7.2.0 EA1 Release Notes

https://campus.barracuda.com/doc/73723948/

Early Release

EA firmware is available to early adopters who wish to test the latest features from Barracuda Networks, or who have a specific need for early access to a new feature or fix that would be beneficial to your environment.

The 7.2.0 EA1 release will not be displayed in the dashboard element of NextGen Admin and will not be listed in the Control Center as a firmware update.

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.

- 2017-12-19 – Firmware version 7.2.0 EA1 released.
- 2018-05-15 – Hotfix 876 - Fixes the security vulnerability CVE-2018-10115 in 7zip.
- 2018-11-21 – **Hotfix 889** - Virus Scanner (CloudGen Firewall) – By installing this hotfix, the Avira scanning engine will be updated to version 4 and update virus definitions even after September 30th 2019. For more information, see Hotfix 889.

Before You Begin

- Back up your configuration.
- The following upgrade path applies – **5.2 > 5.4 > 6.0 > 6.1 (optional) > 6.2 (optional) > 7.0 (optional) > 7.1 (optional) > 7.2**
- Before updating, read and complete the migration instructions.

For more information and a list of supported NextGen Firewall models, see 7.2.0 EA1 Migration Notes.

First-Generation ATP to Second-Generation Barracuda ATP Cloud Migration

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

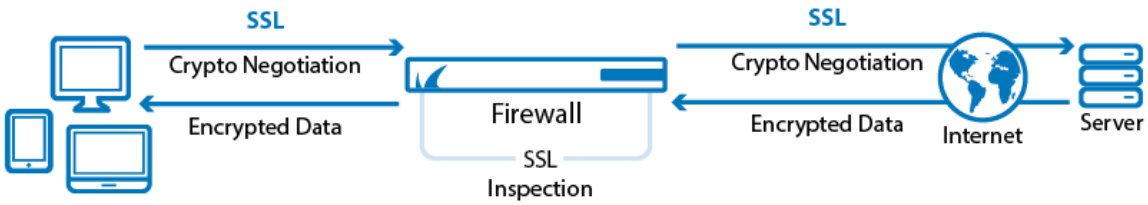
switch to the second-generation ATP cloud service, which is known as Barracuda Advanced Threat Protection (BATP).

For more information, see 7.2.0 EA1 Migration Notes.

What´s New in Version 7.2.0 EA1

SSL Inspection Policies

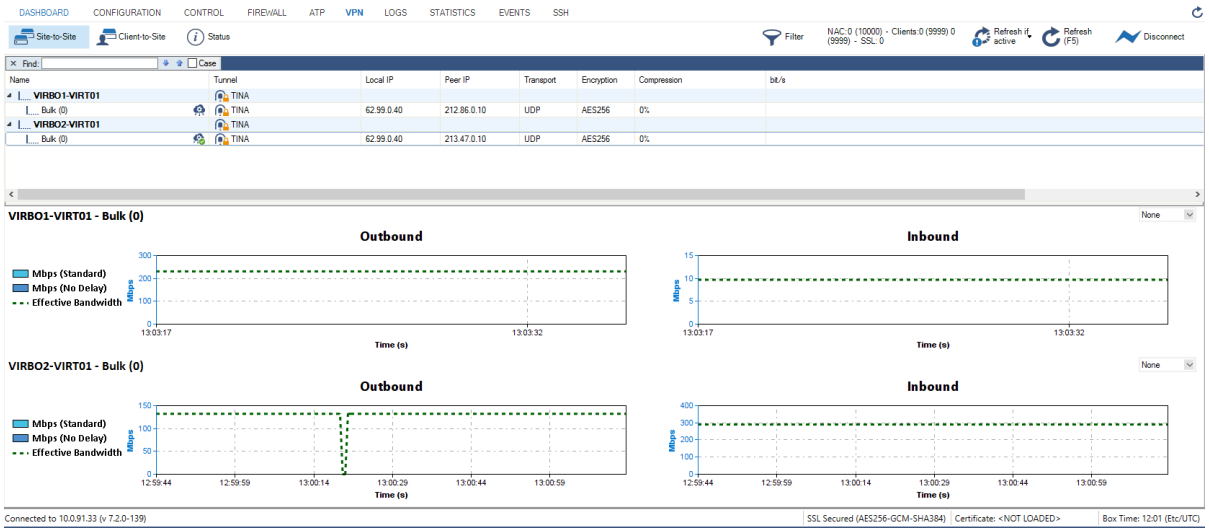
With SSL Inspection Policies you can centrally enforce and manage certain SSL/TLS standards by blocking outdated/insecure ciphers for outbound and inbound connections. For outbound SSL Inspection, the firewall can also handle SSL validation errors, depending on the SSL error policy assigned to the matching access rule of the SSL/TLS session. SSL Inspection is supported for Pass, Map, and Dst NAT access rules. Not supported are SSL connections that require client certificate authentication.



For more information, see SSL Inspection in the Firewall .

VPN Tab Traffic Intelligence Improvement

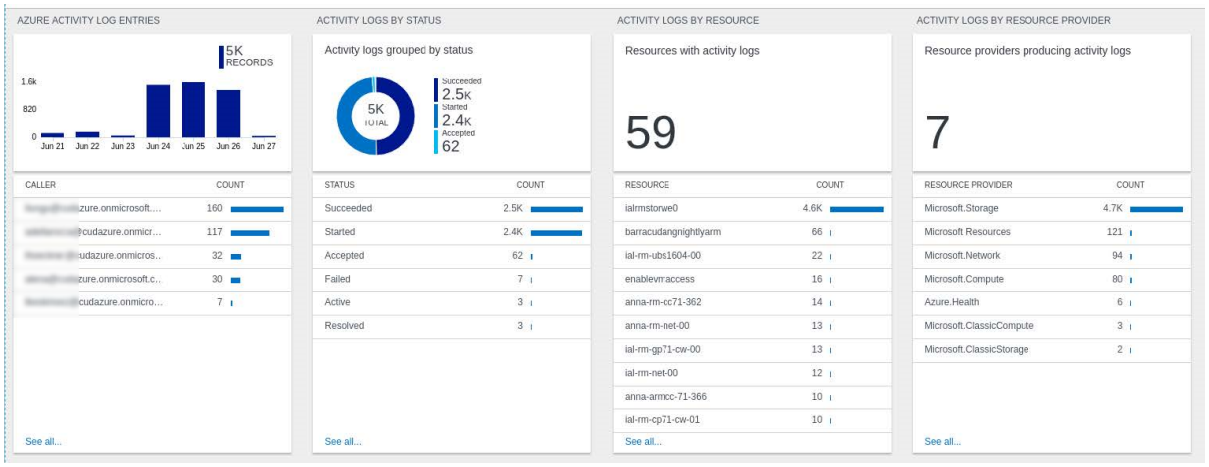
VPN tunnels using the TINA protocol now provide an option to monitor bandwidth and latency for two TINA transports simultaneously.



For more information, see VPN Tab .

Log Streaming and Metrics to Microsoft OMS Workspaces

Streaming of log data and custom metrics from a NextGen Firewall to Microsoft OMS in Azure is now provided.



For more information, see How to Configure Azure OMS Log Streaming .

Volume-Based PAYG Image Available for AWS

A new AWS image is now available that includes a built-in PAYG license and reports consumed volume in MB/hour via an API provided by AWS.

For more information, see How to Create an IAM Role for an F-Series Firewall in AWS , Public Cloud Licensing Types and How to Deploy a Volume-Based (Metered) PAYG CloudGen Firewall image in AWS .

Web Interface

The web-based user interface now also allows administrators to configure TINA VPN tunnels. In addition, the web-based user interface is now also available on CloudGen Firewalls deployed in public clouds.

Hourly PAYG Images for Google Cloud

PAYG is now supported for Google Cloud.

For more information, see Public Cloud .

NextGen Control Center in Google Cloud

The NextGen Control Center is now available for Google Cloud as a Bring Your Own License image.

For more information, see Getting Started - Control Center for Public Cloud .

Cloud Information Element for Google Cloud

NextGen Admin now provides an information element for Google Cloud to be displayed in the dashboard.

Barracuda Reporting Server Integration

Streaming of log data to the Barracuda Reporting Server is now supported via syslog streaming.

For more information, see Barracuda Reporting Server (BRS) Integration .

Named Networks for IPv6

It is now possible to create Named Networks for IPv6 networks.

For more information, see Named Networks.

REST API Improvements

REST API documentation is now available in a separate section. APIs have been added for Control Center, license activation, and modification of network objects. It is now possible to add and remove entries to/from network objects and to add and remove IP addresses to/from custom external objects.

For more information, see https://campus.barracuda.com/product/nextgenfirewallf/api

POP3 / POP3S Virus Scanning

For clients behind the firewall, it is now possible to scan mail traffic to SMTP and from POP3 servers in the Internet using the Virus Scanner and optional SSL Inspection.

For more information, see How to Configure Virus Scanning in the Firewall for Outbound SMTP and POP3 Traffic .

Explicit Authentication Scheme in Username for Client-to-Site VPN Connections

VPN users can now use an authentication scheme that is appended to the username , e.g., @msad. The authentication scheme (e.g., @msad) with the prepended username (e.g., user1@domain.com) is used with the default authentication scheme acting as a fallback if the authentication scheme name is not present on the firewall. E.g., user1@msad1 or user2@domain.com@msad.

For more information, see How to Configure a Client-to-Site VPN Group Policy .

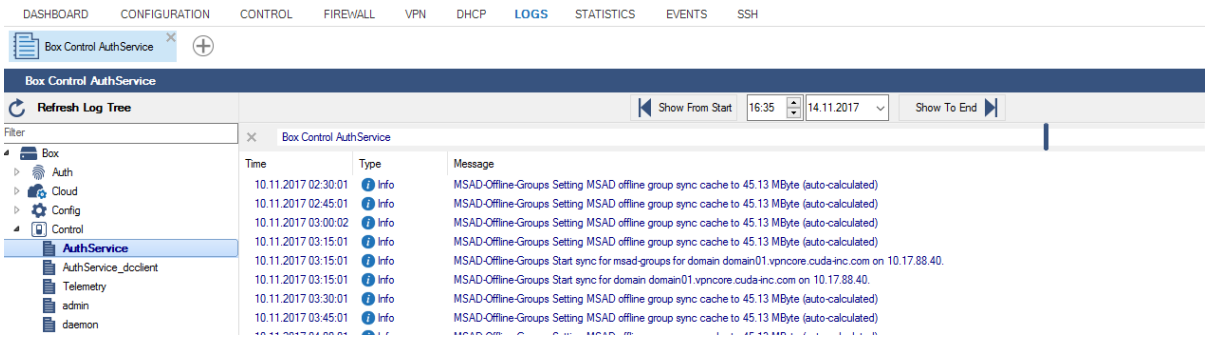
Generic Network Objects

You can now use network objects to reference networks, IPv4 and IPv6 addresses, hostnames, geolocation objects, MAC addresses, or interfaces when you create access rules.

For more information, see Network Objects .

Log Viewer

Log Viewer now displays log files in a new format.



For more information, see LOGS Tab .

SSL VPN Improvements: Single Sign-On and New Attributes for RDP Native App

The native SSL VPN app of the type RDP now also supports single sign-on for improved usability. In addition, it now also supports advanced RDP options for logon settings and connections, display settings (such as multi-screen support), local device and audio support, and connection performance settings.

For more information, see How to Configure SSL VPN Native App for RDP .

Group-Based Management for CC Admin

It is now possible to map Control Center Admins to dedicated Active Directory user groups to conflgure group-based access for Control Center administrators.

For more information, see How to Map Admins From User Groups of External Authentication Schemes .

Improvements Included in Version 7.2.0 EA1

Barracuda NextGen Admin

- NextGen Admin only supports netmasks in CIDR notation in version 7.1 or higher. [BNNGF-40029]
- Auto Refresh on larger Control Centers is now working as expected. [BNNGF-40325]
- Disabling an IPsec IKEv2 tunnel via NextGen Admin now works as expected. [BNNGF-40827]
- Opening the appid status DB via **FIREWALL > Monitor** now correctly displays content older than 7 days. [BNNGF-46908]
- When connecting to a NextGen Firewall with an old version of NextGen Admin, a warning is displayed. [BNNGF-47333]
- Filtering IPv6 addresses containing zero-blocks now works as expected. [BNNGF-47358]
- In case a redirection target list reference is selected in a firewall rule, the **fallback** and **cycle**

combo element is disabled. [BNNGF-48185]
- License tokens now may be entered case insensitive. [BNNGF-49166]
- Up/Lifetime information for VPN tunnels is now displayed correctly. [BNNGF-49261]
- The entry **Toggle Trace** in the popup menu of the Firewall Live View is no longer available. [BNNGF-49574]
- In the **Virtual IP** column of the **VPN > Client-to-Site** table, virtual IPs are now displayed correctly when accessing a box running 7.0.3 from NextGen Admin 7.1.1 [BNNGF-50094]
- For IPsec tunnels, the option **Encaps. Mode Auto Detect** has been renamed to **NAT-T Autodetect**. [BNNGF-50158]
- Firewall Monitor in NextGen Admin now correctly evaluates time information. [BNNGF-50449]

Barracuda OS

- Events for expiring Energize Update licenses are now created as expected. [BNNGF-41720]
- Contacting license update servers through a proxy network now works as expected. [BNNGF-45037]
- F800 Rev. B models with module M801 no longer experience port flapping with higher load. [BNNGF-46304]
- Logging into the firewall via SSH now does not display error messages any longer if no ECDSA key has been configured. [BNNGF-47059]
- DSL now works as expected after an import of a PAR file. [BNNGF-47907]
- VLAN references are no longer displayed after the deletion of the VLAN. [BNNGF-48054]
- In demo mode, the firewall no longer accepts the hardcoded password ngf1r3wall if the administrator changed the default password. [BNNGF-48469]
- Virtual (KVM/GCP) appliances no longer drop packets exeeding the network interface's MTU. [BNNGF-48521]
- The state of the fan is now displayed correctly in the web interface. [BNNGF-48634]
- The NextGen Firewall now creates correct events on boxes when external admins authenticate without a password on the Control Center. [BNNGF-48738]
- For cloud boxes with the web interface enabled, the landing page is no longer displayed. [BNNGF-48851]
- Soft Activation no longer causes a network interruption. [BNNGF-48862]
- Interface names are now mapped correctly from the Defaults file for port names. [BNNGF-49478]
- Closing connections to the configlog database no longer forces users to restart the rangeconf service multiple times a week. [BNNGF-49488]
- After logging into the web interface, open transactions will no longer be existent that may cause unexpected problems. [BNNGF-49617]
- Firewall stability improvements. [BNNGF-49639]
- Auto-created source-based routing now works as expected. [BNNGF-49726]
- The threshold for lower fan speeds has been adjusted to accept cooler ambient temperatures. [BNNGF-49795]
- Multiple SMTP and FTP protocol handling improvements. [BNNGF-49866]
- On a F183R, start of bridging no longer causes the box to freeze. [BNNGF-49987]
- FTP plugin now works with SynFlood Protection both for inbound and outbound connections. [BNNGF-50047]

- Validating licenses for long license names with long box names in a long cluster name no longer fails. [BNNGF-50253]

Control Center

- In the GTI Editor, settings for **Phase 1 Mode** for an IPsec tunnel are now written correctly to the corresponding configuration file. [BNNGF-43874]
- Status colors in the Control Center status map are displayed correctly if an AV license is still valid and less than 90 days. [BNNGF-45530]
- IPv6 addresses are now shown correctly in the GTI Editor. [BNNGF-47295]
- If the serial gets changed on a virtual firewall, the activation daemon now downloads new licenses. [BNNGF-47608]
- GTI configurations for IPsec tunnels now work as expected. [BNNGF-48342]
- Firmware update view is now displayed correctly on a Control Center and no longer causes an error message. [BNNGF-50102]
- Importing a 7.0 PAR file to a 7.1 Control Center no longer triggers a migration. [BNNGF-50137]

DHCP

- DHCP Relay V6 now sends DHCP reply packets as expected. [BNNGF-41604]

DNS

- Adding new PTR entries to the forward lookup zone now works as expected if both the forward AND reverse lookup zone is locked before the change. [BNNGF-46055]

Firewall

- Send Changes/Activate for global firewall objects now works as expected on the Control Center. [BNNGF-38201]
- ICMP policies are now copied together with a related access rule. [BNNGF-48046]
- Multiple stability improvements for the URL Filter service. [BNNGF-48972]
- Interfaces for local traffic are now reported correctly. [BNNGF-48975]
- FTP sessions are now handled correctly and no longer cause different errors. [BNNGF-48996], [BNNGF-49304], [BNNGF-49507]
- The trans7 process no longer produces a segmentation fault in certain situations. [BNNGF-49135]
- The security issue to protect against the WPA2 vulnerability (KRACK attack) has been resolved. [BNNGF-49766]
- The firewall now delivers mails correctly to a client after SMTP mail scanning is finished. [BNNGF-49850]
- **Generic IPv4 Network Objects** have been replaced by **Generic Network Objects** that now also support IPv6 addresses. [BNNGF-50091]
- Client-to-site access rules no longer enable site-to-site tunnels. [BNNGF-50132]

HTTP Proxy

- The reverse proxy now delivers root certificates only once per request. [BNNGF-46029]

Public Cloud

- The web interface is now disabled for autoscaling boxes. [BNNGF-47877]
- In the cloud, provisioning now successfully finishes even if the creation of datacenter network objects fails. [BNNGF-49455]
- The web interface is now disabled for deployment of complex templates with user data. [BNNGF-49614]

REST API

- On a Control Center, REST API post requests no longer cause error 500 if RCS with forced message is enabled. [BNNGF-48475]
- The REST API no longer listens on the management IP per default. [BNNGF-48407]
- The REST firewall plugin for /live and /history endpoints now works as expected. [BNNGF-49656]

SSL VPN

- SSL VPN user attributes no longer show unsupported formats. [BNNGF-49749]

Virus Scanner and ATP

- The setting **Block Encrypted Archives** now works as expected. [BNNGF-48082]
- Configuring the RAM cache for the Virus Scanner no longer causes it to crash. [BNNGF-49323]
- Setting the **Max. Archive size** in the advanced ATP options is limited to the maximum value of 2047 and no longer causes the Virus Scanner to crash. [BNNGF-49413]
- Scanning emails with ClamAV now works as expected. [BNNGF-50194]
- Processing and scanning mails now works as expected after an install of hotfix 852. [BNNGF-50609]

VPN

- One-time passwords now work as expected when using Barracuda license files. [BNNGF-48249]
- VPN routing in combination with BGP, TINA, and IPsec using main routing tables now works as expected. [BNNGF-49698]

Current Known Issues - General

- **Firewall** – Pasting firewall rules that are using SSL Inspection Policies can cause problems if the target firewall ruleset runs with feature level < 7.2. [BNNGF-53952]
- **Firewall** – Copying access rules with enabled SSL Inspection from firewalls running firmware version 7.2.x to firewalls running firmware version 7.1.0 - 7.1.3 can have negative impact on SSL Inspection on the destination system.
- **AWS-Cloud** – Deploying AWS Auto Scaling clusters in the us-east-1 region currently fails to create a S3 bucket automatically. Create the bucket manually instead.

- **Backup/Restore (VPN)** – Restoring a backup does not restore the correct custom policy value for IPsec tunnels. [BNNGF-50652]
- **Backup/Restore (Dynamic interface)** – Restoring a backup does not restore any values for **Dynamic DNS** in **Network > IPConfiguration > Dynamic Interface Configuration**. [BNNGF-50668]
- **Certificate Store** – When referencing certificates in the **Certificate Store** from services like **SSL Inspection**, the reference counter in the **Ref By** column still shows 0. [BNNGF-50666]
- **Mail** - In **Live** and **History** view, the plain text version for POP3 and SMTP are displayed as encrypted and SMTPS and POP3S are displayed as generic. [BNNGF-50878]
- **Mail Security** - Retrieving messages POP3 may result in the first character of the mail body to be missing. [BNNGF-50969]
- **Network** – Transferring data over VLAN interfaces configured on the switch port of NextGen Firewall F180a or F280b fails due to being unable to change the MTU size. [BNNGF-46289]
- **Network** – OSPFv3 is currently not working as expected.
- **NextGen Admin** – On 7.2.0 boxes that are being configured with NG Admin 7.2.1, the SSL Inspection root certificate will not be displayed.
- **NextGen Admin** – Copy and paste of an access rule with explicit Named Network does not copy the Named Network structure. [BNNGF-48588]
- **NextGen Admin** – When connecting with NextGen Admin 7.2.x to a Control Center 7.2.x, the **Open Box Firewall** icon is not displayed for a firewall in the **Status Map** window. [BNNGF-50198]
- **URL-Filtering** – The mechanism for overriding URL categories does not work as expected. [BNNGF-50948]
- **Virus Scanner** - The POP3 protocol currently only works on port 110. [BNNGF-50767]
- **VPN** – When adding a TINA tunnel to **CONFIGURATION > Configuration Tree > Box > Virtual Server > your virtual server > Assigned Services > VPN > Site to site-VPN**, **Local Networks** and **Remote Networks** are not inserted into network objects. [BNNGF-50637]

Current Known Issues Related to the web interface for Cloud

- **Azure Cloud** – In Azure, after switching from NextGen Admin to the web interface, the connection can become very slow or time out. [BNNGF-49960]
- **Azure Cloud** – Resetting the password or an SSH key does not work when the web interface is activated. [BNNGF-50299]
- **Backup/Restore** – For cloud instances, backup and restore does not work except for the VFC8 model with BYOL.
- **SSL VPN** – SSL VPN on public cloud instances is currently not supported.
- **BRS** – Barracuda Reporting Server intergration requires the hostname to be of form `*.brs.cudasvc.com`, where * is the placeholder for a subdomain of your choice.

Figures

1. ssl_inspection.png
2. vpn_s2s1.png
3. oms.png
4. aws_report_traffic.png
5. log_03.png