7.1.0 EA Release Notes

https://campus.barracuda.com/doc/71862306/

This firmware version is affected by a critical security issue resolved by installing Hotfix 835. For more information, see Hotfix 835 - Security Issue.

Barracuda NextGen Firewall 7.1.0 is an Early Availability (EA) version that is currently only available for the following 64bit Barracuda NextGen Firewall models:

- **Hardware Systems** – F18 Rev A, F80 Rev A, F82 Rev A, F180 Rev A, F183 Rev A, F280 Rev A/B, F380 Rev A , F400 Rev A/B, F600 Rev A/B/C , F800 Rev A/B/C, F900 Rev A, F1000 Rev A, C400, C610
- **Virtual Systems** – VF10, VF25, VF50, VF100, VF250, VF500, VF1000, VF2000, VF4000, VF8000, VC400, VC610, VC820
- **Public Cloud** – AWS, Azure, Google Cloud

Support for older appliance models with 32-bit CPUs will be made available with firmware version 7.1.1.

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.

- 2017-06-29 – Firmware version 7.1.0 released.
- 2017-07-04 – Added VLAN, licensing and Google Cloud known issues
- 2017-07-24 – Added known issues for Barracuda DSL and Named Networks
- 2017-08-02 – Added known issue for the Firewall service
- 2017-10-19 – Release Hotfix 847 KRACK Attack.
- 2018-11-21 – **Hotfix 890** - 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 890.

- Back up your configuration.
- The following upgrade path applies – **5.2 > 5.4 > 6.0 > 6.1 (optional) > 6.2 (optional) > 7.0**. **(optional) > 7.1.0**
- Before updating, read and complete the migration instructions.

For more information and a list of supported NextGen Firewall models, see 7.1.0 EA Migration Notes.

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 7.1.0 EA Migration Notes.

What´s New in Version 7.1.0

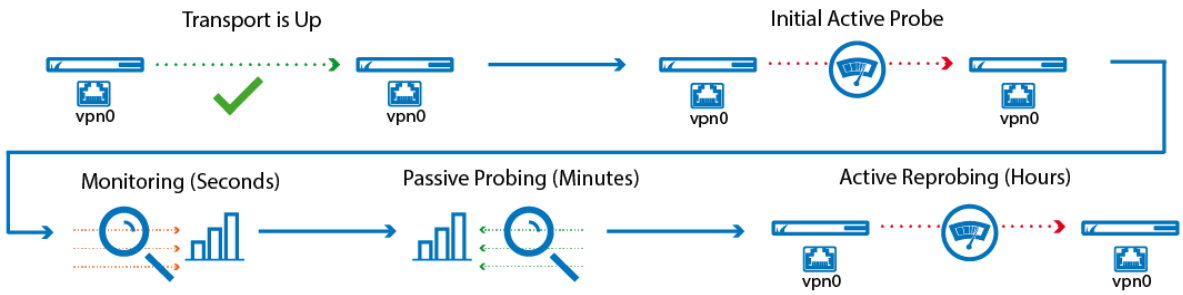
Traffic Intelligence SD-WAN Features

SD-WAN is a technology deployed at the edge of the network to connect remote, on-premises, and cloud networks easily and cost effectively to form a Wide Area Network (WAN). SD-WAN provides better application availability by reducing or even eliminating the need for expensive MPLS lines by partially or completely replacing them with multiple cheaper broadband Internet connections. The SD-WAN Traffic Intelligence features enable the NextGen Firewall F to utilize multiple uplinks for encrypted WAN communication and to apply traffic prioritization, compression, and optimization policies. Routing decisions based on the continuously monitored performance of each WAN connection ensures that the traffic is always using the optimal transport based on your business requirements, thereby eliminating the need for manual routing decisions. The following Traffic Intelligence SD-WAN features are available:

- Dynamic Bandwidth and Latency Detection
- Performance-Based Transport Selection
- Adaptive Bandwidth Protection
- Adaptive Session Balancing

For more information, see Traffic Intelligence.

Dynamic Bandwidth and Latency Detection for Traffic Intelligence



Traffic Intelligence has been enhanced by several new features based on Dynamic Bandwidth and Latency Detection. This allows the firewall to determine the actual bandwidth for UDP transports available for a VPN transport through monitoring, active probing, and passive probing.

For more information, see Traffic Intelligence.

Performance-Based Transport Selection for Traffic Intelligence

Performance-Based Transport Selection selects the optimal transport based on the policy selected in the TI settings of the custom connection object. The VPN transport can be selected to optimize for latency, inbound, outbound, or combined bandwidth.

For more information, see Traffic Intelligence and How to Configure Performance-Based Transport Selection for VPN Tunnels with Traffic Intelligence.

Adaptive Bandwidth Protection for Traffic Intelligence

Adaptive Bandwidth Protection ensures that traffic in the NoDelay (VoIP) QoS band is always prioritized over standard traffic. The firewall uses the link quality metrics gathered by Dynamic Bandwidth and Latency Detection to adjust traffic shaping to always fully utilize the available bandwidth. It is recommended to combine Adaptive Balancing on the VPN transport with consolidated shaping in order to shape the VPN traffic in a two-step process with Adaptive Shaping on the VPN transport and Consolidated Shaping on the VPN traffic a whole. Adaptive Shaping uses a simplified internal shaping tree that reserves 30% for NoDelay traffic and 70% for standard traffic.

For more information, see Traffic Intelligence and How to Configure Adaptive Bandwidth Protection for VPN Tunnels with Traffic Intelligence.

Adaptive Session Balancing for Traffic Intelligence

Adaptive Session Balancing distributes VPN traffic over multiple transports and uses link-quality metrics collected by Dynamic Bandwidth and Latency Detection for both the initial balancing and to rebalance sessions with a lifetime of over 5 seconds.

For more information, see Traffic Intelligence and How to Configure Session Balancing for VPN Tunnels

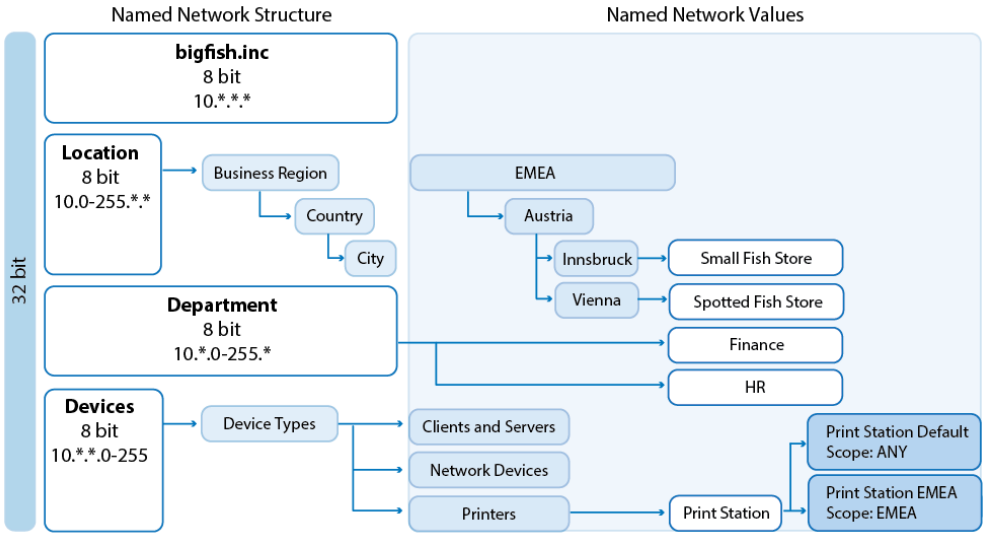
with Traffic Intelligence.

Traffic Duplication for Traffic Intelligence

Traffic duplication copies packets and simultaneously sends them through the selected primary and secondary transports. Both traffic streams are combined again at the other end of the VPN tunnel. Use Traffic Duplication for applications requiring instant failover without a single dropped packet in case a VPN transport goes down. Since traffic is duplicated, both transports must have the same bandwidth and latency.

For more information, see Traffic Intelligence and How to Configure Traffic Duplication for VPN Tunnels with Traffic Intelligence.

Named Networks



Named Networks provide firewalls with structured network information that usually correlates with the company structure while preserving its human-readable names for users. The usage of Named Networks makes the most sense when they are used in the Global, Range, or Cluster Firewall object in the NextGen Control Center. Named Networks can be used solely for firewall ruleset evaluation, or for both ruleset evaluation and visualization.

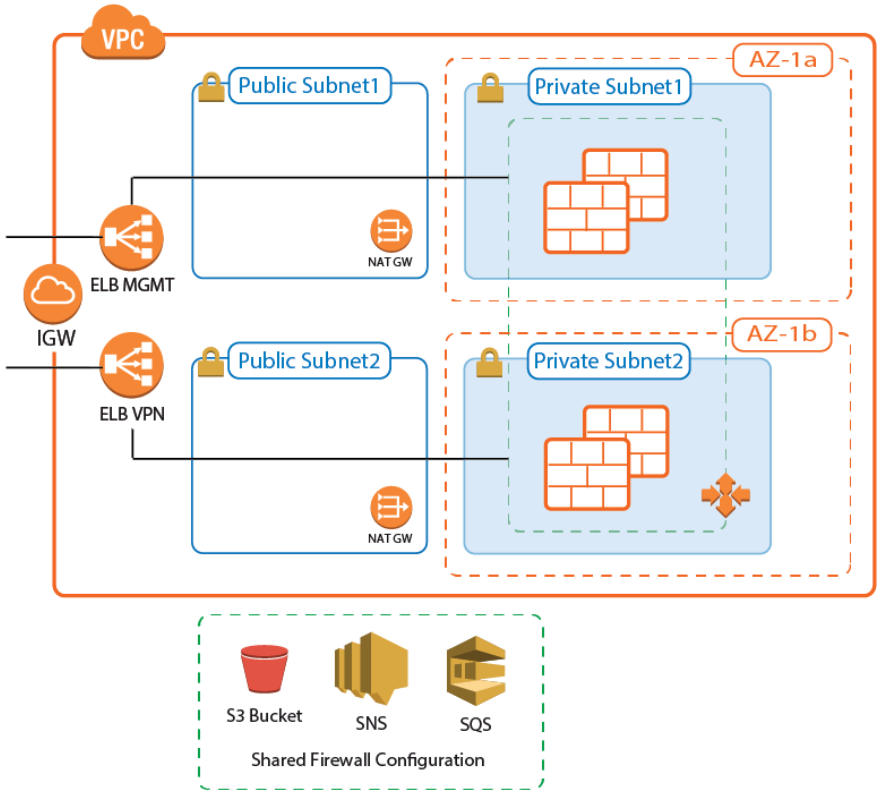
For more information, see Named Networks.

Wildcard Network Objects

Wildcard network objects are network objects that include a network mask containing information regarding which parts of the IP address is to be evaluated. Wildcard network objects can be used to describe IP addresses that cannot be covered by network objects using subnets masks.

For more information, see How to Create Wildcard Network Objects.

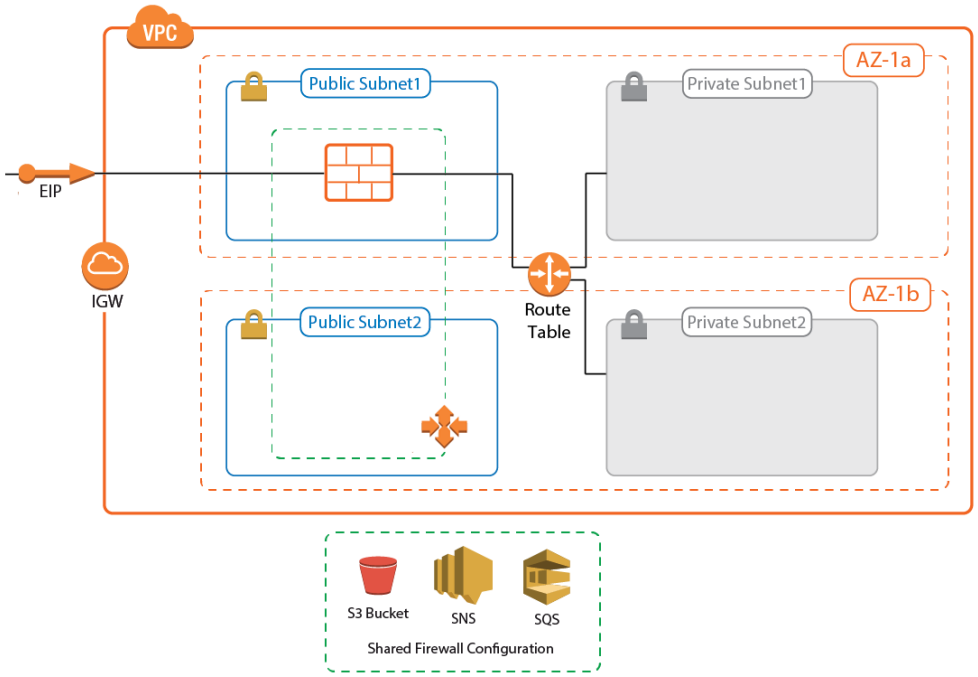
NextGen Firewall Auto Scaling Cluster in AWS



A NextGen Firewall Auto Scaling Cluster scales with demand to create a cost-effective, robust solution for securing and connecting to highly dynamic or cyclical applications running in AWS. The firewall cluster is tightly integrated with AWS services and APIs and can be deployed either to integrate with existing resources in an AWS region, or as part of an auto scaling application. The firewall cluster is highly available and scalable over multiple AWS Availability Zones, without any single point of failure such as additional management or worker node instances.

For more information, see Implementation Guide - NextGen Firewall in AWS and AWS Reference Architecture - NextGen Firewall Auto Scaling Cluster.

NextGen Firewall Cold Standby Cluster in AWS



For deployments that require a low-cost solution, the NextGen Firewall Cold Standby Cluster is an auto scaling cluster with a maximum size of one. If the instance fails, it is automatically replaced within minutes. The firewall configuration is securely stored and synchronized through AWS backend services. Replacing the Elastic Load Balancer used in the NextGen Auto Scaling Cluster with a floating Elastic IP allows the use of both TCP- and UDP-based services on the firewall. The default template uses hourly PAYG licensing, but can be modified to use pool licenses for Control Center-managed instances.

For more information, see Implementation Guide - NextGen Firewall in AWS and AWS Reference Architecture - NextGen Firewall Cold Standby Cluster.

Log File Streaming and Custom Metrics for AWS CloudWatch

The NextGen Firewall F can now stream log data to AWS CloudWatch. All selected log files are streamed via syslog streaming to be analyzed in CloudWatch. CloudWatch also collects a set of custom metrics from each firewall instance to be used for reporting and as data points for Auto Scaling policies.

For more information, see How to Configure Log Streaming to AWS CloudWatch.

Log File Streaming to Azure OMS

The NextGen Firewall F can now stream log data to Microsoft OMS in Azure. All selected log files are streamed via syslog streaming to Azure OMS, where they are stored, analyzed, and/or processed.

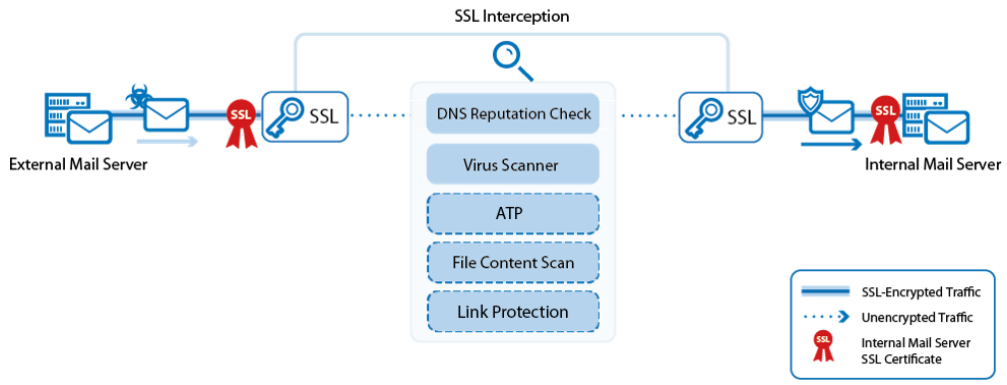
For more information, see How to Configure Azure OMS Log Streaming.

Web Interface

Web interface is an alternative configuration management tool to NextGen Admin that enables you to manage the following stand-alone hardware appliances by using a modern web browser: F18, F80, F180, F280, F380, and F400. When using the web interface for firewall configuration management, NextGen Admin can only be used in monitor mode. Switching configuration management to NextGen Admin automatically disables the web interface.

For more information, see Web Interface.

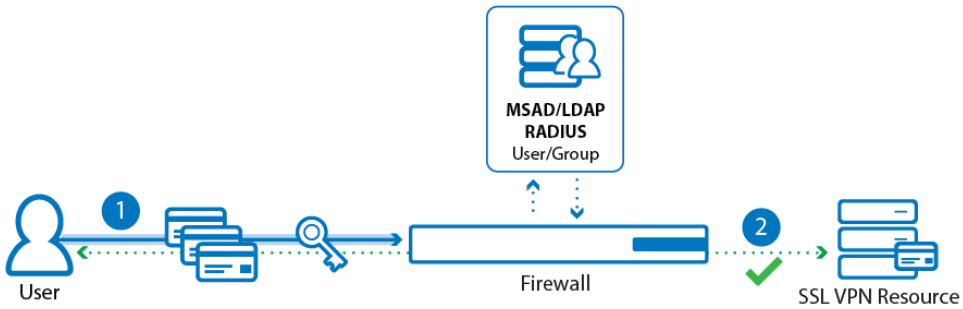
Link Protection for Mail Security in the Firewall



Sharing content with other users has become common on the web. As URLs are exchanged using emails, the risk of using incorrectly typed links can lead to fraudulent websites or unknown domains that can harm users. Link Protection protects users from such fraudulent links inside plain-text and HTML emails. In case a URL link is detected inside of an email, the URL link is checked and rewritten in case it is regarded to be fraudulent.

For more information, see Mail Security in the Firewall, and How to Configure Link Protection for Mail Security in the Firewall.

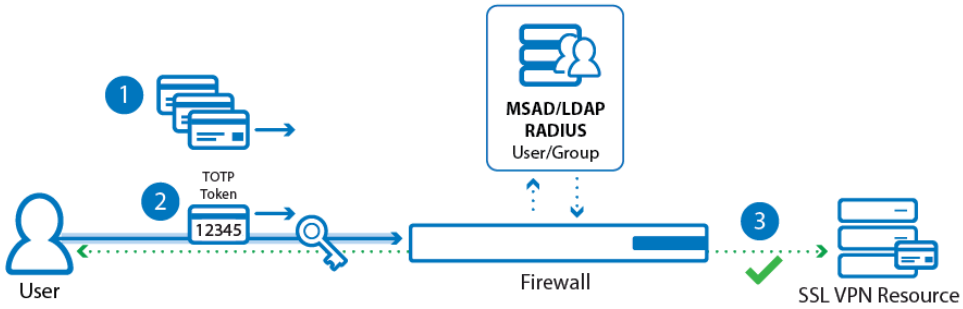
SSL VPN Access Control Policies



Access control policies with multi-factor authentication and multi-policy authentication provide granular control over access to resources by qualifying users based on groups they belong to, the technology they use, and how they authenticate.

For more information, see How to Configure Access Control Policies for Multi-Factor and Multi-Policy Authentication.

SSL VPN Google Authenticator Support



Google Authenticator provides a way of authenticating by using Time-Based One-Time Passwords (TOPT) generated by an app on a mobile device for iOS and Android. On system level, authenticating requires an authentication scheme; on user level, users are required to enroll their device for authentication.

For more information, see How to configure Access Control Policies for Google Authentication and Enroll your Mobile Device for use Google Authenticator Authentication.

SCADA Protocol Support

In industrial fields, components like sensors and actuators send and receive information as part of

industrial processes. The information is transmitted as network data to supervisory control systems for acquisition and management (SCADA). The flow of network data relates to a wide family of protocols, the most common of which are handled by the Barracuda NextGen Firewall.

For more information, see Application Control and How to Configure Application Rules Matching SCADA Protocols .

SMTP Authentication Support for Email Notifications

Email notifications sent by the Virus Scanner or ATP services can now use SMTP servers with SMTP authentication.

For more information, see How to Configure the System Email Notification Address.

Soft Network Activation for VLANs

Activating changes to the VLAN network configurations is now possible with a soft network activation. Since the network subsystem is not restarted during a soft activation, active connections continue uninterrupted.

For more information, see How to Activate Network Changes.

IPv6 Dynamic WAN Connections

The F-Series Firewall can use both stateless and stateful autoconfiguration with prefix delegation to receive IPv6 addresses from an IPv6 ISP.

For more information, see IPv6.

CudaLaunch 2.3.0

CudaLaunch for iOS now uses the TINA VPN protocol and no longer uses the built-in iOS VPN client. CudaLaunch 2.3.0 also added support for multi-factor authentication.

For more information, see CudaLaunch.

New Hardware Model F82 + F800C

Barracuda released two new appliance models: F82A and F800C. F800 Revision C provides increased port density while F82A model DSLA supports AnnexA (using RJ11 an SFP) and model DSLB supports AnnexB/J (using RJ45 and SFP).

For more information, see F82 Revision A, F800 Revision C.

Improvements Included in Version 7.1.0

Barracuda NextGen Admin

- The **Control > Status Map** now displays information in the **Appliance** and **Serial** columns for Secure Connectors. BNNGF-40591
- In NextGen Admin, **ATP** has been removed from **FIREWALL** and is now a tab of its own. BNNGF-43043
- In **NextGen Admin > DASHBOARD**, the number and width of columns for the elements are now configurable. BNNGF-43164
- The **Client Settings** section of the NextGen Admin **OPTIONS** has added a parameter toggle in the in-place editing behavior when double-clicking on a rule in the firewall ruleset. BNNGF-45402
- The built-in SSH client in NextGen Admin now supports EC ciphers. BNNGF-39133, BNNGF-39839
- NextGen Admin now displays SHA1 fingerprints as expected. BNNGF-44292
- For High Availability Clusters: In the bottom table of the **FIREWALL > Live** tab, the synchronized status of firewall sessions is now displayed when **ShowProc** is activated. BNNGF-39368
- In NextGen Admin, the user interface for tunnel settings for IKEv2 tunnels is now displayed correctly. BNNGF-44403
- Rules with the **Firewall History Entry** set to **No** in the **Advanced Settings** are no longer displayed in the **FIREWALL > History** page. BNNGF-45900
- Performance improvements for the Control Center **Status Map**. BNNGF-45011
- Several changes have been made in NextGen Admin to improve user experience on the **VPN** page. BNNGF-19036
- The **VPN Client-to-Site** page now shows correct information regarding the 'Last status' in the column of a user. BNNGF-23879
- On the **VPN Status** page, the default selection now includes IPsec IKEv2 tunnels. BNNGF-39057

Barracuda OS

- The Barracuda NextGen Firewall F10 Rev A is no longer supported for firmware version 7.1.0 or higher. BNNGF-47151

- Performance improvements have been made for bridged interfaces. BNNGF-40751
- Adding or removing interfaces that are part of a bridged interface now works as expected. BNNGF-43407
- The values for maximum session slots for some hardware models have been adjusted. BNNGF-43667
- Resolved issue causing NextGen Admin to fail when managing multiple firewalls and Control Centers. BNNGF-44892
- Logging files to an external USB storage now works as expected if log file-specific settings contain special characters. BNNGF-40129
- ART rescue installation now works as expected for F800 and F900. BNNGF-43060
- The SMTP for sending email notifications can now handle multiple responses. BNNGF-45798
- Firewall stability improvements have been made for handling FTP traffic. BNNGF-45899
- Improved error handling for retrieving available firmware updates and product tips. BNNGF-44050
- For F82 hardware firewalls, the network activation timeout has been increased to 180 seconds. BNNGF-44959
- Cloud integration logs have now been added to the syslog **Logdata Filters**. BNNGF-43075
- Logging of user names has been added to threat log entries. BNNGF-44913
- It is now possible to get the interface alias via SNMP. BNNGF-44543
- DSL Modem status is now displayed as expected. BNNGF-44078
- Removed support for SSHv1. BNNGF-33983
- Using DSA keys for SSH can now be configured as an optional feature. BNNGF-38890
- TCP window size for syslog streaming is now set correctly. BNNGF-45814
- Box layer High Availability sync for the NextGen Control Center now works as expected. BNNGF-45796
- Web Security Gateway authentication scheme now works as expected. BNNGF-45113

Control Center

- Transferring multiple updates via Control Center now shows all processed updates on the hardware firewall. BNNGF-46244
- Upgrading a pool license no longer requires a manual reassignment of the pool licenses. BNNGF-44277
- Managed firewalls using distributed firewalls are now listed on the **CONTROL > File Updates > Application Control Definition Updates** page. BNNGF-39276
- A message is displayed on the **CONTROL > Firmware Update** page if Product Tips are available. BNNGF-42129
- **F-Series VIP Networks** has been renamed to **VIP Networks** In **Global Settings** of the Control Center. BNNGF-40683
- A cluster can now be deleted regardless of existing server references. BNNGF-45322
- The **Barracuda Activation** tab now displays license types and grace periods for **Pool Licenses**. BNNGF-44134
- New columns have been added and improvements have been made to the **Floating Pool Licenses** tab. BNNGF-44497, BNNGF-44074
- New filters have been added for making selections in the **Pool Licenses** tab. BNNGF-45232
- Double-clicking a Secure Connector in the Control Center **Status Map** now opens the Secure

Connector web interface. BNNGF-32846
- On the **Control Center > Firmware Updates** page, the **Product Tips** now show the full firmware version number the hotfix applies to. BNNGF-46584
- Added an option to automatically fail over the virtual server when updating a firewall in a High Availability Cluster. BNNGF-44422, BNNGF-44423
- Updating pool licenses no longer deletes the license comment. BNNGF-42442

Access Control Service

- Memory management improvements for the Access Control service. BNNGF-36173
- Access Control Service **Allowed Client Versions** can now also match on NAC 4.0 clients. BNNGF-45220

DHCP

- DHCP requests are now passed to the DHCP server if a bridge is configured. BNNGF-31658
- DHCP configurations are now converted correctly into text format. BNNGF-32073

DNS

- DNS slave zones are now processed correctly even if multiple DNS masters are configured. BNNGF-44937

Firewall

- Stripping of TCP timestamps can now be enabled/disabled on the **FIREWALL > Forwarding Rules > Access Rules > Advanced** page in the **TCP Policy** section in the **Advanced Settings** of an access rule. BNNGF-29723
- Traffic shaping and firewall service improvements have been made to resolve some cases of high latency and load. BNNGF-39990
- Firewall service stability improvements. BNNGF-41729
- It is now possible to use a hostname network object as a redirection target in Dst NAT access rules. BNNGF-42918
- It is now possible to enable TCP timestamp stripping of the matching access rule. BNNGF-44801
- Skype audio is now detected without a preceding SSL dummy handshake. BNNGF-43091
- In **Advanced Settings** of the **Access Rules** in the **Miscellaneous** section, **Use X-Forwarded-for** has been added as an **Application Ruleset Evaluation** option. BNNGF-42985
- Firewall now supports the option to configure link protection as part of Mail Security. BNNGF-44621
- Risk-level overrides for applications now work as expected. BNNGF-24640
- SSL Interception for FTPS traffic now works as expected. BNNGF-41836
- SSL Interception improvements have been made. BNNGF-43919
- URL Filtering now also accepts URLs entered in lower-case characters. BNNGF-44615
- ONCRPC Firewall plugin stability improvements. BNNGF-46256

FSC-Series

- Deleted and disabled Secure Connectors can now be identified by the icons that display their availability and state. BNNGF-36075
- Corrected naming for Secure Connector FSC-Series parameters. BNNGF-44881,BNNGF-43875

HTTP Proxy

- HTTP Proxy no longer blocks all traffic when MIME type ACLs are configured. BNNGF-43340
- The HTTP Proxy no longer crashes if the Virus Scanner worker process reaches its limit. BNNGF-44542
- When setting the **Front End HTTPS header** to **On** or **Auto** on a reverse proxy, a backend server now redirects requests to HTTPS instead of HTTP if the backend server supports squid-specific HTTP headers. BNNGF-45534
- Importing a key with ECDHE ciphers into an HTTP Proxy now works as expected. BNNGF-36722
- For HTTP Proxies in reverse mode, when the Default Access Control Policy is set to **DENY**, traffic is now blocked as expected. BNNGF-45679

Licensing

- Importing pool licenses no longer requires the user to select the NextGen Firewall model. BNNGF-45338
- Summary information of pool licenses is now displayed correctly. BNNGF-45345
- Comments for pool licenses are now updated correctly after a pool license update. BNNGF-42442

RIP/OSPF/BGP

- For BGP over IKEv1 VPN tunnels, the BGP daemon is now only notified if the VPN tunnel status changes. BNNGF-45984

REST API

- Updated support for the REST API to send more than one response back to the client. BNNGF-36243
- HTTP and HTTP/S on the REST API are now allowed on the same port. BNNGF-37852
- It is now possible to create and mange network objects via REST-API. BNNGF-40609
- The REST API now supports importing .YANG files in order to create common types. BNNGF-40941

Virus Scanner and ATP

- File downloads using HTTP POST requests no longer fail with the ATP policy Scan First Then Deliver. BNNGF-42269
- File scanning results from the Avira virus scanning engine that contain multiple result messages are now interpreted correctly. BNNGF-42674
- IPS no longer scans traffic on the loopback interface. BNNGF-42855

- Files in the Virus Scanner quarantine are now purged on a hourly and size basis. BNNGF-45303
- It is now possible to trigger an immediate email delivery while the file is being scanned in the ATP cloud. BNNGF-42621
- In the **Virus Scanner Settings**, trusted IP addresses and host names that are excluded from scanning can now be configured. BNNGF-42746
- On the **ATP > Emails in Progress** page, the columns **State**, **Priority**, **File Type** and **Start Time** have been added to the **Attachments** list. BNNGF-45739
- ATD has been renamed to ATP. BNNGF-45846, BNNGF-45092
- In **ATP**, a new tab has been added to handle exceptions for whitelisted and blacklisted files. BNNGF-45943
- Virus scanning in the firewall now works as expected if the Virus Scanner service is on different virtual server. BNNGF-46675

VPN

- Users with VPN client access are now displayed by their CN name on the **VPN Client-to-Site** and **VPN Status** pages. BNNGF-29310
- Upgrading to 7.1.0 no longer causes VPN traffic to be missing from the IPFIX flow. BNNGF-44308
- NextGen Admin now shows IPsec local / remote network settings as expected. BNNGF-45097
- Disabling an IPsec IKEv2 tunnel via NextGen Admin now works as expected. BNNGF-34631
- Changes in the IPsec IKEv2 VPN tunnel configuration dialog are now recorded by RCS as expected. BNNGF-42869
- Enrollment of Simple Certificates (SCEP) now works as expected. BNNGF-44266
- For dynamic routing over VPN, it is now possible to rewrite the next hop to a reachable IP. BNNGF-44604
- Security associations for IKEv2 IPsec tunnels are now grouped on the **VPN > Site-to-Site** page. BNNGF-44319
- On the **VPN > Site-to-Site** page, a Dynamic Mesh does not display a VPN tunnel to itself any more. BNNGF-45073
- Simultaneous client-to-site VPN connection attempts of multiple clients no longer leads to invalid cookie errors. BNNGF-46589

SSL VPN

- New client-to-site events have been added for sending notifications either when a user establishes or terminates a client-to site VPN tunnel, or when a client-to-site VPN tunnel is terminated by the firewall. BNNGF-28171
- Favorites and Attributes for single sign-on (SSO) VPN profiles are now preserved during backup and restore. BNNGS-199
- Users can now authenticate with RADIUS even if unfinished authentication processes are pending. BNNGS-208
- Failed downloads from network places now let users stay in the web portal. BNNGS-2318
- Launching a network place to a share that does not support anonymous connections now prompts users to enter credentials. BNNGS-2361
- Recursively removing non-empty folders now works properly in VFS. BNNGS-2389
- Uploads are sent to the correct directory and renamed. BNNGS-2364

- Downloading files works even if the file is empty. BNNGS-2395
- Logging back into the web portal after a session timeout now works properly. BNNGS-2404
- Files larger than 2 GB can be uploaded on Android and iOS. BNNGS-2539
- Server requests initiated by a web app now work after doing an NTLM SSO. BNNGS-2598
- Access to the system is granted only if the client certificate is within its valid period. BNNGS-2600
- Access to network folders via CudaLaunch works for directory names that include the '#' character. BNNGS-2754
- Single sign-on works when using Microsoft Open Web Access 2010. BNNGS-2759
- Username and password can now be set for a network place in NextGen Admin. BNNGS-1928
- If authentication fails on a VPN connection, a user is prompted for a password. BNNGS-2517
- Android is now supported by NAC. BNNGS-2675
- Admins are allowed to set username/password for VPN profiles. BNNGS-2672
- SSL VPN now provides a whole certificate chain. BNNGF-45763
- Running a greater number of tunnels in conjunction with frequent DNS lookups now works as expected. BNNGF-46461

Public Cloud

- On all NextGen Firewalls and Control Centers in the public cloud SSH login via password is now disabled by default. BNNGF-46408
- On all NextGen Firewalls and Control Centers a password change is now enforced on the first login. BNNGF-44509

Known Issues

The following known issues have been fixed for 7.1.0EA via hotfix:

Hotfix 847 - KRACK Attack

- Security fix for the WPA2 vulnerability.

Hotfix 835 Security Issue

- Security hotfix to address issue that could lead to unauthorized, low privilege access via the management IP addresses

Hotfix 830 Azure

- Fixes issue causing the Azure OMS Agent to not start correctly.

Current Known Issues

- **June 2018: Firewall** – Copying access rules with enabled SSL Inspection from firewalls running firmware version 7.2.x to firewalls running firmware version 7.1.0, can have negative impact on

SSL Inspection on the destination system.

- **August 2017: VLAN** – After updating from 7.0.2 to 7.1.0 the MTU is set to 0 for all VLAN interfaces. The MTU must be set manually to 1500, otherwise the firewall will drop the connections with *Received Packet Exceeds NIC MTU (Invalid TCP-Segmentation-Offload ?)* error message. (BNNGF-47369)
- **August 2017: Firewall** – Using network object containing references to other networks objects as a **Redirection Target** in a **Dst NAT** rule currently results in an invalid firewall ruleset when trying to commit the changes. (BNNGF-47697)
- **July 2017: Named Networks** – Configuring explicit network objects referencing to Named Networks is currently not possible. (BNNGF-47751)
- **July 2017: Internal DSL Modem** – It is not possible to start, stop, or restart the DSL connections using the Barracuda DSL modem in the **Dynamic Networks** section on the **CONTROL > Box** page. (BNNGF-47819)
- **July 2017: VLAN** – After updating from 7.0.2 to 7.1.0 **Header Reordering** must be enabled for the VLAN interface, otherwise the firewall will drop the connections with *Received Packet Exceeds NIC MTU (Invalid TCP-Segmentation-Offload ?)* error message. (BNNGF-47369)
- **July 2017: Google Cloud** – In some cases NextGen Firewalls deployed in the Google Cloud are unreachable after provisioning. (BNNGF-47380)
- **July 2017: Licensing** – Downloading licenses on newly reinstalled firewalls fails if one or more licenses are expired. (BNNGF-47284)
- **June 2017** – Activating gateway routes on non-VLAN interfaces via soft network activation may cause short network downtime. Gateway routes on non-VLAN interfaces must be activated with a failsafe network activation.
- **June 2017: SSL VPN** – Google Authenticator backup codes generated on stand-alone High Availability Clusters work only when the firewall is active at the time the device was enrolled.
- **June 2017: Traffic Intelligence** – Dynamic Bandwidth and Latency Detection currently does not work on VPN transports using an IPv6 envelope. (BNNGF-47114)
- **June 2017: Control Center** – Importing an archive.par that does not contain a CC database dump fails if the CC database is enabled. (BNNGF-46601)
- **Oct 2016: Application Based Routing** – Streaming web applications such as WebEx, GoToMeeting, or BitTorrent always use the default connection configured in the application-based provider selection object. (BNNGF-42261)
- **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: 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: 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: 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: 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** – 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 2014: Barracuda OS** – **Provider DNS** option for DHCP connections created with the box wizard must be enabled manually. (BNNGF-26880)
- **Oct 2014: SSL VPN** – User Attributes do not support UTF-8. (BNNGS-435)

Figures

1. ti_probing.png
2. named_networks_01.png
3. aws_autoscale_cluster_plain.png
4. cold_standby_01.png
5. web_ui.png
6. virus_scanning_mail_traffic_atp-01.png.png
7. auth_01.png
8. auth_02.png
9. F82_Front.png
10. F800c-CCC-Front.png