7.1.1 Release Notes

https://campus.barracuda.com/doc/73008386/

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.

- 2017-09-20 – Firmware version 7.1.1 released.
- 2017-09-27 – Release Hotfix 844 Google Cloud
- 2017-10-19 – Release Hotfix 847 KRACK Attack
- 2017-10-25 – Added Web Interface Known Issue
- 2017-11-06 – Release Hotfix 851 - Public Cloud
- 2017-11-10 – Release Hotfix 852 – Firewall service stability improvements
- 2017-11-23 – Release Hotfix 856 – Resolves issue causing network interruptions after a soft network activation.
- 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) > 7.1.1**
- Before updating, read and complete the migration instructions.

For more information and a list of supported NextGen Firewall models, see 7.1.1 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 7.1.1 Migration Notes.

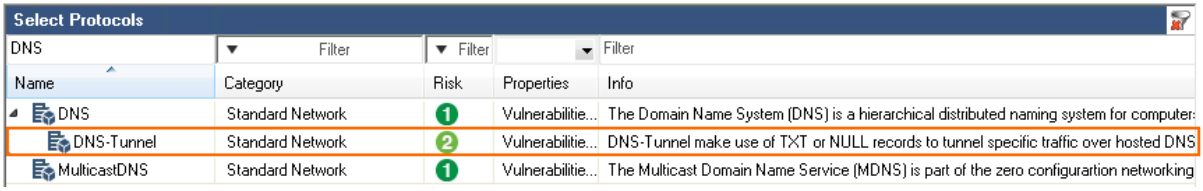
What´s New in Version 7.1.1

VPN Apps in the SSL VPN

VPN Apps for the SSL VPN are used to allow users to connect to internal web applications not suitable for SSL VPN Web Apps or native apps. CudaLaunch transparently opens a client-to-site VPN tunnel and then opens the resource in the default browser. VPN Apps are available on Windows, iOS, and Android clients through the CudaLaunch app.

For more information, see SSL VPN VPN Apps

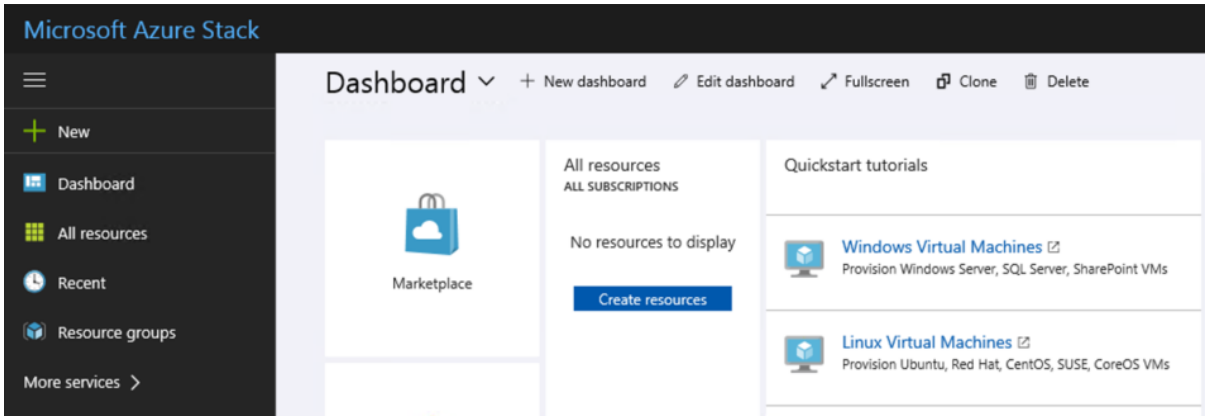
Detect and Block DNS Tunnels



DNS tunnels make use of TXT or NULL DNS records to tunnel traffic through DNS queries and responses. The NextGen Firewall can now detect and block DNS tunneling via protocol object in Block or Deny application rules.

For more information, see How to Create a Protocol Object and How to Create an Application Rule.

Azure Stack Support



The NextGen Firewall and Control Center can now be deployed in your Azure Stack environment. You can deploy either by making the standard Azure Marketplace images available for your users, or by uploading and then deploying the BYOL VHD disk images from the Barracuda Download portal.

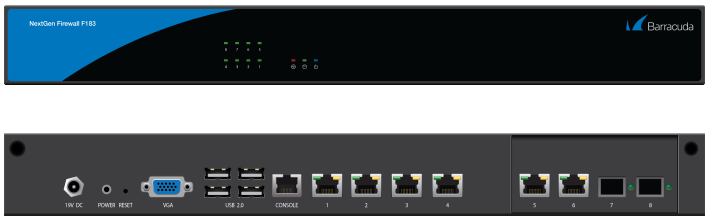
For more information, see Microsoft Azure Deployment and How to Upload Azure VHD Images for User Defined Images using ARM.

New Rugged Hardware Model F183R

Barracuda released a new ruggedized industrial appliance: The 7-port F183R with two fiber ports.

For more information, see F183R (Rugged).

New Hardware Model F183



The F183 is a desktop appliance with 6 gigabit and 2 fiber ports.

For more information, see F180 and F183 Revision A.

Improvements Included in Version 7.1.1

Barracuda NextGen Admin

- Resolved issue causing the second column of the VPN Server Settings to be invisible. BNNGF-46515
- NextGen Admin now supports virtual DPI scaling for high resolution displays. BNNGF-48005
- Increased timeout for submitting the CC Wizard configuration settings to 120 seconds. BNNGF-45136
- NextGen Admin dialogs after a **Send Changes** are no longer sometimes opened on non-existing displays. BNNGF-47238
- DSL connections using the internal Barracuda DSL modem can now be started and stopped on the **CONTROL > Box** page in the **Dynamic Networks** section of the left menu. BNNGF-47819
- On a Control Center, the **CONTROL > Pool Licenses** page querying for licenses now works as expected for all time periods. BNNGF-47616
- Failed license activations in NextGen Admin no longer block subsequent license activation attempts. BNNGF-47317
- The certificate dialog in NextGen Admin now displays the correct expiration date and fingerprint. BNNGF-39201
- Using the **Im/Export** certificate button in NextGen Admin now works for certificate chains. BNNGF-32287
- The GTI Editor no longer allows VPN tunnels to have both Dyn Mesh and WAN Optimization enabled. BNNGF-44805
- The Application Control revision browser now also contains information about changes to protocols, and file content and user agents objects. BNNGF-47300
- Added a keyboard shortcut to the **ATP** tab to allow files to be removed from the lists using the **Del** key. BNNGF-47154
- Cluster and range firewall objects are now automatically refreshed when opening the configuration dialog. BNNGF-46288
- On the **FIREWALL > Users** page, double-clicking a user now displays a formatted list of groups. BNNGF-45817
- Copying MAP access rules between different rule lists no longer changes the connection object. BNNGF-46090
- It is now possible to include references to other network objects when importing a list of network objects from a CSV file. BNNGF-45490

Barracuda OS

- Resolved logic error in the configuration process that could allow an attacker to gain unauthorized, low-privilege access to the NextGen Firewall via the management IP addresses. BNNGF-48134
- **Copy from default** with a **Send Changes** and **Activate** now writes the default values correctly into the configuration file without requiring an additional configuration change. BNNGF-46249

- Downloading licenses on newly reinstalled firewalls no longer fails if one or more licenses are expired. BNNGF-47284
- Logging into ART via SSH now works as expected for firewall models with more than one network card. BNNGF-47275
- "Changed the maximum number of concurrent connections to the firewall authentication daemon to 1020 connections." BNNGF-47067
- Increased the timeout for OCSP/CRL validation responses. BNNGF-47017
- The firewall no longer crashes if more than 250 VLANs are configured. BNNGF-46702
- DSL WAN connections using DHCP to receive the IP address from the ISP now work as expected. BNNGF-48064
- When updating from 7.0.2, the MTU for the VLAN interfaces are now set correctly. BNNGF-47369
- Configuration settings for SSL-encrypted syslog streaming are now re-enabled for managed firewalls. BNNGF-47576
- A soft network activation for a VLAN interface now also checks if the underlying physical interface also needs to be enabled. BNNGF-46619
- The **Google Authentication** configuration node has been moved from **Advanced Configuration** to **Infrastructure Services**. BNNGF-47096
- Added **Legacy Cryptography** setting in the **Advanced View** of the **Default Permission Profile** setting of the **SSH Proxy** to allow admins to re-enable pre-7.1 cryptography settings. BNNGF-46674
- Log file disk usage improvements. BNNGF-48239
- Updated ntpd to version 4.2.6p5 to fix several security vulnerabilities. BNNGF-36184
- Configuring weights between 1 and 100 for source-based multipath routes now work as expected. BNNGF-46324
- Resolved issues where a ""Login master from X.X.X.X: unkown user"" event was triggered every hour on the passive firewall in a high availability cluster. BNNGF-35824
- When using health checks for gateway routes, a state change no longer enables previously disabled routes. BNNGF-44821
- Updated bind to version 9.9.9-P8 due to multiple security vulnerabilities. BNNGF-46368
- Configuration changes via NextGen Admin no longer cause user authentication session information to be reset on the firewall. BNNGF44891

DHCP

- Setting the Max, Min, and Default lease times in the DHCP lease configuration is now mandatory. BNNGF-46098

Firewall

- Setting the **Max Session Source Accounting Objects** in the **General Firewall Settings** to a non-zero value no longer causes errors when loading the ACPF kernel module. BNNGF-47622
- Using a network object containing references to other networks objects as a Redirection Target in a Dst NAT rule no longer results in an invalid firewall ruleset. BNNGF-47697
- Local out (LOUT) IPv6 sessions on port 636 are now terminated correctly. BNNGF-46877
- Setting **Action if online URL database is unavailable** to block traffic to all websites in

the **Advanced Settings** of the URL Filter policy objects now works as expected. BNNGF-47206
- Using Link Protection as the only Application Control feature for SMTP traffic now works as expected. BNNGF-46264
- Configuring explicit network objects referencing Named Networks now works as expected when used in the access rules. BNNGF-47751
- Blocking SCADA traffic with a **DENY** rule now works as expected. BNNGF-46726
- Mail Security in the Firewall now uses the correct response messages. BNNGF-47176
- Named Networks can now be configured in the global, range, and cluster objects on a Control Center. BNNGF-48188
- Internal IPS rules are now included in the IPS signature list. BNNGF-43544
- Application Provider Selection improvements for applications using SNI in the TLS 1.2 handshake. BNNGF-45975
- Added option for the **Firewall Activity Log** to write either key-value pairs or only the value in the **General Firewall Configuration**. By default, only the values are written. BNNGF-48268
- The file name of the removed attachment is now displayed correctly in the response message included in the email. BNNGF-46783
- Link Protection improvements for plaintext emails. BNNGF-46878
- Updated **Root DNS** network object to include the the current DNS root servers. BNNGF-38070
- PAP authentication on the NextGen Firewall F82 now works as expected. BNNGF-47762
- FTP connections are now terminated with the correct server reply code when the virus scanner blocks a file. BNNGF-46581
- SSL Interception now correctly handles connections where the MTU/MSS size is smaller than the default. BNNGF-48135

Control Center

- Improved error message when a Control Center license update for managed firewalls fails due to a failed lock on the license configuration node. BNNGF-40233
- All available and uploaded update files are now displayed in the **Download Portal** and **Files on Control Center** sections of the **Firmware Update** page on the Control Center. BNNGF-46467
- Fixed fringe cases causing the license start dates in the firewall configuration and the **Barracuda Activation** tab to be displayed differently for some time / timezone combinations. BNNGF-45464
- On the **Barracuda Activation** page in the pool license context menu, changed **Remove Pool BAR-XXX** to the more accurate **Remove Pool BAR-XXX from Activation**. Removing pool licenses does not remove the floating licenses in the firewall configurations. BNNGF-46991
- Information in the **Start Date** and **End Date** columns on the **CONTROL > Barracuda Activation** page are now displayed as expected. BNNGF-46635
- Email notifications for RCS changes now work as expected. BNNGF-46898

HTTP Proxy

- Explicit IPv6 service listener IP addresses no longer cause the HTTP Proxy service to crash during the configuration activation. BNNGF-46808

Virus Scanner and ATP

- Only files uploaded to the ATP cloud are now counted toward the monthly ATP limit; files previously scanned or manually uploaded are no longer counted. BNNGF-47148
- Pending emails in the **ATP** tab are now sorted numerically. BNNGF-46734
- The file queue waiting to be scanned by ATP is now sorted based on the start time. BNNGF-47595

VPN

- IKEv2 client-to-site VPN connections with Windows 10 running the Anniversary Update (build 1067) now works as expected. BNNGF-44912
- The **Virtual IP** for client-to-site connections on the **VPN > Client-to-Site** page is now displayed. BNNGF-48136
- Changed the label of the **Listening IP** drop-down list to **Use Transport Source** instead of **default-from-My-IP**. BNNGF-44618
- Memory-handling improvements for IPsec IKEv1 tunnels in the VPN service. BNNGF-44360
- Client-to-site VPN connections using SHA2 certificates in combination with password authentication now work as expected. BNNGF-42586
- It is now possible to enter a hostname as the **Remote Gateway** in the IKEv2 IPsec VPN tunnel configuration. BNNGF-41471
- Performance improvements for VPN tunnels on Ethernet Bundles (bond) interfaces running on NextGen Firewall hardware models using the igb driver. BNNGF-42808

Public Cloud

- Stability improvements to the Google Cloud provisioning process. BNNGF-47380
- Google Cloud SDK is now available on the firewall. BNNGF-47363
- New firewall instances in an Auto Scale Cluster are now detected and included correctly in aggregated pages in NextGen Admin. BNNGF-46003
- Firewalls deployed in Azure can now also send metrics to Azure OMS.
- Internal and external IP addresses and internal networks for public cloud firewalls in Azure and AWS are now stored in dedicated dynamic network objects and no longer in custom external network objects.

SSL VPN

- Text-based user attributes now handle UTF-8 encoded text. BNNGS-435
- RADIUS authentication with challenge response now works as expected. BNNGS-937
- Clearing the address bar no longer results in a new SSL VPN session. BNNGS-1644
- Excessively long Native App names with more than 75 characters no longer cause the SSL VPN service to fail. BNNGS-2170
- Custom replacements in proxied web apps with more than 256 characters now work as expected. BNNGS-2703
- SSL Tunnel path length of more than 64 characters no longer causes resource to fail on use. BNNGS-2960
- It is now possible to use the hash ('#') symbol in a user attribute. BNNGF-2991

- It is now possible to use the hash ('#') symbol in a web app single sign-on configuration. BNNGS-2992
- When evaluating the SSL VPN with the included single user license, one CudaLaunch and one SSL VPN web portal connection are now allowed. BNNGS-3085
- Default values for user attributes now work as expected. BNNGS-3106
- Network places on CudaLaunch for Android/iOS now prompt for credentials if the supplied credentials are incorrect. BNNGS-3113
- Multiple stability improvements for Google Authenticator. BNNGS-3074
- Added a link to the Windows App store to the SSL VPN web portal. BNNGS-3120
- Removed legacy Java applet-based health check components from SSL VPN service. BNNGS-3073

Zero Touch

- Improvements to automatic revert detection. BNNGS-2884
- The Zero Touch client process now cleans up /tmp folder after provisioning. BNNGS-3108

Issues Resolved by Hotfixes

Hotfix 844 - Google Cloud

- Generic Segmentation Offloading (GSO) is now disabled in the KVM networking drivers used for firewalls running in the Google Cloud.

Hotfix 847 - KRACK Attack

- Security fix for the WPA2 vulnerability.

Hotfix 851 - Public Cloud

- The OMS Agent now works as expected after upgrading from 7.1.0 to 7.1.1.
- Custom metrics collected by the OMS Workspace now work as expected.

Hotfix 852 - Firewall Service Stability Improvements

- Firewall plugin stability improvments, resolving issues with failed FTP data sessions when handling a large number of FTP sessions.
- Resolved issue where in some cases application rules did not match for HTTPS sessions. This also caused URL Filter and File Content policies configured in the application rule to not be evaluated.
- Multiple SMTP and FTP protocol handling improvements.

Hotfix 856 – Control: Network Activation

- A soft network activation now only removes changed virtual server IP addresses and no longer

causes a network interruption.

Current Known Issues

- **Jun 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 - 7.1.1, can have negative impact on SSL Inspection on the destination system.
- **Nov 2017: URL Filter** – URL Filtering currently does not work with PAYG images.
- **Nov 2017: VLANs** – Transferring data over configured VLAN interfaces of a NextGen Firewall F180 or F280b can fail even if the MTU size is changed. BNNGF-46289
- **October 2017: Web Interface** – New NextGen Firewalls using the Web Interface must start the basic setup wizard manually on the **ADVANCED > Wizard** page after the first boot. BNNGF-49057
- **September 2017: Azure ASM** – NextGen Firewalls deployed using Azure Service Manager do now show the status **running** after deployment in the Azure portal. This does not affect the firewall VMs functionality. BNNGF-48296
- **September 2017: Authentication** – Web Security Gateway authentication schemes are currently not working. BNNGF-45113
- **September 2017: FTP Firewall Plugin** – If a FTP server responds to a RETR or STOR command with a multi-line reply, the FTP control session hangs. BNNGF-48996
- **September 2017: Zero Touch** – On freshly installed 7.1.1 Control Centers Zero Touch fails with `No CC identifier found` logged periodically in the ztd.log file. Execute `/opt/phion/hooks/service/rangeconf/hook_rangeconf START` as root to fix this issue. BNNGF-48898
- **September 2017: Statistics** – Retrieving performance statistics for inBytes, OutPkts, and OutPktsload is currently not possible. BNNGF-48574
- **September 2017: NextGen Firewall F82** – The DSL connection is not started automatically after restoring the configuration from a PAR file. This also includes reinstalling via USB stick with an PAR file included. BNNGF-47097
- **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. BNNGF-48862
- **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: 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). BNNGF-38823
- **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 Firewall as the Firewall service. This issue does not occur when running the HTTP Proxy service on a second NextGen Firewall behind the NextGen 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 via RIP, OSPF, or BGP, a duplicate routing entry is created and the route that was 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 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

Figures

1. vpn_apps.png
2. dns_tunnel.png
3. Azure_stack.png
4. F183-R.PNG
5. F183_Front.png
6. F183.back.png