7.0.1 Release Notes

https://campus.barracuda.com/doc/71862315/

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

This firmware version includes a critical security issue resolved by installing Hotfix 834. For more information, see Hotfix 834 - Security Issue.

Before installing or upgrading to the new firmware version:

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

Changelog

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

- 24.10.2016 – Firmware version 7.0.1 released.
- 27.10.2016 – Added ClamAV known issue.
- 29.11.2016 – Added summaries for the following hotfixes: 803, 804, 808, 809, 811, and 812
- 29.11.2016 – F800 Rev B and F900 Rev A ART recovery known issue
- 30.11.2016 – FSC firmware 1.0.5 released
- 24.01.2017 – Added IPv6 IPS known issue
- 25.01.2017 – Added summaries for the following hotfixes: 817, 815, and 816
- 25.01.2017 – CudaLaunch 2.2. released
- 16.02.2017 – Added known issue for the NextGen Firewall F10 Rev A installation via F-Series Install.
- 21.02.2017 – Added CC Syslog and Application Control known issues.
- 19.10.2017 – Release Hotfix 848 KRACK Attack.

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

For more information, see Migrating to 7.0.

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

For more information, see 7.0 Migration Notes.

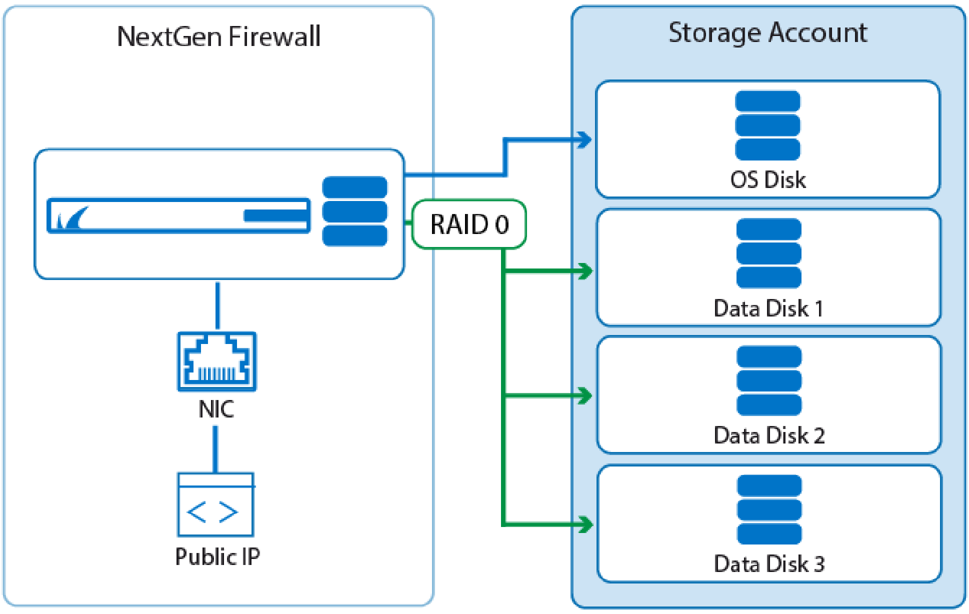
What´s new in version 7.0.1

NextGen Firewall F-Series for Google Cloud Platform

You can deploy the Barracuda NextGen Firewall F-Series to Google Cloud Platform as a gateway or remote connectivity device. The firewall is deployed into a dedicated subnet (public subnet) in the Google Cloud network, and the instances for your cloud-based applications are deployed into backend or private subnets of the network. The firewall has a single dhcp network interface with a private IP address. The public IP address assigned to the firewall is either static or ephemeral (dynamic).

For more information, see Public Cloud and How to Manually Upload and Deploy the F-Series Firewall in the Google Cloud.

Azure data disk support



Azure limits the number of IOPS per second based on the VM size and storage account. To distribute the I/O load across multiple disks, the NextGen Firewall now supports data disks. If present during deployment via PowerShell or Azure Templates, a RAID device is automatically created and mounted on /phion0/. Data disks can also be added to existing firewall VMs or firewall VMs that have been deployed through the Azure portal. Both ASM and ARM are supported.

For more information, see How to Add and Remove Data Disks in Azure and How to Add and Remove Data Disks in Azure using ASM.

NextGen Control Center for Amazon AWS

The NextGen Control Center is now available as a BYOL image in the AWS Marketplace.

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

Secure Access Concentrator for AWS and Azure

The Secure Access Concentrator can now also be deployed in AWS and Azure public clouds via the NextGen Firewall F image in the respective marketplaces.

For more information, see Secure Access Concentrator in Azure and AWS.

CudaLaunch 2.2

CudaLaunch for Windows and macOS is now available as a portable executable and as a Windows installation package. CudaLaunch now also offers support for SSL VPN network places on all platforms and offers VPN client integration on Windows and macOS.

For more information, see CudaLaunch and SSL VPN Network Places.

Improvements included in version 7.0.1

NextGen Admin

- Information from the activation form now supports all UTF-8 characters. (BNNGF-38779)
- The **FIREWALL > Monitor** page now no longer crashes if an element is selected that is not supported by the firmware. (BNNGF-40884)
- Users authenticated via the HTTP Proxy are now displayed on the **FIREWALL > Live** and **FIREWALL > History** pages. (BNNGF-40826)
- When entering hostnames or IP addresses on the login screen, spaces are now removed. (BNNGF-40959)
- IPv6 management session information is now displayed correctly in the **Break Lock**, **Show Lock Info**, and **Configuration Sessions** dialogs. (BNNGF-38926)

- Editing a CC admin no longer requires a password change to be able to save the changes. (BNNGF-38985)
- NextGen Admin now checks if the configuration imported from the clipboard matches the configuration node. (BNNGF-40394)
- Checking for duplicates when entering IPv6 addresses in the connection object dialog now works for both abbreviated and non-abbreviated notations. (BNNGF-38671)
- Disabled NAT view for the host firewall ruleset. (BNNGF-40164)
- A warning is shown when connecting to a firewall running a newer firmware than is supported by this version of NextGen Admin. (BNNGF-39095)
- **Available IPs** in the **Service Properties** are now displayed correctly if the **Secondary IP** in the **Server Properties** is left empty. (BNNGF-22643)
- The **Firmware Update** tab of the Control Center now has an additional button to **Create update tasks**. (BNNGF-39138)
- A new range is now displayed immediately in the configuration tree before activating the changes. (BNNGF-26668)
- Manually deleting ATD files from the **Scanned Files** or **Malicious Files** tabs now marks them as deleted in the **Top Threats** dashboard element. (BNNGF-39915)
- A new cluster is now displayed immediately in the configuration tree when creating a new cluster with an activation template. (BNNGF-38703)
- IP addresses for firewalls accessed not via the login screen are now added to the **Recent Connection** column. (BNNGF-39421)
- NextGen no longer crashes when restarting the CC VPN service and then clicking **Disconnect**. (BNNGF-39257)
- The correct updated firmware version is shown after updating a managed firewall via the **Firmware Update** page on the Control Center. (BNNGF-38839)
- RDP clients using the Touch API to emulate the right-click now work as expected for NextGen Admin. (BNNGF-27845)

Barracuda OS

- Updated Wi-Fi kernel module to fix security vulnerability CVE-2014-2672. (BNNGF-40703)
- Optimized internal syslog settings to improve performance. (BNNGF-40887)
- UMTS/3G parameters were renamed to WWAN to be more generic. (BNNGF-39977, BNNGF-40127)
- The HTTP Proxy service is no longer included in the default configuration. (BNNGF-26032)
- Enabling the URL Filter is now shown correctly in RCS. (BNNGF-40534)
- It is now possible to enter a hostname as the NTP server. (BNNGF-38950)
- The trust level for the **Additional IPs** is added to the respective network objects as expected. (BNNGF-30560)
- Logging in to the ART menu via SSH key now works as expected. (BNNGF-30782)
- USB log file storage now works as expected on firewall models with flash storage. (BNNGF-39913)
- Event **2045 Entering GRACE mode** is now triggered correctly when the license enters grace mode. (BNNGF-41064)
- Web Log streaming now works as expected for HTTPS sessions when no additional Application Control features are enabled in the access rule. (BNNGF-41274)

Firewall

- Inline firewall authentication now uses a browser authentication pop-up window by sending 401 unauthorized, and no longer redirects to the login page. (BNNGF-40979)
- Block access rules using the DNS sinkhole dynamic network object now work as expected. (BNNGF-39567)
- Application Control statistics now work as expected when the **Maximum sessions** in the **General Firewall Settings** are set to a high value . (BNNGF-39474)
- SSL Interception now works as expected for clients using the TLS certificate status request extension (OCSP stapling). (BNNGF-41093, BNNGF-41413, BNNGF-41451)
- DHCP requests forwarded over a bridged interface no longer intermittently drop requests. (BNNGF-30262)
- Schedule objects with a large number of objects (>128) now work as expected. (BNNGF-40857)
- In rare cases, virus scanning FTP traffic caused a firewall lockup. This no longer occurs. (BNNGF-41082)
- Hostname network objects no longer remain in a pending state if the AAAA lookup times out. (BNNGF-40022)
- Changed documentation to state the forwarding and distributed firewall services may not be run on the same firewall. (BNNGF-40947)
- Improved user agent detection for browsers on Android devices. (BNNGF-40067)
- It is now possible to use transparent redirect in combination with Application Control features. (BNNGF-40384)
- Removed Transparent Proxy rules from default firewall ruleset. (BNNGF-33747)
- Improved Application Control detection rate. (BNNGF-38584)
- Web log streaming now works as expected if no additional Application Control features are enabled on the access rule. (BNNGF-31274)
- Unusual HTTP trailing header fields are now handled correctly. (BNNGF-40200)
- The default connection object names are renamed to match the **Translated IP** policy names. (BNNGF-39803)
- Internet Explorer 11 on Windows 10 is now detected by User Agent Filtering. (BNNGF-40690)
- Custom block pages now display custom applications correctly. (BNNGF-40060)
- Creating a **List of IPv6 Addresses** or **List of IPv6 Networks** network object type with only a MAC address now works as expected. (BNNGF-38937)
- For virus scanning in the firewall, the event **5005 Virus Scan file blocked** is triggered when a virus is blocked. (BNNGF-28344)
- Offline firewall authentication now redirects HTTP traffic to the HTTPS page on port 443, 444, and 445. (BNNGF-29074)
- The DNS sinkhole network object is now included in the default configuration of the forwarding and distributed firewall. (BNNGF-40473)
- Hostname network objects not using a FQDN are now resolved correctly. (BNNGF-35815)
- It is not possible to set the **Same Port** option in connection objects with the **Translated Source IP** set to **Network Interface**. (BNNGF-40375)
- Improved session handling of the firewall service to fix random system crash. (BNNGF-38163)
- Firewall ruleset re-evaluations no longer terminate sessions matching rules using hostname network objects. (BNNGF-40353)
- Virus scanning FTP traffic now works as expected. (BNNGF-41082)

- The firewall no longer crashes when manually terminating sessions using WAN Optimization via command line interface. (BNNGF-39730)
- The **PORTMAPPER** service object now uses the **oncrpc** firewall plugin. (BNNGF-36160)
- The default ruleset now includes a service object and rule for **Barracuda ScreenConnect**. (BNNGF-40180)
- Changes to the list of trusted CA certificates is now take effect immediately. (BNNGF-34630)

Virus Scanner

- Mail scanning in the firewall now logs to **/<virtual server name>/<firewall service name>/virusscan.log**. (BNNGF-41351)
- The **<factory-default-mime-types>** now include all **application/*** MIME types. (BNNGF-41376)

VPN

- IPsec IKEv1 tunnels using AES256 encryption and SHA256 hashing now work as expected. (BNNGF-39297, BNNGF-39295)
- Added option to disable **Replay Protection** for IPsec IKEv1 site-to-site VPN tunnels by setting the **Replay Window**
  Size to -1. (BNNGF-38991)
- Enabling **High Performance Settings** for TINA site-to-site tunnels not using UDP as the **Transport** is no longer possible. (BNNGF-38981)
- The correct key size (512bit) is now used when automatically generating the server key for export-restricted VPN services. (BNNGF-39659)
- IKEv2 log messages now have the correct type and no longer all use **info** as the type. (BNNGF-38992)
- Activating IKEv2 IPsec site-to-site tunnel configurations no longer rely on a valid IKEv2 IPsec client-to-site configuration. (BNNGF-38880)
- Changed naming for RSA ACE authentication prompts to match official naming for SecurID. (BNNGF-36838)
- The WAN optimization deduplication process no longer crashes if a large number of sessions are using WAN optimization. (BNNGF-39729)
- Increased the maximum number of sessions for WAN optimization. (BNNGF-40787)
- Importing a certificate in the VPN Settings after the first import fails now works as expected. (BNNGF-38909)

HTTP Proxy

- It is now possible to include an **ACL File** when creating an HTTP Proxy access control policy. (BNNGF-40314)
- It is now possible to configure the incoming and outgoing IP addresses in the **Access Control Policy**. (BNNGF-40820)
- When configured as a reverse proxy, ATD now scans uploaded files in deliver first, then scan mode. (BNNGF-39932)
- Modified help text to state that **User authentication objects** using NTLM/ MS Chap

authentication must enter the username as follows – DOMAIN\user (BNNGF-41070)

NextGen Report Creator

- Added option to report based on a subnet or network. (BNNGF-40862)

Control Center

- Non-local references for global, range, and cluster network objects are no longer removed when the object is renamed. (BNNGF-40370)
- CC Admins can no longer see file updates for firewalls out of their administrative scope. (BNNGF-38799)
- Deleting an **Update Task** after the transfer has been completed now also removes the file from the firewall. (BNNGF-38906)
- It is now possible to configure the source IP address used to send file updates to managed firewalls. (BNNGF-24538)
- Configuring the log cycling action **move to external storage** for a managed firewall via the Control Center now sets the **storage dir** correctly. (BNNGF-40128)
- Renamed **Generic Network Object** to **Generic IPv4 Network Object**. (BNNGF-40955)
- File content, user agent and schedule objects can now be configured as global, range and cluster objects. (BNNGF-36850)

DHCP

- The **All Clients Policy** is now set to **Allow** per default. (BNNGF-30820)

S-Series

- After deleting and re-creating an S-Series VIP network, the correct CIDR network is used. (BNNGF-40348)
- It is no longer possible to change the S-Series VIP network on the Secure Access Concentrator VPN service. (BNNGF-39936)
- It is no longer possible to unlock the SC Editor before activating the changes. (BNNGF-39910)
- Deleting a cluster now also removes the configuration for the SCs in the cluster. (BNNGF-40654)
- It is now possible to explicitly set the Wi-Fi channel used by the SC. (BNNGF-40062)
- Removed DES and NONE, and set the default encryption to AES256 for SC VPN. (BNNGF-40435)
- **Copy from Default** now works as expected for **S-Series VIP Networks** and **SC Editor** configuration nodes. (BNNGF-41048)
- SCs not within the CC admin's administrative scope are no longer visible on the **Configuration Update** and **Firmware Update** pages. (BNNGF-40018)
- SCs created from a template now have default values. (BNNGF-39776)
- It is now possible to disable a FSC in the SC Editor. (BNNGF-38032)
- Removed the **VPN** column from the SC Editor. (BNNGF-40502)

Virus Scanner and Advanced Threat Detection

- It is no longer possible to manually quarantine mail attachments scanned by ATD to avoid the

the mail server IP address being placed in quarantine. (BNNGF-39476)

SSL VPN

- Increased the maximum URL length for SSL VPN web apps. (BNNGS-2441)
- Using NTLM authentication for SSL VPN web apps now works as expected. (BNNGS-2314)

RIP/OSPF/BGP

- Allow **other** interfaces in RIP filter configuration. (BNNGF-35502)

Issues resolved by hotfixes

The following hotfixes have been released for firmware version 7.0.1

Hotfix 848 - KRACK Attack

- Security fix for the WPA2 vulnerability.

Hotfix 804 – Azure

- Add support for Cloud Integration for Azure Germany.
- Add support to configure API endpoints for custom Azure environments.
- UDR updates and IP forwarding protection now work as expected when the firewall is not in an high availability cluster.

Hotfix 803 – HTTP Proxy

- Updated HTTP Proxy to fix connection error handling.

Hotfix 808 – Firewall

- Resolves problems with asynchronous ATD download page
- Sensor data for F800 Rev C and F900 Rev B are now displayed correctly.
- Resolves problems with firewall memory consumption and hostname network object resolution

Hotfix 809 – Public Cloud VPN Service

- The client-to-site VPN configuration dialog now works as expected.

Hotfix 811 – SSL VPN

- Updates code signing certificate required to validate integrity of the SSL VPN Java applets.

Hotfix 812 – DNS Server

- Updates BIND to version 9.9.9-p4 to fix security vulnerability CVE-2016-8864.

Hotfix 815 – Firewall

- Resolves problems with asynchronous ATD download page.
- Sensor data for F800 Rev C and F900 Rev B are now displayed correctly.
- Resolves problems with firewall memory consumption and hostname network object resolution.
- Improves issues with the UDP session timer.
- Resolves issues with custom block page delivery.

Hotfix 816 – VPN

- Added advanced configuration parameters to improve vendor interoperability.
- Added option to enforce UDP encapsulation for ESP packets (port 4500).
- Added support for negotiation of Traffic Selectors and Cipher Suite Proposals.
- Upgraded strongSwan to 5.4.0.
- Fixed an issue that potentially results in intermittent connectivity problems during CHILD_SA rekeying.
- Dead Peer Detection (DPD) is now enabled by default.
- Resolved various stability issues with site-to-site VPN tunnels to the Microsoft Azure VPN Gateway.
- Added support for creating dedicated SAs for each subnet pair (Cisco ASA).
- Allow coexistence of multiple SAs with identical Traffic Selectors.
- It is now possible to use hostnames as the remote gateway.
- Added support for Elliptic Curve-based DH Groups (NIST, Brainpool).
- ESP Lifetimes are now reliably enforced in all cases.
- Rekeying is no longer disabled if the ESP lifetime is too low.
- VPN routes for disabled IKEv2 tunnels are removed immediately.

Hotfix 817 – Cumulative Hotfix

- Updating patterns and definitions for a large number of managed firewalls no longer overloads the Control Center.
- The client-to-site VPN configuration dialog now works as expected.
- Repository linked global firewall objects no longer prevents cluster migration to firmware version 7.0.

Hotfix 823 – Cumulative Hotfix

- Added option to disable preview mails of pending ATD email scans in the Virus Scanner Settings
- It is now possible to override the Scan Fail, Large File and Archive policies for SMTP and SMTPS connections in the Virus Scanner Settings
- Improves issues with the UDP session timer
- Resolves issues with custom block page delivery
- Added advanced configuration parameters to improve vendor interoperability

- Added option to enforce UDP encapsulation for ESP packets (port 4500)
- Added support for negotiation of Traffic Selectors and Cipher Suite Proposals
- Upgraded strongSwan to 5.4.0
- Fixed an issue that potentially results in intermittent connectivity problems during CHILD_SA rekeying
- Dead Peer Detection (DPD) is now enabled by default
- Resolved various stability issues with site-to-site VPN tunnels to the Microsoft Azure VPN Gateway
- Added support for creating dedicated SAs for each subnet pair (Cisco ASA)
- Allow coexistence of multiple SAs with identical Traffic Selectors
- It is now possible to use hostnames as the remote gateway
- Added support for Elliptic Curve-based DH Groups (NIST, Brainpool)
- ESP Lifetimes are now reliably enforced in all cases
- Rekeying is no longer disabled if the ESP lifetime is too low
- VPN routes for disabled IKEv2 tunnels are removed immediately
- Rekeying management tunnels on a Secure Access Concentrator now works as expected
- Resolves issue that may lead to incorrect routing for Dynamic Mesh VPN tunnels

Current known issues

- **Feb 2017: Application Control** – Risk level overrides for Applications are currently not honored and the default risk level used instead. (BNNGF-24640)
- **Feb 2017: CC Syslog** – It is currently not possible to select **UDP** as the **Supported Protocol** for the CC Syslog service. To use UDP select **TCP&UDP** as a workaround. (BNNGF-44632)
- **Feb 2017: NextGen Firewall F10 Rev A** – It is currently not possible to install a Barracuda NextGen Firewall F10 Rev A via F-Series Install. Install 6.2.2 and upgrade to 7.0.1 instead. (BNNGF-43579)
- **Jan 2017: IPv6 IPS** – It is currently not possible to use IPS in **Report Only** mode for IPv6 traffic. All IPv6 traffic matching one of the IPS signatures is dropped. (BNNGF-23520)
- **Nov 2016: ART** – It is currently nor possible to successfully recover a Barracuda NextGen Firewall F-900 Rev A or F800 Rev B via ART. (BNNGF-43060)
- **Oct 2016: Virus Scanner** – In some cases the clamAV virus scanner engine no longer responds after a pattern update. (BNNGF-42429)
- **Oct 2016: FSC Series** – Assigning a second FSC pool licenses to an Access Concentrator currently does not add the second license float to the Access Concentrator. (BNNGF-39627)
- **Oct 2016: Application Based Routing** – Streaming web applications such as WebEx, GoToMeeting or bit torrent always use the default connection configured in the Application based provider selection object. (BNNGF-42261)
- **Oct 2016: File Content Policy Filtering** – Configuring a file content policy with multiple filename entries may result in not all configured filenames being blocked. (BNNGF-35982)
- **Sept 2016 IPsec IKEv1 IPv6** – It is not possible to use hostnames as the remote gateway.
- **Sept 2016: IPsec IKEv1 IPv6** – It is not possible to use a dynamic local gateway.
- **Sept 2016: IPsec IKEv2** – It is not possible to establish a VPN tunnel if the active partner uses a dynamic IP address.

- **Sept 2016: IPsec IKEv2** – NAT Traversal is not possible when using a dynamic local gateway.
- **Sept 2016: TINA IPv6** – It is not possible to use proxies for TINA VPN tunnels using IPv6.
- **Sept 2016: OSPF** – Enabling OSPF through the **Run OSPF Router** setting currently has no effect on freshly installed 7.0.0 firewalls. Enable OSPF by entering a dummy IP address in the **Summary Range IP/ Mask** list of the **OSPF Area Setup**.
- **Sept 2016: VMware** – Network interfaces using the VMXNET3 driver do not send IPsec keepalive packets unless TX checksumming is disabled for the interface (ethtool -K INTERFACE tx off).
- **Sept 2016: URL Filter** – Firewalls running 6.2.0 or higher that are managed by a Control Center using firmware 6.0.X or 6.1.X must complete a dummy change in the security policy whenever enabling/disabling the URL Filter in the **General Firewall Settings**.
- **Sept 2016: Azure** – After updating a firewall using Azure UDR via Azure Service Manager, the **Deployment Type** may be displayed incorrectly as **y**. This does not affect updating Azure UDR routes.
- **Sept 2016: Public Cloud** – Performing **Copy from Default** of Forwarding Firewall rules currently locks out administrators from the unit and requires a fresh installation of the system. (BNNGF-41514)
- **Sept 2016: IKEv1 IPsec** – When using 0.0.0.0 as a local IKE gateway, you must enable **Use IPsec Dynamic IPs** and restart the VPN service before a listener on 0.0.0.0 is created.
- **Sept 2016: HTTP Proxy** – Custom block pages do not work for the HTTP Proxy when running on the same NextGen F-Series Firewall as the Firewall service. This issue does not occur when running the HTTP Proxy service on a second NextGen F-Series Firewall behind the NextGen F-Series Firewall running the Firewall service.
- **Sept 2016: VPN Routing** – When a duplicate route to an existing VPN route in the main routing table is announced to the NextGen Firewall F-Series via RIP, OSPF, or BGP, a duplicate routing entry is created and the route that was added last is used.
- **Sept 2016: VPN Routing** – Creating a direct or gateway route with the same metric and destination as a VPN route in the main routing table results in duplicate routes. The route added last is used.
- **Sept 2016: ATD** – Only the first URL in the Quarantine tab that leads to a quarantine entry is displayed, even if the user and/or IP address downloaded more than one infected file. This can be dangerous if the first downloaded file is a false-positive.
- **Sept 2016: Terminal Server Agent** – It is not currently possible to assign connections to Windows networks 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 currently not supported for Control Centers deployed using Barracuda F-Series Install. (BNNGF-28210)
- **Dec 2015: URL Filter** – It is not possible to establish WebEx sessions when the URL Filter is enabled on the matching access rule. (BNNGF-35693)
- **Nov 2015: IKEv2** – Changing a setting for an IKEv2 tunnel disabled in the configuration causes all active IKEv2 tunnels to initiate a re-keying.
- **Nov 2015: IKEv2** – Client certificate authentication for client-to-site IKEv2 IPsec VPNs requires

X509 Certificate to be enabled in the **VPN Settings**. Enabling this setting requires all VPN group policies to use client certificate authentication.

- **Nov 2015: IKEv2** – After a restart, the **Last Access** and **Last Duration** time displayed for site-to-site IKEv2 IPsec tunnels is not reset.
- **Nov 2015: IKEv2** – Using a hostname or subnets as **Remote Gateway** is currently not possible. (BNNGF-34681,BNNGF-41471)
- **Nov 2015: IKEv2** – Using pre-shared keys with IKEv2 client-to-site VPNs is not possible. (BNNGF-34874)
- **Nov 2015: IKEv2** – Using X509 Subject Policy in a client-to-site **Group VPN Settings** is not possible.
- **Nov 2015: IKEv2** – Connecting to an IKEv2 IPsec client-to-site VPN using iOS or Android devices is not possible. (BNNGF-3487)
- **Nov 2014: Barracuda OS** – **Provider DNS** option for DHCP connections created with the box wizard must be enabled manually. (BNNGF-26880)
- **Oct 2014: SSL VPN** – Favorites are not included in the PAR file. (BNNGS-199)
- **Oct 2014: SSL VPN** – User Attributes do not support UTF-8. (BNNGS-435)

Figures

1. Azure_data_disks1.png