Release Notes 7.1.X

https://campus.barracuda.com/doc/50659991/

Before you Begin

Before updating, back up your configuration and read through the release notes for all versions more current than the version you are currently running on your firewall.

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 10 minutes. If the process takes longer, please contact Barracuda Networks Technical Support for further assistance.

Due to most modern browsers removing SSL VPN Java applet support CudaLaunch is required to retain SSL VPN functionality previously handled via Java applets. An **additional Remote Access Premium subscription is required**. By default a one-user demo license for CudaLaunch is included.
For more information, see How to Configure a Tunneled Web Forward and SSL VPN Applications.

What's new in Barracuda NextGen Firewall X-Series Version 7.1.5

Barracuda NextGen Firewall X-Series version 7.1.5 is a maintenance release and contains no new features.

Firmware Improvements

- Sessions with certain invalid combinations of TCP flags are dropped to avoid false-positive security scans. BNF-7005
- HTTP headers now have the value "X-Content-Type-Options" set correctly in the response. BNF-6946

What's new in Barracuda NextGen Firewall X-Series Version 7.1.4

Barracuda NextGen Firewall X-Series version 7.1.4 is a maintenance release and contains no new features.

Firmware Improvements

- High severity vulnerability: incorrect initialization logic of RAR decoder objects (CVE-2018-10115) has been fixed. BNF-6921
- Low severity vulnerability: log entries/templates are now encoded to protect from code injection/XSS attacks. BNF-6887
- Low severity vulnerability: fields of certificates loaded via the certificate manager are now encoded to protect from code injection/XSS attacks. BNF-6885
- TLS protocol version and cipher specifications of the user interface are now configurable. BNF-6861
- The Application Monitor now works as expected and no longer reports errors. BNF-6861

What's new in Barracuda NextGen Firewall X-Series Version 7.1.3.008

Barracuda NextGen Firewall X-Series version 7.1.3.008 is a maintenance release and contains no new features.

Firmware Improvements

- The security issue to protect against the WPA2 vulnerability (KRACK attack) has been resolved. BNF-6862

What's new in Barracuda NextGen Firewall X-Series Version 7.1.3.009

Barracuda NextGen Firewall X-Series version 7.1.3.009 is a maintenance release and contains no new features.

Firmware Improvements

- Logging in using the recovery console now works as expected. BNF-6875

What's new in Barracuda NextGen Firewall X-Series Version 7.1.3.008

Barracuda NextGen Firewall X-Series version 7.1.3.008 is a maintenance release and contains no new features.

Firmware Improvements

- The security issue to protect against the WPA2 vulnerability (KRACK attack) has been

resolved. BNF-6862
- SSL VPN is now providing certificate chain as expected. BNF-6675
- Creating a user exception for the DC agent authentication is now creating a group filter pattern. BNF-6754
- OpenSSL has been updated to support version 7.1.3. BNF-6755
- Adding more than one Google account now works as expected. BNF-6760
- Adding a static IP to the VPN > PPTP settings now works as expected. BNF-6763
- Certificates can now be removed when SSL interception and the used certificate is set to no/none. BNF-6764
- Displaying objects in FIREWALL > Application Objects > Add List Based Application Objects now works as expected. BNF-6770
- Setting the service defaults for FIREWALL > Access Rules now works as expected. BNF-6792
- Creating and editing a Service Object now works as expected. BNF-6800
- The Protect My Network wizard now accepts only lower case letters. BNF-6804
- Copying an application block rule now works as expected. BNF-6816
- FIREWALL > Application Objects now accept only unique naming. BNF-6819
- The table of Recent Connections now displays allowed connections as expected. BNF-6823
- HA syncing between two firewalls does not affect the machine ID any more. BNF-6827
- Service filter is now working as expected. BNF-6852

What's new in Barracuda NextGen Firewall X-Series Version 7.1.2.005

Barracuda NextGen Firewall X-Series version 7.1.2.005 is a maintenance release and contains no new features.

- Google discontinued YouTube for Schools on July 1, 2016. With firmware version 7.1.2.005, the NextGen Firewall X removed all user interface elements related to this feature.
- Barracuda recommends to update all firewalls shipped after January 2017 to firmware version 7.1.2.005. The update solves an issue with non existing SSL VPN templates.

Firmware Improvements

- The wildcard user group ' * ', is now the default access group policy for CudaLaunch client-to-site connections. (BNF-6693)
- The newly introduced Premium Remote Access subscriptions are now correctly displayed on the Dashboard of models X50, X51, X100, and X101. (BNF-6758)
- The Basic Setup wizard no longer stalls upon product activation. (BNF-6761)
- Filtering for unknown applications in the Application Monitor no longer returns a server error message. (BNF-6738)
- Configuration elements **Visible Name** and **CudaLaunch Server** are now mandatory information when adding a Access Policy for CudaLauch. (BNF-6725)

- A missing configuration setting was added to allow proper configuration of the File Content scan feature. (BNF-6707)
- MSAD connectivity tests no longer use an invalid port with SSL enabled. (BNF-6686)
- Email notifications for changes in the routing table are now correctly triggered. (BNF-6674)
- WiFi Access Point IP addresses are no longer available as VPN server IP addresses in the Remote Access Gateway wizard. (BNF-6658)
- Filtering for log files in LOGS > Firewall Log now works as expected. (BNF-6624)

What's new in Barracuda NextGen Firewall X-Series Version 7.1.1.010

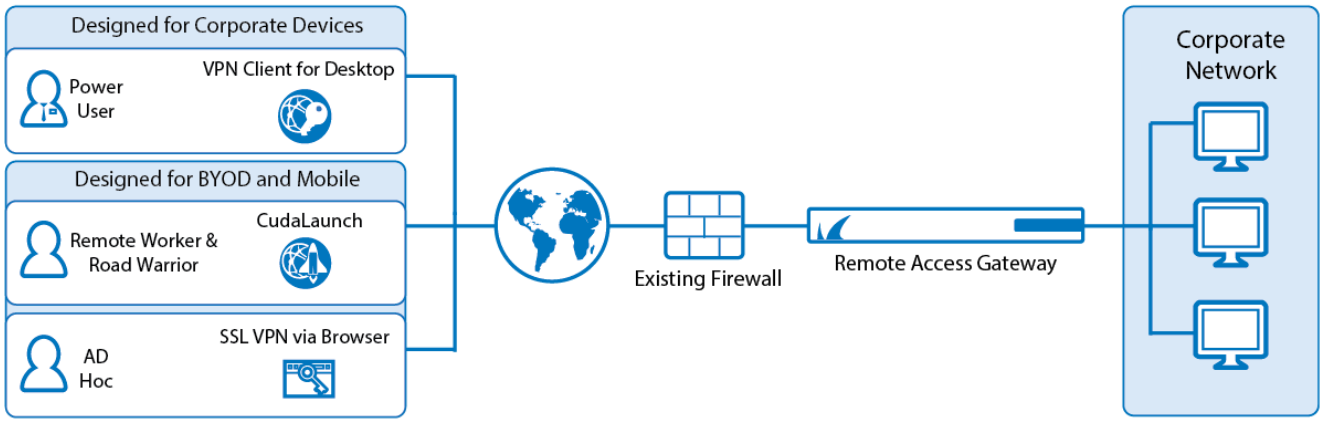
Barracuda NextGen Firewall X-Series version 7.1.1.010 is a maintenance release and contains no new features.

Firmware Improvements

- Updated bind to version 9.9.9-P4 to fix security vulnerability CVE-2016-8864. (BNF-6696)

What's new in Barracuda NextGen Firewall X-Series Version 7.1.1.008

Remote Access Gateway wizard



You can now deploy your X-Series Firewall as a remote access gateway behind your border firewall. This allows you to leverage the remote connectivity options offered by the SSL VPN and client-to-site VPN services on the X-Series Firewall to offer easy remote connectivity for all your users. The remote access gateway wizard can be launched separately or during the deployment.

For more information, see Getting Started and Deploy as Remote Access Gateway.

Firmware Improvements

- The **Top 10 Application** element now works as expected. (BNF-6583)
- Health checks for a DNS record in the **Authoritative DNS** service now work as expected. (BNF-6595)
- The **Autostart wizard** is now started automatically after the basic setup wizard. (BNF-6609)
- Checking for duplicate certificate names by the **Certificate Manger** is now case insensitive. (BNF-6628)

What's new in Barracuda NextGen Firewall X-Series Version 7.1.0.017

Barracuda NextGen Firewall X-Series version 7.1.0.017 is a maintenance release and contains no new features.

Firmware Improvements

- OpenSSL update to resolve security vulnerability CVE-2016-6304. (BNF-6644)

What's new in Barracuda NextGen Firewall X-Series Version 7.1.0.013

Barracuda NextGen Firewall X-Series version 7.1.0.013 is a maintenance release and contains no new features.

Firmware Improvements

- Multiple SSL VPN improvements. (BNF-6591)
- Virus Scanner and ATP startup improvements. (BNF-6579)

What's new in Barracuda NextGen Firewall X-Series Version 7.1.0.008

Barracuda NextGen Firewall X-Series version 7.1.0.008 is a maintenance release and contains no new features.

Firmware Improvements

- Site-to-site VPN tunnel stability improvements. (BNF-6570)

What's new in Barracuda NextGen Firewall X-Series Version 7.1.0.007

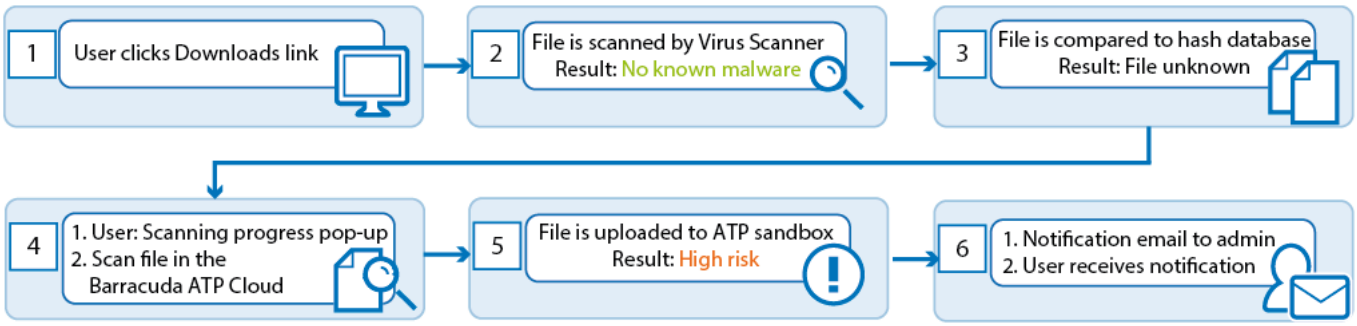
Barracuda NextGen Firewall X-Series version 7.1.0.007 is a maintenance release and contains no new features.

Firmware Improvements

- IPsec client-to-site VPN tunnel rekeying now works as expected. (BNF-6565)

What's new in Barracuda NextGen Firewall X-Series Version 7.1.0.006

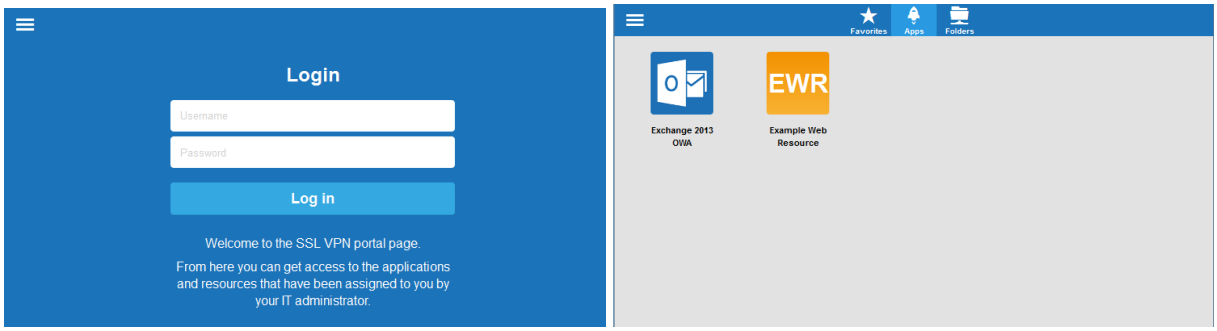
Advanced Threat Protection (ATP)



Advanced Threat Protection offers protection against advanced malware, zero-day exploits, and targeted attacks that are not detected by the virus scanner or intrusion prevention system. ATP analyzes files in the Barracuda ATP cloud and assigns a risk score. Local ATP policies then determine how files with a high, medium, or low risk score are handled. You can configure administrator email notifications and/or enable one of the automatic blacklisting policies. To check local files, you also have the option to manually upload a file via the management web interface.

For more information, see Advanced Threat Protection (ATP/ATD)

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 Forward

A tunneled web forward 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 forward will only work as long as all links stay on the same destination host; it does not modify the data stream.

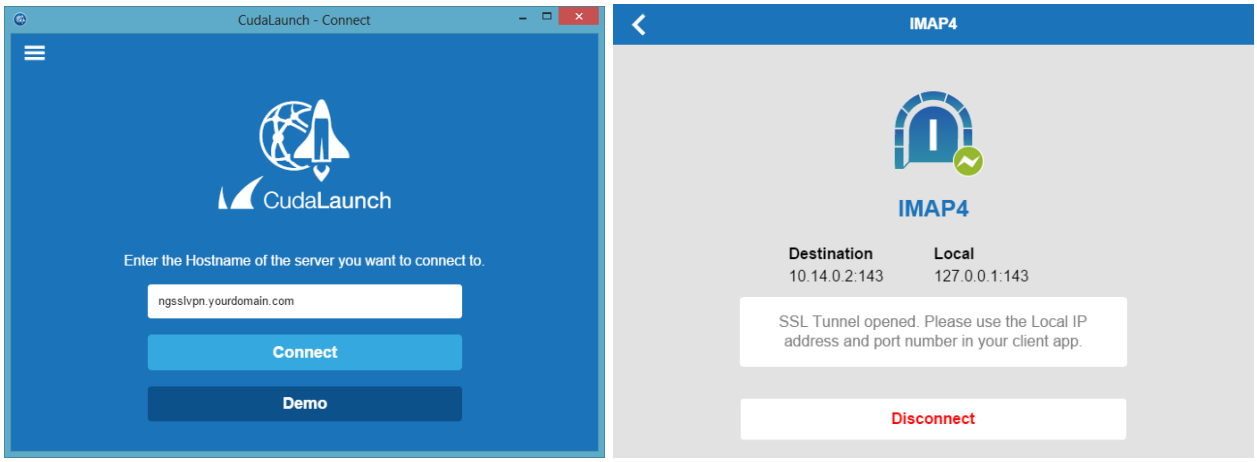
For more information, see How to Configure a Tunneled Web Forward.

SSL VPN Applications

Some tasks require the use of client-server applications. To connect with a service behind the SSL VPN service on the X-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 Applications.

CudaLaunch 2.0



CudaLaunch 2.0 for iOS, Android, and now also for Windows and macOS 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 **SSL Tunnels** and **SSL VPN Applications**.

For more information, see CudaLaunch.

Firmware Improvements

- Time stamps on the **BASIC > Alerts** page now match the configured time zone settings. (BNF-6143)
- Improved filtering on the **LOGS > Firewall Log** page. (BNF-6343, BNF-6344, BNF-6481)
- Entering IP addresses in the failover and load balancing settings of a custom connection object is now possible. (BNF-6359)
- Incoming NetBIOS traffic is no longer allowed on WAN interfaces. (BNF-6407)
- The virus scanning block page now shows the correct URL for FTP over HTTP Proxy connections. (BNF-6465)
- SSL Interception with certificate chains now works as expected. (BNF-6466)
- The virus scanner result cache is now cleared after a virus pattern update. (BNF-6468)
- Manually setting the **bit rate** for the Wi-Fi interface no longer results in poor bandwidth.
- Improved URL categorization for SSL-intercepted hosts. (BNF-6474)
- Editing the custom block page for the virus scanner now works as expected. (BNF-6480)
- The **BASIC > Status** page no longer fails if the firewall has an uptime of more than a year. (BNF-6488)
- Tool tips on the **BASIC > Status** pages now display the time correctly when set to auto refresh. (BNF-6130)
- It is now possible to filter for **Scan Exception** on the **BASIC > Recent Threat** page. (BNF-6298)
- You can now add a filter on the **LOGS > Firewall Log** page by clicking on the mouse-over magnifying glass icon next to the value you want to filter for. (BNF-6378)

Migration Instructions

Due to most modern browsers removing SSL VPN Java applet support CudaLaunch is required to retain SSL VPN functionality previously handled via Java applets. An **additional Remote Access Premium subscription is required**. By default a one-user demo license for CudaLaunch is included.
For more information, see How to Configure a Tunneled Web Forward and SSL VPN Applications.

- Support for webDAV SSL VPN resources is discontinued and is no longer available after updating.

Known Issues

- IPsec client-to-site connections using the Android 6.0 and 6.1 native IPsec client are not possible. As a work-around, you can use CudaLaunch instead. CudaLaunch requires a Remote Access Premium subscription.
- Only first DNS and WINS servers are used for client-to-site tunnels.
- Barracuda Report Creator is only available for Microsoft Windows 7, 8, and 10.
- HA boxes in Barracuda Cloud Control are not read-only.
- Virus scanning requires TCP Stream Reassembly to be enabled. The product will automatically do this when switching on Malware Protection.

Figures

1. ra_wizard.png
2. atp_scan_then_deliver.png
3. web02.png
4. web01.png
5. cudalaunch_dt_01.png
6. cudalaunch_dt_08.png

© Barracuda Networks Inc., 2020 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.