Creator reports filtering for exactly one destination are empty. BNNGF-43852

DNS Service

- Very long TXT DNS record entries are no longer truncated in NextGen Admin. BNNGF-43417
- Creating DNS SRV records containing an underscore character, now works as expected. BNNGF-44193
- Using underscores in DNS Zones now works as expected. BNNGF-44153

SSL VPN

- Certificate expiration dates are now enforced for client certificate authentication. BNNGS-2615
- Web App configurations now allow for longer hostnames up to 270 characters in length. BNNGS-2650
- In rare cases adding group restrictions to Web App resources caused the service to crash. This no longer occurs. BNNGS-2595
- Sending POST requests to web apps that use NTLM single-sign on now works as expected. BNNGS-2608
- It is now possible to upload files larger than 2 GB to Network Places resource. BNNGS-2540
- Upgraded libCURL to version 7.51.0. BNNGS-2613

Issues Resolved by Hotfixes

Hotfix 848 - KRACK Attack

- Security fix for the WPA2 vulnerability.

Current Known Issues

- **Feb 2017: Application Control** – Risk level overrides for applications are not currently honored, and the default risk level is used instead. (BNNGF-24640)
- **Feb 2017: NextGen Firewall F10 Rev A** – It is not currently possible to install a Barracuda NextGen Firewall F10 Rev A via F-Series Install. Install 6.2.2 and upgrade to 7.0.2 instead. (BNNGF-43579)
- **Nov 2016: ART** – It is not currently possible to successfully recover a Barracuda NextGen Firewall F-900 Rev A or F800 Rev B via ART. (BNNGF-43060)
- **Oct 2016: Application Based Routing** – Streaming web applications such as WebEx, GoToMeeting or bit torrent always use the default connection configured in the Application-based provider selection object. (BNNGF-42261)
- **Oct 2016: File Content Policy Filtering** – Configuring a file content policy with multiple filename entries might result in not all configured filenames being blocked. (BNNGF-35982)
- **Sept 2016 IPsec IKEv1 IPv6** – It is not possible to use hostnames as the remote gateway.
- **Sept 2016: IPsec IKEv1 IPv6** – It is not possible to use a dynamic local gateway.
- **Sept 2016: IPsec IKEv2** – It is not possible to establish a VPN tunnel if the active partner uses a dynamic IP address.
- **Sept 2016: IPsec IKEv2** – NAT traversal is not possible when using a dynamic local gateway.
- **Sept 2016: TINA IPv6** – It is not possible to use proxies for TINA VPN tunnels using IPv6.
- **Sept 2016: OSPF** – Enabling OSPF through the **Run OSPF Router** setting currently has no effect on freshly installed 7.0.0 firewalls. Enable OSPF by entering a dummy IP address in the **Summary Range IP/ Mask** list of the **OSPF Area Setup**.
- **Sept 2016: VMware** – Network interfaces using the VMXNET3 driver do not send IPsec keepalive packets unless TX checksumming is disabled for the interface (ethtool -K INTERFACE tx off).
- **Sept 2016: URL Filter** – Firewalls running 6.2.0 or higher that are managed by a Control Center using firmware 6.0.X or 6.1.X must complete a dummy change in the security policy whenever enabling/disabling the URL Filter in the **General Firewall Settings**.
- **Sept 2016: Azure** – After updating a firewall using Azure UDR via Azure Service Manager, the **Deployment Type** might be displayed incorrectly as **y**. This does not affect updating Azure UDR routes.
- **Sept 2016: Public Cloud** – Performing **Copy from Default** of Forwarding Firewall rules currently locks out administrators from the unit and requires a fresh installation of the system. (BNNGF-41514)
- **Sept 2016: IKEv1 IPsec** – When using 0.0.0.0 as a local IKE gateway, you must enable **Use**

IPsec Dynamic IPs and restart the VPN service before a listener on 0.0.0.0 is created.

- **Sept 2016: HTTP Proxy** – Custom block pages do not work for the HTTP Proxy when running on the same NextGen F-Series Firewall as the Firewall service. This issue does not occur when running the HTTP Proxy service on a second NextGen F-Series Firewall behind the NextGen F-Series Firewall running the Firewall service.
- **Sept 2016: VPN Routing** – When a duplicate route to an existing VPN route in the main routing table is announced to the NextGen Firewall F-Series via RIP, OSPF, or BGP, a duplicate routing entry is created and the route that was added last is used.
- **Sept 2016: VPN Routing** – Creating a direct or gateway route with the same metric and destination as a VPN route in the main routing table results in duplicate routes. The route added last is used.
- **Sept 2016: ATD** – Only the first URL in the **Quarantine** tab that leads to a quarantine entry is displayed, even if the user and/or IP address downloaded more than one infected file. This can be dangerous if the first downloaded file is a false-positive.
- **Sept 2016: Terminal Server Agent** – It is not currently possible to assign connections to Windows network shares to the actual user.
- **Aug 2016: IKEv2** – Disabling a site-to-site tunnel on the **VPN > Site-to-Site** page is not possible. (BNNGF-40827)
- **Mar 2016: SSH** – There is no sshd listener for IPv6 management IP addresses. (BNNGF-37403)
- **Feb 2016: Azure Control Center** – On first boot, "fatal" log messages may occur because master.conf is missing. These log messages can be ignored. (BNNGF-36537)
- **Feb 2015: CC Wizard** – The CC Wizard is not currently supported for Control Centers deployed using Barracuda F-Series Install. (BNNGF-28210)
- **Dec 2015: URL Filter** – It is not possible to establish WebEx sessions when the URL Filter is enabled on the matching access rule. (BNNGF-35693)
- **Nov 2015: IKEv2** – Changing a setting for an IKEv2 tunnel disabled in the configuration causes all active IKEv2 tunnels to initiate a re-keying.
- **Nov 2015: IKEv2** – Client certificate authentication for client-to-site IKEv2 IPsec VPNs requires **X509 Certificate** to be enabled in the **VPN Settings**. Enabling this setting requires all VPN group policies to use client certificate authentication.
- **Nov 2015: IKEv2** – After a restart, the **Last Access** and **Last Duration** time displayed for site-to-site IKEv2 IPsec tunnels is not reset.
- **Nov 2015: IKEv2** – Using a hostname or subnet as **Remote Gateway** is not currently possible. (BNNGF-34681,BNNGF-41471)
- **Nov 2015: IKEv2** – Using pre-shared keys with IKEv2 client-to-site VPNs is not possible. (BNNGF-34874)
- **Nov 2015: IKEv2** – Using X509 Subject Policy in a client-to-site **Group VPN Settings** is not possible.
- **Nov 2015: IKEv2** – Connecting to an IKEv2 IPsec client-to-site VPN using iOS or Android devices is not possible. (BNNGF-3487)
- **Nov 2014: Barracuda OS** – **Provider DNS** option for DHCP connections created with the box wizard must be enabled manually. (BNNGF-26880)
- **Oct 2014: SSL VPN** – Favorites are not included in the PAR file. (BNNGS-199)
- **Oct 2014: SSL VPN** – User Attributes do not support UTF-8. (BNNGS-435)

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.