6.2.0 Release Notes

https://campus.barracuda.com/doc/71862723/

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 836. For more information, see Hotfix 836 - Security Issue.

Changelog

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

- 19.10.2017 – Release Hotfix 849 KRACK Attack.

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.

In these Release Notes:

- Back up your configuration.
- The following upgrade path applies: **4.2 > 5.0 > 5.2 > 5.4 > 6.0 > 6.1 (optional) > 6.2**.
- Before updating, read and complete the migration instructions.

For more information, see Migrating to 6.2.

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).

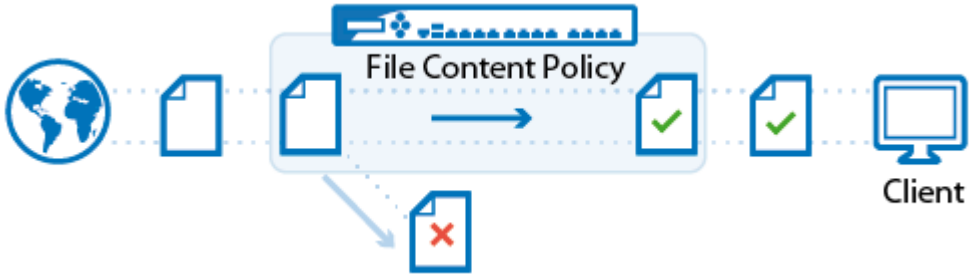
For more information, see 6.2 Migration Notes.

Hotfixes Included with Version 6.2.0

- Hotfix **722**: Boxconfig
- Hotfix **724**: Cumulative Hotfix

What´s New in Version 6.2.0

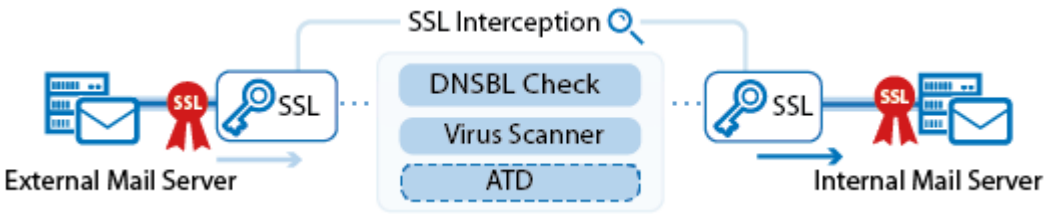
File Content Filtering in the Firewall



The F-Series Firewall offers real-time file content filtering for HTTP, HTTPS, FTP, SMTP, and SMTPS connections. File content policies are configured in policy objects that are added to the application rules. Each policy object contains a list of policy rules defining the action executed for the matching file types. In addition to blocking or allowing file content, you can also assign a QoS band for the duration of the file transfer of the detected file type.

For more information, see File Content Filtering in the Firewall.

Mail Security in the Firewall



The Barracuda NextGen F-Series Firewall enforces mail security in the firewall by transparently scanning incoming and outgoing SMTP and SMTPS connections for malware and checking the reputation of the sender's IP address via a DNS blacklist (DNSBL).

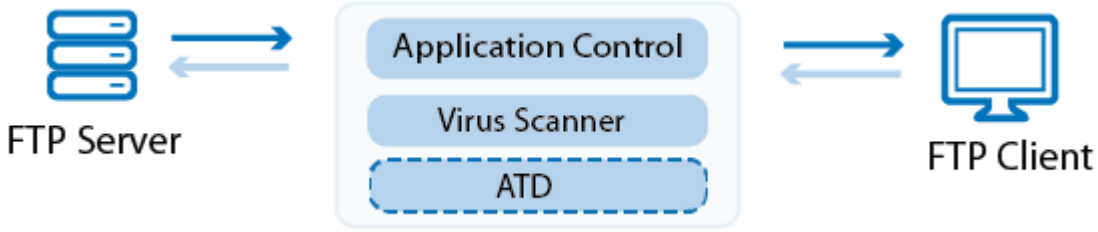
For more information, see Mail Security in the Firewall.

User Agent Filtering in the Firewall

The NextGen Firewall F-Series can filter HTTP and HTTPS traffic based on the user agent string of the browser. The information contained in the user agent string allows you to create policies based on web browser / operating system combinations or to define up to five generic patterns for more specific filters.

For more information, see User Agent Filtering in the Firewall.

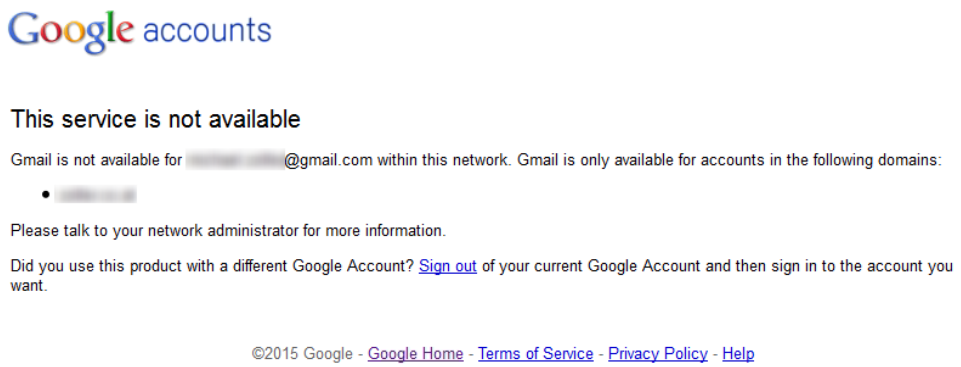
Virus Scanning for FTP in the Firewall



The Barracuda NextGen Firewall F-Series can transparently scan FTP traffic passing through the Forwarding Firewall service for malware. For in-depth scanning of more advanced malware for which there are no virus scanner patterns available, the F-Series Firewall can also scan traffic using Advanced Threat Detection. If malware is detected, the file is discarded and the file transfer is terminated.

For more information, see Virus Scanning and ATP in the Firewall and How to Configure Virus Scanning in the Firewall for FTP Traffic.

Google Accounts Filtering



The Barracuda NextGen F-Series Firewall can filter traffic to Google services based on the domain attached to the G Suite account. This allows you to block access to personal Google accounts and non-whitelisted G Suite domains.

For more information, see How to Configure Google Accounts Filtering in the Firewall.

IPsec IKEv2 Site-to-Site and Client-to-Site VPN

In addition to our proprietary TINA VPN protocol, the Barracuda NextGen Firewall F-Series also supports both IKEv1 and IKEv2 client-to-site and site-to-site IPsec VPN tunnels. This allows you to create connections to IKEv2-only services and devices such as the dynamic Azure VPN Gateway and Windows Phone devices.

For more information, see

- IPsec VPN Tunnels
- Client-to-Site VPN
- How to Configure an IKEv2 IPsec Site-to-Site VPN to a Routed-Based Microsoft Azure VPN Gateway.

Custom Applications to Block Search Terms

For custom search terms not covered by Safe Search, you can configure custom application objects and then block access to them via application rules. Custom search applications are supported for Google, Yahoo, Bing, and YouTube. Custom search applications do not override the **Safe Search** settings of the matching access rule.

For more information, see How to Block Search Terms using a Custom Application Object.

Import Network Objects from CSV File

You can import and update existing static network objects from a CSV file containing the network object data in plain text. Each line of the CSV file contains one IP address or network in CIDR format for the new network object. For network objects containing multiple IP addresses or networks, create a line for each IP address or network. You can import firewall objects in the Forwarding, Host, or Distributed Firewall, and the Global, Range, or Cluster Firewall objects on the NextGen Control Center. If the network object already exists, the user has the option to replace it with the data stored in the CSV file.

For more information, see How to Import Network Objects from a CSV File.

Barracuda NextGen Control Center for Microsoft Azure

The NextGen Control Center for Microsoft Azure is available as a Bring Your Own License (BYOL) image from the Azure Marketplace or as a VHD disk image from the Barracuda Download portal. It includes two preconfigured ranges. By default, the Azure range is configured with a cluster for each Azure datacenter. The Control Center can manage both on-premise hardware and virtual units, as well as public cloud F-Series Firewalls.

For more information, see Getting Started - Control Center for Microsoft Azure.

Azure High Availability UDR Failover Support

Azure User Defined Routing allows you to use the NextGen Firewall F-Series high availability cluster in the frontend subnet as the default gateway for all your VMs running in the backend networks. Using a management certificate, the F-Series Firewall VMs can change the Azure User Defined Routing Table on the fly when the virtual server fails over from one VM to the other. This feature is available for both the Azure Service Manager (ASM) and Azure Resource Manager (ARM).

For more information, see How to Configure Azure Cloud Integration using ASM and How to Configure Azure Route Tables (UDR) in Azure using PowerShell and ASM.

Web Log Streaming

Web Log streaming allows you to send a syslog stream of all HTTP and HTTPS connections to an external device, such as the Barracuda Web Filter, for visualization and reporting purposes. Web Logs can only be streamed, not stored locally. If a different destination device than a Barracuda Web Filter is used, you can customize the log format using streaming templates.

For more information, see How to Configure Web Log Streaming.

NextGen Report Creator 3.0

You can now use the group information on your Microsoft Active Directory server to create custom reports for users and user groups. Reports now also include the option to add threats detected by IPS, Application Control, Virus Scanner or ATD to the report.

For more information, see Barracuda NextGen Report Creator.

New Firewall Monitor

The Firewall Monitor allows you to drill down and visualize real-time information and statistics on your network traffic. The Firewall Monitor d isplays all detected applications, protocols, content, and threats, and provides information on the clients causing the traffic.

For more information, see Monitor Page.

Wi-Fi Client Connections

Barracuda NextGen Firewall F-Series models with built-in Wi-Fi can now connect to wireless networks as Wi-Fi clients.

For more information, see How to Configure Wi-Fi Client Connection.

AWS Enhanced Networking Support

For new deployments, the Barracuda NextGen Firewall F-Series supports AWS Instance Types with enhanced networking support.

For more information, see Public Cloud.

Windows Security Center Health Checks for Policy Service

Policy Server health checks now use information gathered by the Windows Security Service for the health check.

For more information, see Configuring Access Control Service Trustzones.

PFS and ECC Support for TINA Tunnels

Added support for Perfect Forward Secrecy and Elliptic Curve Cryptography for TINA Tunnels.

For more information, see TINA Tunnel Settings.

Telemetry Data

To allow us to continuously update and improve the features frequently used by our customers based on real-world data, the Barracuda NextGen Firewall F-Series sends performance and usage data to the Barracuda telemetry servers. Sending statistics is opt-out for new or freshly installed NextGen Firewalls and opt-in for updated firewalls. The Barracuda NextGen Control Center only sends data collected on box level. No data from the Control Center layer is collected.

For more information, see Telemetry Data.

Improvements Included in Version 6.2.0

Barracuda NextGen Admin

- Removed the option to select the DSA key size when creating box certificates. (BNNGF-31481)
- Added message to **FIREWALL > Live** how many sessions are not displayed if there are more than 10,000 active sessions on the firewall. (BNNGF-33273)
- Importing certificate chains with intermediate certificates now works as expected. (BNNGF-31539)
- Configuration files for the dashboard and Firewall monitor are now written to the correct folder. (BNNGF-33185)
- Interface element now shows the correct port state for ports using a substitute name. (BNNGF-32208)
- Deleting multiple public or SSH keys in the NextGen Admin settings now works as expected. (BNNGF-33108)
- Removed **Simple Config**. (BNNGF-33450)
- NextGen Admin now shows **Update Completed popup** after the firewall has rebooted after an update. (BNNGF-34469)
- Removed **FIREWALL > Trace** page.

Barracuda OS

- Update samba to version 3.6. (BNNGF-32488)
- Changed default hashing algorithm to SHA256. (BNNGF-34124)
- IPFIX log streaming with intermediary reports no longer causes high system load. (BNNGF-34016)
- You can now enter up to two SNMP servers as the destination for event notifications. (BNNGF-22010)
- Added support for /31 bit networks. (BNNGF-34175)
- Changed default settings for Netflow/IPFIX collectors. (BNNGF-34020)
- Added option to import certificates for syslog streaming. (BNNGF-33447)

Firewall

- The DCERPC firewall plugin no longer silently drops packets. (BNNGF-26756)
- Updated list of available DCERPC services. (BNNGF-33718)
- When logging forwarding firewall traffic to a **own logfile**, **log session state change**, data is now written to the correct log file. (BNNGF-33658)
- Ruleset reevaluation no longer terminates active sessions not affected by changes to the ruleset. (BNNGF-32343)
- Moved **Operation TAP** configuration options from **General Firewall Settings** to the **Security Policy** page. (BNNGF-34404)

URL Filter

- Configuration options moved from **General Firewall Settings** to the **Security Policy** page. (BNNGF-34404)

SIP Proxy

- SIP connections using a different connection IP address than the connecting IP address are now handled correctly. (BNNGF-33448)

VPN

- Added support for the following Diffie Hellman groups for IKEv1: 1, 2, 5, 14-18. (BNNGF-32748)
- IPsec ID Type is now configurable for IPsec Site-to-Site VPN tunnels. (BNNGF-32639, BNNGF-17248)

HTTP Proxy

- Counting of files blocked by ATD now works as expected. (BNNGF-34400)

Control Center

- Clarified that **CONFIGURATION > Multi Range > Global Settings > VIP Networks** expects the **network name** and not the first IP address in the VIP network. (BNNGF-28520)

Azure/AWS

- Added **Remote Access** premium licenses to PAYG images in Azure and AWS.

SSL VPN

- Added support for Elliptic Curve Ciphers. (BNNGS-1477)
- Updated the list of supported operating systems for SSL VPN NAC. (BNNGS-1363)
- Renamed **Application Tunneling** to **Applications / Tunnels**, **Service Configuration** to **Applications** and **Generic Application Tunneling** to **Tunnels**. (BNNGS-1410)
- Added note to help to restart service after changing ciphers. (BNNGS-1519)
- Empty Help Text field now passed correctly from NextGen Admin to the Desktop portal.

(BNNGS-1495)
- Invalid host in Application resource no longer causes the service to restart. (BNNGS-1466)
- Restrict to **strong ciphers only** now correctly disables SSLv3 and the **SSL Cipher Spec** text box. (BNNGS-1234)
- Restrict to **strong ciphers only** now set correctly on upgrade if **SSL Cipher Spec** is empty. (BNNGS-1078)
- When prompted, attribute values are not saved; they are now correctly prompted again on subsequent uses. (BNNGS-1211)
- Resolved intermittent problem where client VPN files were available. (BNNGS-1199)
- Resolved issue on upgrade where an incorrect resource could be launched. (BNNGS-989)
- Web forward navigation bar no longer appears incorrectly when using CudaLaunch. (BNNGS-793)

Issues resolved by hotfixes

The following hotfixes have been released for firmware version 6.2.0

Hotfix 849 - KRACK Attack

- Security fix for the WPA2 vulnerability.

Known Issues

6.2.0

- Azure: If the MAC address changes on a managed and unlicensed F-Series Firewall, subsequent attempts to add a license to it fail due to a **MAC address mismatch**.
- File Content Filtering and Virus Scanner: Files transmitted via HTTP chunked encoding are not scanned and file content policies are not applied
- File Content Filtering: Files compressed with **gzip** are detected as **tar** instead of **zip**.
- VMware: Network interfaces using the VMXNET3 driver do not send IPsec keep alive packets unless TX checksumming is disabled for the interface (ethtool -K INTERFACE tx off).
- URL Filter: F-Series 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 every time when enabling/disabling the URL Filter in the **General Firewall Settings**.
- Application Control: In some cases **Ultrasurf** may not be detected.
- Azure: After updating a firewall using Azure UDR via Azure Service Manager, the **Deployment Type** may be displayed incorrectly as **y**. This does not affect updating Azure UDR routes.
- HTTP Proxy: In some cases, SSL Interception does not work in combination with the HTTP Proxy.
- SSL VPN: Some modern browsers such as Chrome and Firefox no longer support Java applets. Instead, use browsers with Java applet support, such as Internet Explorer or Safari.

- User Agent Filtering: The user agent for Microsoft Edge is detected as Google Chrome.
- File Content Policy: If the QoS band for a File Content policy rule is set to **no change**, the QoS column of the entry is empty after a **Send Changes** and **Activate**.
- NextGen Admin: Firewall traces on the **FIREWALL > Trace** page does not work.
- IKEv2: Disabling a site-to-site tunnel on the **VPN > Site-to-Site** page is not possible.
- IKEv2: Changing a setting for a IKEv2 tunnel disabled in the configuration causes all active IKEv2 tunnels to initiate a re-keying.
- 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.
- IKEv2: After a restart the **Last Access** and **Last Duration** time displayed for site-to-site IKEv2 IPsec tunnels is not reset.
- IKEv2: The following actions may result in multiple Security Associations (SA) per tunnel and cause packet loss: Re-initialization of an active site-to-site tunnel, configuration changes to any IKEv1 or IKEv2 site-to-site tunnel, or if the remote VPN gateway is no longer reachable and DPD is used.
- IKEv2: Using a hostname or subnets as **Remote Gateway** is currently not possible.
- IKEv2: Using pre-shared keys with IKEv2 client-to-site VPNs is not possible.
- IKEv2: Using X509 Subject Policy in a client-to-site **Group VPN Settings** is not possible.
- IKEv2: Changing client-to-site minimum and maximum lifetime values has no effect.
- IKEv2: Connecting to an IKEv2 IPsec client-to-site VPN using iOS or Android devices is not possible.
- IKEv2: You can only use MSAD authentication schemes for client-to-site IKEv2 IPsec VPNs.
- Azure Control Center: On first boot "fatal" log messages may occur because master.conf is missing. These log messages can be ignored.
- 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.

Miscellaneous

- Product Tips: Product Tips on the Control Center are enabled, even though the **Enabled** is set to **No** in the **Set Area Config** for **Product Tips** on the **CONTROL > File Update** page. Do a dummy change to set the configuration. This setting also applies to all firewalls managed by the Control Center.
- Application Control: The URL Category **Search Engine** may not be set to **override** when URL Filtering is used in combination with Safe Search.
- 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.
- SSL VPN: Favorites are not included in the PAR file.
- SSL VPN: Text fields do not accept the # character.
- SSL VPN: The mobile navigation bar is missing from servers entered in the **Allowed Hosts**.
- SSL VPN: User Attributes do not support UTF-8.
- SSL VPN: The allowed host filter path must be unique.
- Safe Search: In some cases, YouTube safety mode does not work when logged in with a Google

account.

- Safe Search: If Safe Search is enabled, it is not possible to log into YouTube when cookies are disabled.
- Safe Search: Safe Search is not enforced by Bing when using HTTP.
- VPN Routing: When a duplicate route to an already 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.
- 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.
- HTTP Proxy: **Custom Cipher String** and **Allow SSLv3** settings only apply to reverse proxy configurations.
- CC Wizard: The CC Wizard is currently not supported for Control Centers deployed using Barracuda F-Series Install.
- 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.
- Firewall: It is not possible to join a **join.me** session if SSL Interception and Virus Scanning is enabled in the matching access rule.
- Firewall: Using SSL Interception in combination with URL Filtering and category exemptions may result in degraded performance.
- Barracuda NextGen Admin: SPoE does not work if an IPv6 virtual server IP address is used.
- Barracuda OS: **Provider DNS** option for DHCP connections created with the box wizard must be enabled manually.
- Terminal Server Agent: It is not currently possible to assign connections to Windows networks shares to the actual user.
- Firmware Update: Log messages similar to `WARNING: /lib/modules/2.6.38.7-9ph5.4.3.06.x86_64/kernel/drivers/net/wireless/zd1211rw/zd1211rw.ko needs unknown symbol ieee80211_free_hw` may appear while updating, but can be ignored.
- **Attention**: Amazon AWS/Microsoft Azure: Performing **Copy from Default** of Forwarding Firewall rules currently locks out administrators from the unit and requires a fresh installation of the system.
- Application Control and Virus Scanning: Data Trickling is only done while the file is downloaded, but not during the virus scan. This may result in browser timeouts while downloading very large files.
- Application Control and Virus Scanning: If the Content-Length field in HTTP headers is missing or invalid, the **Large File Policy** may be ignored.
- Application Control and Virus Scanning: In very rare cases, if the SSL Interception process is not running, but the option **Action if Virus Scanner is unavailable** is set to **Fail Close**, a small amount of traffic may already have passed through the firewall.
- Application Control and Virus Scanning: In rare cases, Google Play updates are sometimes delivered as partial updates. These partial updates cannot be extracted and are blocked by the virus scanning engine. The engine reports **The archive couldn't be scanned completely**. Either create a dedicated firewall rule that does not scan Google Play traffic, or set **Block on Other Error** in **Avira Archive Scanning** to **No.**
- High Availability: IPv6 network sessions might not be established correctly after an HA failover.

- Barracuda OS: Restoring units in default configuration with par files created on a Control Center may result in a corrupt virtual server. Instead, copy the par file to *opt/phion/update/box.par* and reboot the unit.
- VPN: Rekeying does not currently work for IPsec Xauth VPN connections. The VPN tunnel terminates after the configured rekeying time and needs to be re-initiated.

Figures

1. file_content_pol.png
2. av_mail_traffic.png
3. user_agent_pol.png
4. av_ftp_traffic.png
5. Google_accounts_04.png
6. ipsec_ikev2_tn.png