

## 7.0.0 Release Notes

<https://campus.barracuda.com/doc/71862316/>

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 837. For more information, see [Hotfix 838 - Security Issue](#).

### Update available

NextGen Firewall 7.0.0 build 672 is now available from the Barracuda Download Portal.

#### For customers already using 7.0.0

Existing units running 7.0.0 can update via the update package to 7.0.0 build 672.

For more information, see [Updating F-Series Firewalls and Control Centers](#).

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](#).

- 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](#).

## Changelog

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

- 19.10.2017 – Release [Hotfix 848](#) KRACK Attack.

## Hotfixes included with version 7.0.0

- Hotfix **748** – glibc
- Hotfix **752** – Realtek Network Interfaces
- Hotfix **753** – SSLv2
- Hotfix **762** – HTTP Proxy
- Hotfix **763** – SSL VPN
- Hotfix **765** – DNS Server
- Hotfix **771** – Wi-Fi Service
- Hotfix **777** – Cumulative Hotfix
- Hotfix **779** – Secure Access Concentrator and Control Center
- Hotfix **780** – Azure Control Center
- Hotfix **781** – VPN service and OSPF

## What's new in version 7.0.0

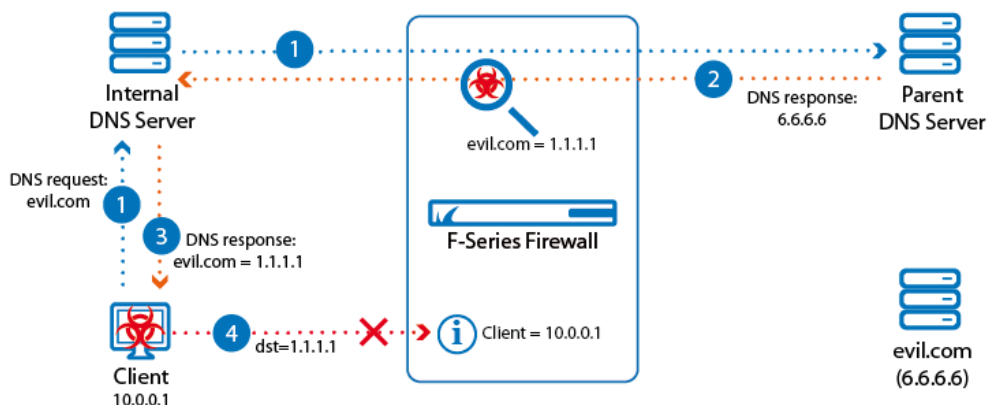
### VPN service IPv6 support



You can now connect two locations using IPv6 addresses via site-to-site VPN with either the TINA, IPsec IKEv1, or IKEv2 VPN protocols. The GTI Editor and Traffic Intelligence also added support for IPv6 transports, allowing you to configure and use a mix of IPv4 and IPv6 transports. Client-to-site and remote management tunnels can also connect using IPv6 addresses. Traffic passing through the tunnel is IPv4-only.

For more information, see [Authentication, Encryption, Transport, IP Version and VPN Routing](#).

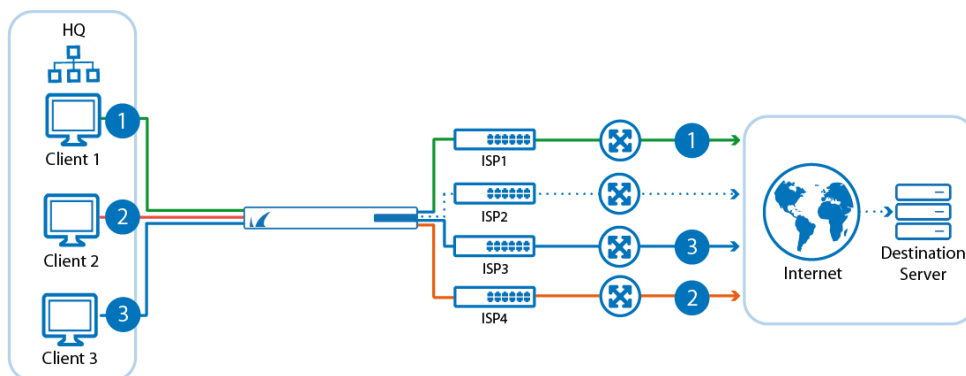
### DNS sinkhole in the Firewall



DNS traffic handled by the Firewall service is monitored and, if a domain is found that is considered to be malicious, the A and AAAA DNS response is replaced by fake IP addresses. An access rule blocks the clients from accessing the fake IP addresses and logs the attempt in the Threat Scan and Firewall Monitor.

For more information, see [Botnet and Spyware Protection in the Firewall](#).

### Connection object and load balancing improvements



You can now create custom connection objects with failover and/or load balancing of up to eight connections. For applications requiring sticky sessions, the **Source IP Hash** load balancing policy is added. This load balancing policy uses the hash of the source IP address to determine the egress interface. This setting is persistent as long as the source IP address of the client is not changed. Failover alternatives can now also use the **Original IP** and **Dynamic NAT** policies.





For more information, see [Connection Objects](#).

### Rest API

Barracuda Network provides you with a Rest API for the F-Series Firewall, allowing you to integrate the firewall into your applications. See our Rest API developer documentation for more information.

For more information, see [Rest APIs](#).

### Firmware update directly from UPDATES element

UPDATES				FILTER 
Available			Installed	
Scope	Type	Release Date	Name	
 Maintenance	Package	01.03.2016	Cumulative Hotfix including Hotfix 729, 730, and 742	
 Maintenance	Package	28.01.2016	<div> Download  Download and Install  Download with your default Browser  Copy Download Link to Clipboard </div>	
 Maintenance	Package	28.01.2016		

You can download and install updates and hotfixes directly from the UPDATES element on the NextGen Admin dashboard for stand-alone firewalls. For managed firewalls, the update or hotfix package is downloaded directly to the Control Center and then distributed to the managed firewalls.

For more information, see [Updating F-Series Firewalls and Control Centers](#).


## IPv6 support for hostname network objects and custom external network objects

It is now possible to resolve IPv6 addresses of FQDNs of hostname network objects. Importing IPv6 addresses into custom external network objects is also supported.

For more information, see [Hostname \(DNS Resolvable\) Network Objects](#) and [Custom External Network Objects](#).

## NAT information

NAT Information					
Access Rule	Original Packet			Translated Packet	
Name	Original Source	Original Destination	Original Service	Translated Source	Translated Destination
WAN-ADC-to-INTERNAL-ADC-IP	Internet 0.0.0.0/0, NOT 10.0.0.0/8, NOT 172...	ADC-WAN-EXTERNAL 62.99.0.42	Ref: HTTP+S , Ref: ICMP-UNLTD , ... ECHO , TCP 22, TCP 443, TCP 80	Dynamic SNAT Dynamic NAT	10.0.10.42
SSHDynamicAccess	Internet 0.0.0.0/0, NOT 10.0.0.0/8, NOT 172...	HQ-ISP1-PublicIP1 62.99.0.40	SSH TCP 22	Original	127.0.0.1
SSH-HQ-2-SRV	HQ-LAN 10.0.10.0/25	InternetSRV 214.51.2.80	SSH TCP 22	Dynamic SNAT Dynamic NAT	Original
SETUP-MGMT-ACCESS	Private IPv4 Addresses 10.0.0.0/8, 172.16.0.0/12, 192.168.0...	DHCP1 Local IP	NGF-MGMT-BOX ECHO , TCP 22, TCP 680, TCP 68...	Original	192.168.200.200

The NAT Information view allows you to see the NAT operations configured in the action and connection method of the access rules. To access the NAT view, click the  icon and select **Show NAT information**.

For more information, see [Firewall Rule List Interface and Icons](#).

## Bulk import for URL Filter policy objects

Block and allows lists for URL Filter policy objects can now be entered using bulk edit. This allows you to copy/paste a file containing a large number of domains without having to enter them individually.

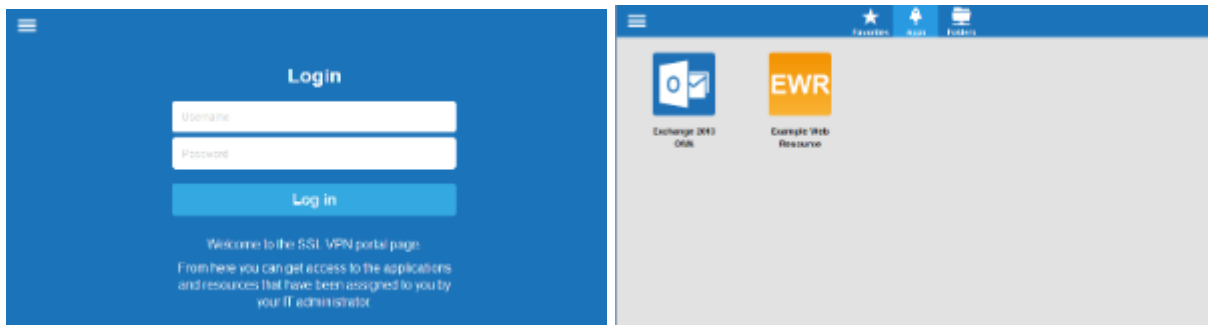
For more information, see [How to Create a URL Filter Policy Object](#).

## External logfile storage

You can now configure log cycling to move your logfiles to an external USB storage device attached to your firewall.

For more information, see [Log File Handling](#) and [How to Prepare External USB Storage for Log File Storage](#).

## SSL VPN web portal redesign



The web portal is redesigned to give desktop and mobile devices a single responsive interface. The web portal is designed to automatically display a version customized for the device type you are using.

For more information, see [SSL VPN User Interfaces](#).

### SSL VPN tunneled web apps

A tunneled web app uses an SSL tunnel established by CudaLaunch to connect to a web server behind the firewall. The user's browser connects to a localhost address (e.g., <http://localhost:5678>). A direct connection to the resource located behind the SSL VPN is then established through the SSL tunnel. This type of web app will only work as long as all links stay on the same destination host; it does not modify the data stream.

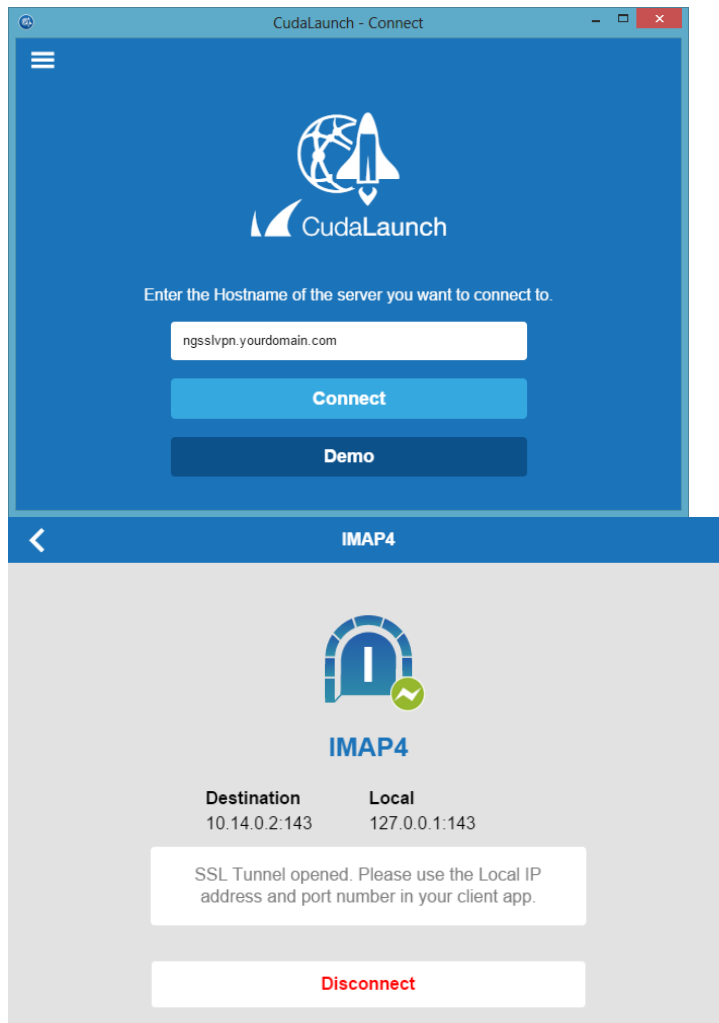
For more information, see [How to Configure a Tunneled Web App](#).

### SSL VPN Native Apps

Some tasks require the use of client-server applications. To connect with a service behind the SSL VPN service on the F-series Firewall, CudaLaunch establishes a secure tunnel and then automatically launches the locally installed application. The connection is terminated if the session is closed or times out.

For more information, see [SSL VPN Native Apps](#).

### CudaLaunch 2.0



CudaLaunch 2.0 for Windows, macOS, iOS, and Android is an update for the app that offers secure remote access to your organization's applications and data from mobile devices. CudaLaunch 2.0 now also supports **Generic Tunnels** and **Tunneled Web Apps**.

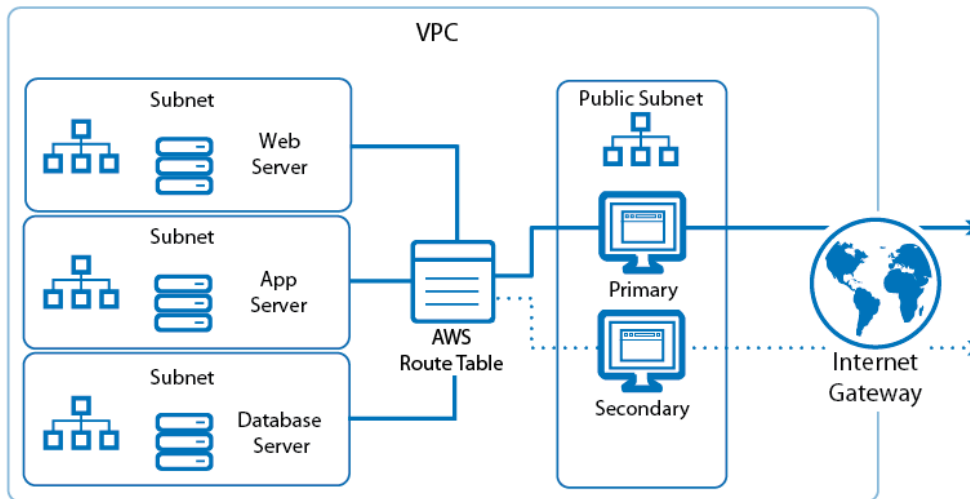
For more information, see [CudaLaunch](#).

### Retrieve PAR file during deployment using Azure and AWS CloudFormation templates

If you are using the NextGen Control Center either on-premises or in the cloud, you can modify your Azure or AWS CloudFormation templates to retrieve the PAR file for the new F-Series Firewall VM directly from the Control Center during deployment. The *getpar* script uses either CC admin credentials or a shared secret to authenticate. Licenses that are already installed on PAYG firewall Instances are pushed to the Control Center before retrieving the PAR file, whereas BYOL images use the licenses configured on the Control Center.

For more information, see [How to Modify Azure Templates to Retrieve the PAR File from a Control Center](#).

## High availability cluster in AWS



Deploy a Barracuda NextGen Firewall F-Series HA cluster in the Amazon AWS Cloud to ensure that your AWS resources are always available. Cloud Integration allows the firewall to rewrite the AWS route table to always use the active firewall instance. Incoming traffic can be directed to the active firewall by either Amazon Load Balancer for TCP connections or the DNS-based Route 53.

For more information, see [High Availability in AWS](#) and [How to Configure Cloud Integration for AWS](#).

## Azure Cloud Integration - IP Forwarding protection

Cloud Integration for F-Series Firewall and Control Center VMs allows the firewall to connect to the Azure service fabric and monitor and, if necessary, correct the **IP Forwarding** setting of the NIC attached to the VM.

For more information, see [How to Configure Azure Cloud Integration using ARM](#) and [How to Configure Azure Cloud Integration using ASM](#).

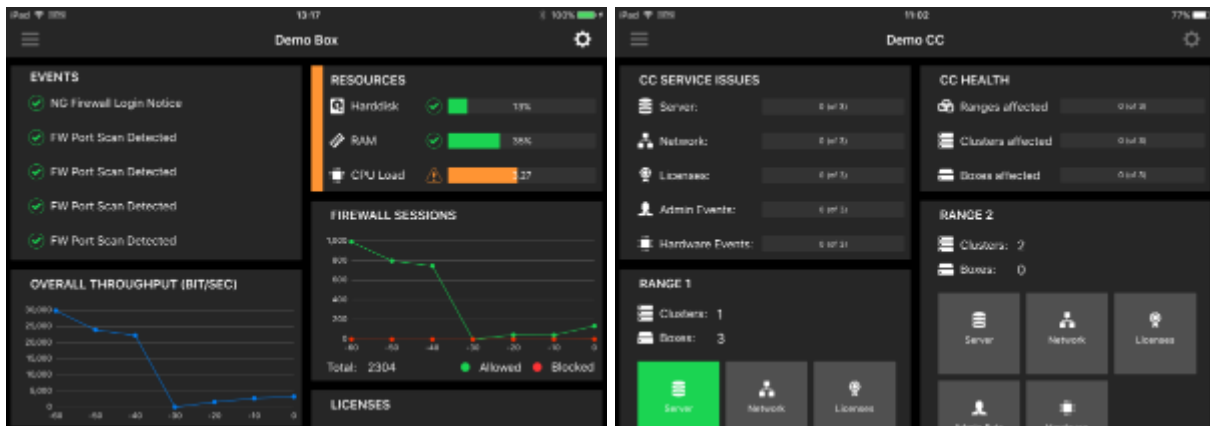
## Cloud information dashboard element

F-Series Firewalls deployed in Azure or AWS now display additional information in the cloud information element on the **General** tab of the dashboard.

For more information, see [DASHBOARD General Page](#).

## NextGen Remote





Barracuda NextGen Remote for Apple iOS provides system administrators easy remote access to their F-Series Firewalls and Control Centers through their iOS device. Barracuda NextGen Remote added support for push notifications for events.

For more information, see [Barracuda NextGen Remote](#).

#### UMTS/3G modem and link selection support for SC1

The NextGen Firewall SC1 now supports WAN connections using the Barracuda M11 3G/UMTS modem. Link selection allows you to configure a fallback connection for your Secure Connector. When the primary interface is down, traffic is routed over the backup interface to the Secure Access Concentrator. By default, the gateway of the interface is probed every five seconds, but you can also configure an explicit probing target.

For more information, see [FSC WAN Connections](#) and [FSC Link Selection](#).

## Improvements included in version 7.0.0 build 672

### RIP/OSPF/BGP

- Enabling OSPF by setting **Run OSPF Router** to **yes** on the **OSPF/RIP/BGP Settings** page now works as expected. (BNNGF-39115)

### VPN

- The VPN service now works as expected on F-Series Firewalls and Control Centers using 32-bit kernels: NextGen Firewall F10, F15, F100, F101, F200, F201, F300 and F301. (BNNGF-39297)
- IPsec IKEv1 tunnels using AES256 encryption and SHA256 hashing now work as expected. (BNNGF-39297, BNNGF-39295)

## Firewall

- Connection object failover and loadbalancing policies now work as expected when the first entry is a network interface. (BNNGF-39287)
- Application Control for SSL encrypted traffic now works as expected when used in combination with IPS and SSL Interception. (BNNGF-39221)
- Improvements to the IP defragmentation handling of acpftctrl monitor mode. (BNNGF-39394)

## Control Center

- NextGen Control Centers in Azure using the old VFC610 model names can now be updated. (BNNGF-39040)
- CC Database no longer causes problems logging in to the Control Center. (BNNGF-39285)

## Improvements included in version 7.0.0 build 664

---

### Barracuda NextGen Admin

- Redesigned the login screen. (BNNGF-23706)
- NextGen Admin now uses a native activation form instead of the browser based activation. (BNNGF-34151)
- Configuring VPN Firewall rulesets now works as expected. (BNNGF-38858)
- The **Message Board** is no longer missing an entry. (BNNGF-36584)
- Added **Shared Secret** input validation to check for invalid characters in the IPsec site-to-site configuration dialog. (BNNGF-37984)
- Added input validation to disallow pound signs ('#') in password fields. (BNNGF-37737)
- The firmware update element only shows updates for NextGen Admin newer than the currently used version. (BNNGF-35723)
- Improved the port speed indicator in the DASHBOARD > Port element, that, in some cases, showed incorrect information. (BNNGF-36663)
- Filtering for **IPS Severity** in the **FIREWALL > Monitor** now works as expected. (BNNGF-36469)
- Redesigned **Translation Map** configuration dialog. (BNNGF-37678)
- Redesigned **Connection object** configuration dialog and adjusted naming for **Translated Source IP** policies. (BNNGF-36639)
- NextGen Admin and the Report Creator now both round the risk rating number. (BNNGF-36765)
- Cloning a connection object with a reference to a network object now works as expected. (BNNGF-38459)

### Barracuda OS

- Changed help text to state that **Matched Domains** in the DNS Interception whitelist may not use special characters or wildcards. (BNNGF-36230)
- Monitoring routes with **Reachable IPs** now works as expected. (BNNGF-37128)

- Hardware pool licenses are now also valid for the direct predecessor of the model they are issued for. E.g., F80 pool licenses are also valid on F100/101. (BNNGF-37618)
- Updated 7zip to be able to extract v5 RAR files. (BNNGF-37391)
- Update packages are now detected correctly by the **Firmware Update** element. (BNNGF-36299)
- For freshly installed firewalls, the IPv6 routing cache is now set to the same value as the IPv4 routing cache. (BNNGF-38034)
- The primary firewall in a stand-alone high availability cluster now downloads the licenses for the secondary as expected. (BNNGF-24200)
- IPv6 autoconfig and DHCPv6 now works as expected for stateful and stateless configurations. (BNNGF-36634)
- CC admins can now log in via SSH when TACPLUS authentication is used. (BNNGF-37442)
- Removed hardware detection for **HG-S25** to reduce false positives when using standard hardware. (BNNGF-2870)
- The **Service User** is no longer mandatory in the **Advanced View** configuration of the **Administrative Settings**. (BNNGF-36300)
- Updated ixgbe.ko to version 4.3..13 module to fix issue after reboot. (BNNGF-38080)
- IP addresses where all four segments use 3 digits can now be entered via LCD. (BNNGF-29888)
- Added time zone for **America/Indiana**. (BNNGF-25727)
- VMware images now use **dynmod** as the default networking driver. (BNNGF-35781)
- Default keyboard layout for NextGen Install F installations set to **us**. (BNNGF-37159)

## Firewall

- Fixed race condition between the traffic shaping and routing subsystems. (BNNGF-38048)
- Creating a self-signed certificate in the Security Policy now works as expected. (BNNGF-38006)
- Sessions now sync correctly in an HA cluster between firewalls. (BNNGF-37024)
- The IPS now works as expected when scanning SSL Intercepted traffic. (BNNGF-35440)
- Safe Search for Yahoo over HTTP now works as expected. (BNNGF-29639)
- Improved URL categorization for SSL-intercepted hosts. (BNNGF-35450)
- SMTP and SMTPS connections can now use the **scan first, then deliver** option for ATD. (BNNGF-37129)
- The firewall no longer freezes in rare cases and requires a manual reboot. (BNNGF-36816)
- Configuring Traffic Shaping in the GTI Editor with the **shape on output interface** option now works as expected. (BNNGF-36548)
- Added support to scan HTTP and HTTPS connections using chunked transfer encoding. The **Stream Scanning Buffer** can be configured in the **Advanced Virus Scanner Settings** on the **Security Policy** page. (BNNGF-37938)
- In rare cases **Block Other Session Limit Exceeded** would occur for non-TCP traffic without having exceeded the limit. This is now handled correctly. (BNNGF-36808)
- SMTPS on port 465 is no longer scanned if virus scanning for SMTP/SMTPS is disabled. (BNNGF-36953)
- The feature level of the firewall service is now limited to the cluster version instead of the firmware version of the Control Center. (BNNGF-38254)
- URL Filter block pages are no longer partially delivered. (BNNGF-35578)
- Added support for IPv6 hostname network objects. (BNNGF-35070)

- SSL Interception with certificates chains now works as expected. (BNNGF-38655)
- FWD Firewall statistics now work as expected. (BNNGF-36005)
- IPv6 rulesets using network objects with references now work as expected. (BNNGF-37111)
- The skinny plugin now works with Cisco Call Manager. (BNNGF-32217)
- IPS now logs the correct **action state** in the threat log. (BNNGF-34323)
- SMTPS added to **Any-Email** service object. (BNNGF-34998)
- Guest ticketing now supports setting a maximum time limit for guest tickets. Ticketing admins cannot create tickets exceeding this limit. (BNNGF-35797)
- Resolving a large number of hostname network objects now works as expected. (BNNGF-35963)
- File Content policy now detects HTML5 video content (BNNGF-37277)
- acpfcrl monitoring now works as expected. (BNNGF-36754)

## RIP/OSPF/BGP

- Improved interface state changes detection. (BNNGF-37510)
- It is now possible to use global network objects in the **BGP Router Setup**. (BNNGF-37095)
- To enable repository linked RIP/OSPF/BGP configurations, neighbor configurations where AS equals the router AS are ignored. (BNNGF-37091)
- Handling for OSPF/RIP/BGP routes improved. (BNNGF-37374)

## VPN

- Terminating and initiating a TINA tunnel using **Null** cipher with **PFS** now works as expected. (BNNGF-38310)
- The VPN hub now correctly detects if the remote VPN service is restarted and automatically removes the dynamic tunnels. (BNNGF-35968)
- VPN service no longer crashes if the IPsec key length is not set correctly. (BNNGF-37133)

## HTTP Proxy

- Update squid to version 3.5.19 due to the following security vulnerabilities: CVE-2016-4555, CVE-2016-4556, CVE-2016-4554, CVE-2016-4553 and SQUID-2016:3+4+5+6 (BNNGF-37828, BNNGF-38384, BNNGF-36855)
- The default deny-all ACL is now also applied to the reverse proxy. (BNNGF-30773)
- Statistics for HTTP Proxy now use correct destination entries. (BNNGF-36962)
- URL Filtering in the HTTP Proxy now works as expected. (BNNGF-36963)
- The virus scanning block page now shows correct URL for FTP over HTTP Proxy connections. (BNNGF-38910)
- Added **no-digest** to the backend configuration for the reverse proxy. (BNNGF-36566)

## Azure / AWS

- The Azure UDR daemon no longer crashes on system shutdown. (BNNGF-36856)
- Added IPsec to the default App Redirect rule for the VPN service. (BNNGF-37548)
- PAYG licenses now include the HTTP Proxy. (BNNGF-35742)
- If **IP Forwarding** is disabled, the status icon for the firewall routes in the **Azure UDR** tab are changed to red. (BNNGF-36970)

- Setting a root password using extended ASCII characters during deployment now works as expected. (BNNGF-35994)

## Control Center

- The configurations in the Set area config on the **File Updates** configurations are now included in the archive.PAR file. (BNNGF-29061)
- Deleting a range with a Secure Access Concentrator now also deletes the corresponding SC VIP network. (BNNGF-38563)
- RCS changelog messages now allow the "-" character. (BNNGF-37119)
- When removing a SC1 from a template, it no longer disappears from the Status Map. (BNNGF-37616)
- Added Azure Control Center VCC400 model. (BNNGF-36985)
- It is no longer possible to add blank entries to the **Additional CC IP addresses** list. (BNNGF-37952)

## Virus Scanner and ATD

- Added support to scan RTF files with ATD. (BNNGF-38150)
- Files using HTTP content type of chunked encoding are now scanned by the virus scanner and ATD. (BNNGF-37692)
- Infected mail attachments are now stored in the quarantine folder on the firewall. (BNNGF-37336)
- Mail subject is now shown on the **FIREWALL > ATD** page. (BNNGF-37148)
- Added PUA configuration option for ClamAV virus scanning engine with exceptions for win32packer and Block OLE2 Macros. (BNNGF-37177)
- Improved handling of multi-volume RAR files. (BNNGF-37427)

## SSL VPN

- Reworked the help text displayed in NextGen Admin to make it more informative. (BNNGS-2078)
- Ensure that VPN configuration files delivered to iOS9.3 clients do not have an empty **localidentifier** field. (BNNGS-2082)
- Allow the password field on the login page to be clicked into correctly in Internet Explorer. (BNNGS-2044)
- Fixed issue where long URLs in web forwards can crash the SSL VPN service. (BNNGS-1931)
- Add user defined attributes to all resource types, rather than just Web Apps. (BNNGS-1926)
- Allow Custom Icons to be associated with all resource types. (BNNGS-1898)
- Allow Dynamic App Control rules to be activated/deactivated via SSL VPN. (BNNGS-1882)
- Re-structured resource pages in NextGen Admin. (BNNGS-1774)
- Change the NextGen Admin setting **Enable Mobile App** to **Enable CudaLaunch**. (BNNGS-1668)
- Removed Text area and check box attribute types. (BNNGS-1553)
- Internationalized the **License Exceeded** and other error messages returned from the SSL VPN service. (BNNGS-1546)

- Fixed issues in web forward single sign-on where timeouts used in the JavaScript sign on mechanism were not working correctly. (BNNGS-1543)
- Improvements to the OWA web forward template. It now no longer sporadically fails to connect to the server. (BNNGS-1542)
- Removed the **Deny Auto Complete** option from NextGen Admin because this functionality is no longer supported by modern browsers. (BNNGS-1539)
- Renamed all references to **VPN Profiles** to be **VPN Group Policies**. (BNNGS-1525)
- Fixed issue where the Access Control Service was sometimes unable to connect to the Policy Server. (BNNGS-1493)
- Fixed issue where specifying an invalid host on application resource would cause the service to restart. (BNNGS-1470)
- Removed the cache cleaner functionality from NextGen Admin because this was no longer supported on modern browsers. (BNNGS-1352)
- Fixed issue with the configuration of NAC exceptions not working on a Control Center. (BNNGS-1121)

## DHCP-Relay

- The **Relay Interface** list now shows the correct port names. (BNNGF-37057)

## DHCP Server

- Added options for PXE boot in **Basic View** mode. (BNNGF-37516)

## Wi-Fi

- Setting the **Wi-Fi bit rate** manually no longer results in poor throughput. (BNNGF-38395)

## Issues resolved by hotfixes

---

The following hotfixes have been released for firmware version 7.0.0

### Hotfix 848 - KRACK Attack

- Security fix for the WPA2 vulnerability.

## Known issues

---

### 7.0.0

- URL Filter: It is not possible to establish WebEx sessions when the URL Filter is enabled on the matching access rule.



- IPsec IKEv1 IPv6: It is not possible to use hostnames as the remote gateway.
- IPsec IKEv1 IPv6: It is not possible to use a dynamic local gateway.
- IPsec IKEv2: It is not possible to establish a VPN tunnel if the active partner uses a dynamic IP address.
- IPsec IKEv2: When using a dynamic local gateway NAT Traversal is not possible.
- TINA IPv6: It is not possible to use proxies for TINA VPN tunnels using IPv6.
- SSH: There is no sshd listener for IPv6 management IP addresses.
- NextGen Admin: IPv6 listeners are not displayed in the **Info** dialog on the **CONTROL > Resources** page.
- NextGen Admin: The activation dialog only accepts: A-Z, a-z, 0-9 and spaces.
- 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**.
- SSL VPN Network Places: Some modern browsers such as Chrome and Firefox no longer support Java applets. Instead, use browsers with Java applet support, such as Internet Explorer or Safari.

## Miscellaneous

- VMware: Network interfaces using the VMXNET3 driver do not send IPsec keep alive packets unless TX checksumming is disabled for the interface (ethtool -K INTERFACE tx off).
- URL Filter: F-Series Firewalls running 6.2.0 or higher that are managed by a Control Center using firmware 6.0.X or 6.1.X must complete a dummy change in the security policy whenever enabling/disabling the URL Filter in the **General Firewall Settings**.
- 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.
- IKEv2: Disabling a site-to-site tunnel on the **VPN > Site-to-Site** page is not possible.
- IKEv2: Changing a setting for an IKEv2 tunnel disabled in the configuration causes all active IKEv2 tunnels to initiate a re-keying.
- IKEv2: Client certificate authentication for client-to-site IKEv2 IPsec VPNs requires **X509 Certificate** to be enabled in the **VPN Settings**. Enabling this setting requires all VPN group policies to use client certificate authentication.
- IKEv2: After a restart, the **Last Access** and **Last Duration** time displayed for site-to-site IKEv2 IPsec tunnels is not reset.
- IKEv2: Using a hostname or subnets as **Remote Gateway** is currently not possible.
- IKEv2: Using pre-shared keys with IKEv2 client-to-site VPNs is not possible.
- IKEv2: Using X509 Subject Policy in a client-to-site **Group VPN Settings** is not possible.
- IKEv2: Changing client-to-site minimum and maximum lifetime values has no effect.
- IKEv2: Connecting to an IKEv2 IPsec client-to-site VPN using iOS or Android devices is not possible.
- Azure Control Center: On first boot "fatal" log messages may occur because master.conf is missing. These log messages can be ignored.
- IKEv1 IPsec: When using 0.0.0.0 as a local IKE gateway, you must enable **Use IPsec Dynamic IPs** and restart the VPN service before a listener on 0.0.0.0 is created.
- HTTP Proxy: Custom block pages do not work for the HTTP Proxy when running on the same NextGen F-Series Firewall as the Firewall service. This issue does not occur when running the

HTTP Proxy service on a second NextGen F-Series Firewall behind the NextGen F-Series Firewall running the Firewall service.

- SSL VPN: Favorites are not included in the PAR file.
- SSL VPN: Text fields do not accept the # character.
- SSL VPN: User Attributes do not support UTF-8.
- SSL VPN: The allowed host filter path must be unique.
- Safe Search: In some cases, YouTube safety mode does not work when logged in with a Google account.
- Safe Search: If Safe Search is enabled, it is not possible to log into YouTube when cookies are disabled.
- 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.
- VPN Routing: Creating a direct or gateway route with the same metric and destination as a VPN route in the main routing table results in duplicate routes. The route added last is used.
- HTTP Proxy: **Custom Cipher String** and **Allow SSLv3** settings only apply to reverse proxy configurations.
- CC Wizard: The CC Wizard is currently not supported for Control Centers deployed using Barracuda F-Series Install.
- ATD: Only the first URL in the Quarantine Tab that leads to a quarantine entry is displayed, even if the User and/or IP address downloaded more than one infected file. This can be dangerous if the first downloaded file is a false-positive.
- Barracuda OS: **Provider DNS** option for DHCP connections created with the box wizard must be enabled manually.
- Terminal Server Agent: It is not currently possible to assign connections to Windows networks shares to the actual user.
- Firmware Update: Log messages similar to WARNING:  
/lib/modules/2.6.38.7-9ph5.4.3.06.x86\_64/kernel/drivers/net/wireless/zd1211rw/zd1211rw.ko needs unknown symbol ieee80211\_free\_hw may appear while updating, but can be ignored.
- **Attention:** Amazon AWS/Microsoft Azure: Performing **Copy from Default** of Forwarding Firewall rules currently locks out administrators from the unit and requires a fresh installation of the system.
- Application Control and Virus Scanning: Data trickling is only done while the file is downloaded, but not during the virus scan. This may result in browser timeouts while downloading very large files.
- Application Control and Virus Scanning: If the Content-Length field in HTTP headers is missing or invalid, the **Large File Policy** may be ignored.
- Application Control and Virus Scanning: In very rare cases, if the SSL Interception process is not running, but the option **Action if Virus Scanner is unavailable** is set to **Fail Close**, a small amount of traffic may already have passed through the firewall.
- Application Control and Virus Scanning: In rare cases, Google Play updates are sometimes delivered as partial updates. These partial updates cannot be extracted and are blocked by the virus scanning engine. The engine reports **The archive couldn't be scanned completely**. Either create a dedicated firewall rule that does not scan Google Play traffic, or set **Block on Other Error** in **Avira Archive Scanning** to **No**.



- Barracuda OS: Restoring units in default configuration with par files created on a Control Center may result in a corrupt virtual server. Instead, copy the par file to *opt/phion/update/box.par* and reboot the unit.

## Figures

1. s\_to\_s\_c\_to\_s\_IPv6\_VPN.png
2. dns\_sinkhole\_02.png
3. isp\_src\_hash.png
4. update\_element\_03.png
5. NAT\_view.png
6. modify.png
7. web02.png
8. web01.png
9. cudalaunch\_dt\_01.png
10. cudalaunch\_dt\_08.png
11. aws\_vpc\_multitier\_ha-01.png
12. status\_fw.png
13. demo\_cc\_01.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.