Release Notes 7.0.X

https://campus.barracuda.com/doc/49054879/

Please Read Before Upgrading

Before installing the new firmware version, back up your configuration and read all of the release notes that apply to the versions that are more current than the version that is running on your system.

Do not manually reboot your system at any time while the update is in process, unless otherwise instructed by Barracuda Networks Technical Support. Depending on your current firmware version and other system factors, upgrading can take up to 10 minutes. If the process takes longer, please contact Barracuda Networks Technical Support for further assistance.

What's New in Barracuda NextGen Firewall X-Series Version 7.0.1.005

Barracuda NextGen Firewall X-Series version 7.0.1.005 is a maintenance release and contains no new features.

Firmware Improvements

- Fixed a rare case where configuring access rules caused an error in the WebUI. (BNF-6494)
- Improvements to active and recent connections pages. (BNF-6494)

What's New in Barracuda NextGen Firewall X-Series Version 7.0.0.010

Barracuda NextGen Firewall X-Series version 7.0.0.010 is a maintenance release and contains no new features.

Firmware Improvements

- Updated OpenSSL to fix the following security vulnerabilities:
  CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2109, CVE-2016-2176 (BNF-6413)

What's New in Barracuda NextGen Firewall X-Series Version 7.0.0.008

Barracuda NextGen Firewall X-Series version 7.0.0.008 is a maintenance release and contains no new features.

Firmware Improvements

- Creating log filters with empty values no longer breaks the LOG page. (BNF-6492)

What's New in Barracuda NextGen Firewall X-Series Version 7.0.0.006

Barracuda NextGen Firewall X-Series version 7.0.0.006 is a maintenance release and contains no new features.

Firmware Improvements

- Restoring from a cloud backup now works as expected. (BNF-6340)

Known Issues

- Client-to-site VPN connections currently only use the first DNS and WINS server.
- The Barracuda Report Creator is available only for Microsoft Windows 7, 8, and 10.
- The secondary firewall in an HA cluster is not read-only when accessing the configuration through Barracuda Cloud Control.

What's New in Barracuda NextGen Firewall X-Series Version 7.0.0.005

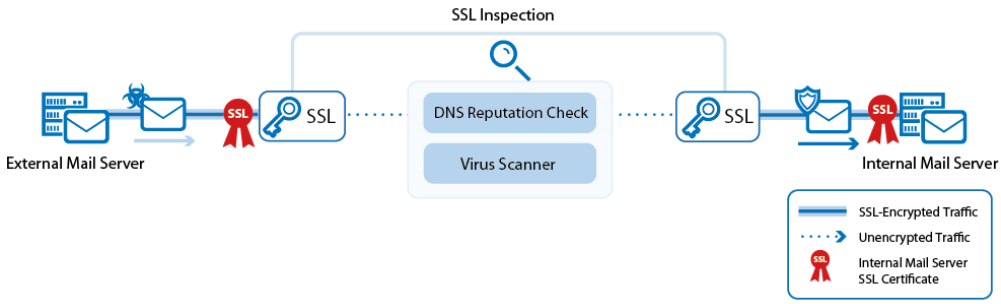
Barracuda NextGen Firewall X-Series version 7.0.0.005 is a maintenance release and contains no new features.

Firmware Improvements

- Increased firewall engine stability. (BNF-6348)

What's New in Barracuda NextGen Firewall X-Series Version 7.0.0.004

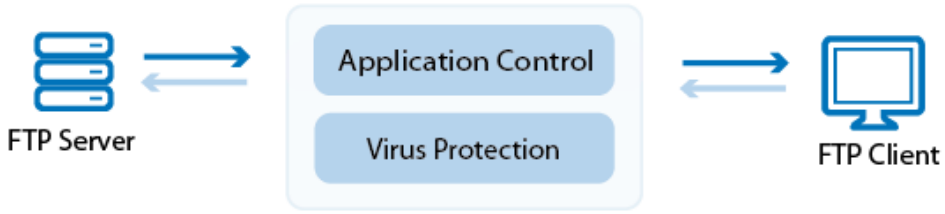
Mail Security in the Firewall



The X-Series Firewall enforces mail security in the firewall by transparently scanning incoming and outgoing SMTP and SMTPS connections for malware and by checking the reputation of the sender's IP address via a DNS blacklist (DNSBL).

For more information, see Mail Security in the Firewall and Virus Protection in the Firewall.

Virus Protection for FTP in the Firewall



The X-Series Firewall can transparently scan FTP traffic passing through the Forwarding Firewall service for malware. If malware is detected, the file is discarded and the file transfer is terminated.

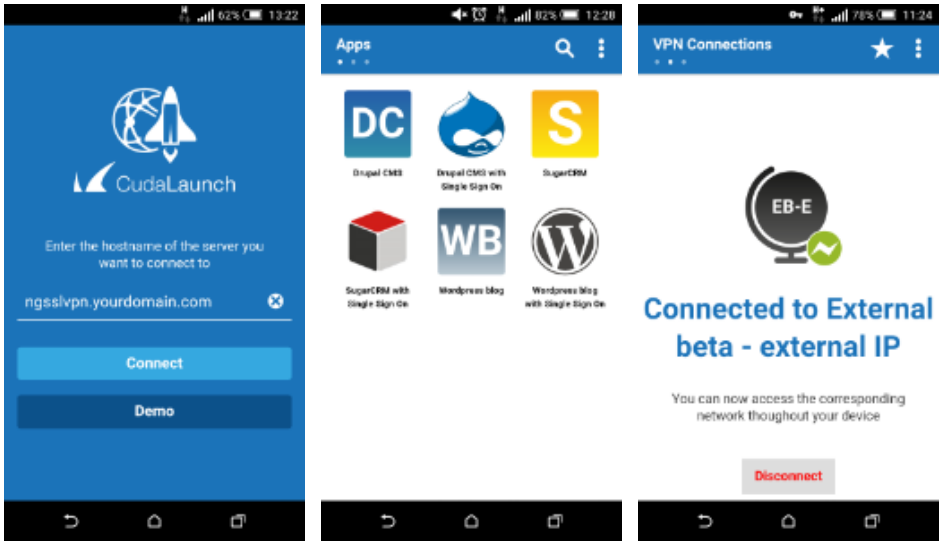
For more information, see Virus Protection in the Firewall and How to Configure Virus Scanning in the Firewall for FTP Traffic.

DHCP Relay

DHCP relaying allows you to share a single DHCP server across logical network segments that are separated by the firewall.

For more information, see How to Configure a DHCP Relay.

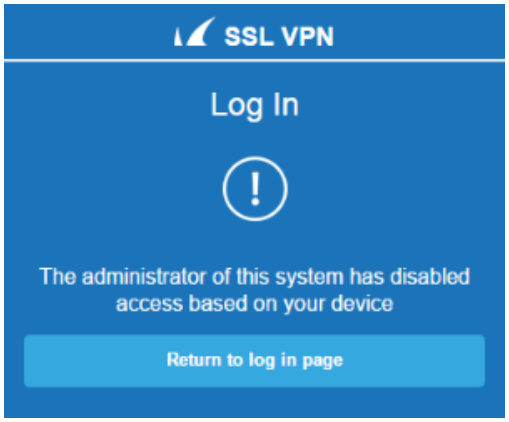
CudaLaunch



CudaLaunch offers secure remote access to your organization's applications and data from mobile devices. CudaLaunch is available for iOS and Android devices via the Apple App Store or Google Play Store. Both versions offer the same functionality. Full Device VPN uses the same VPN group policy.

For more information, see CudaLaunch.

NAC for SSL VPN



SSL VPN Network Access Control (NAC) limits access to the web portals of the SSL VPN service according to a variety of factors that are not connected to the user. Users who fail the NAC check are not allowed to log in until they have a conforming system.

For more information, see How to Configure NAC for SSL VPN.

SSL VPN Web Forwards Improvements

Create web forwards to allow SSL VPN users to access web-based internal applications. There are predefined web forward types for Outlook Web Access and SharePoint servers as well as generic settings that allow you full control over how the web content is rewritten.

For more information, see How to Configure an Outlook Web Access Web Forward, How to Configure a SharePoint Web Forward, and How to Configure a Generic Web Forward.

SSL VPN User Attributes

User attributes are placeholder variables used to personalize web forwards or to configure single sign-on authentication. They are created by the admin and filled in by the end user in either the desktop or mobile portal.

For more information, see How to Use and Create Attributes.

Single Sign-On for Web Forwards

Web forwards can be configured to automatically log the user in when accessing web forwards requiring authentication. Both HTTP and form-based (POST, GET, and JavaScript) authentication is supported. User attributes allow you to use different user credentials than those used to log into the SSL VPN to authenticate to a web application made available as a web forward.

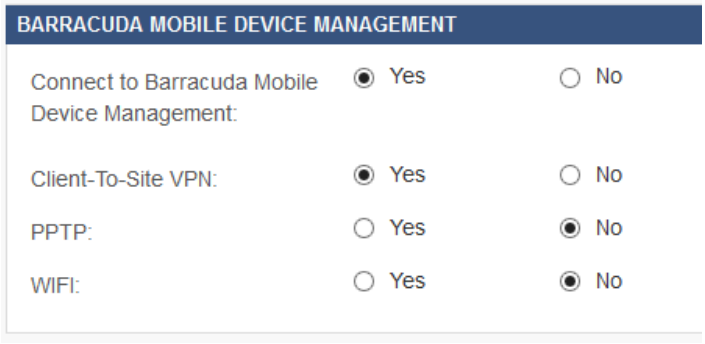
For more information, see How to Configure Single Sign-On for Web Forwards.

SSL VPN Self-Provisioning for VPN Templates

The SSL VPN service allows end users to self-provision their VPN client on Windows, macOS, or iOS devices. To automatically download and install the configuration, the user must log into one of the SSL VPN portals and click the VPN Template provisioning link. VPN templates are created as a part of the client-to-site VPN configuration.

For more information, see How to Configure VPN Templates in the SSL VPN.

Barracuda Mobile Device Manager BETA



The Barracuda Firewall now supports connecting to the Barracuda MDM using your Barracuda Cloud Control account. Configurations for Client-to-site VPN, PPTP and Wi-Fi connections can be pushed to your MDM managed mobile phones. This is a beta feature and should not be used in a production environment. MDM support is enabled on the **BASIC > Cloud Control** page.

For more information, see Barracuda Mobile Device Manager.

Firmware Improvements

- Disabling IPS in an access rule is now displayed correctly in the access rule list. (BNF-6068)
- Disabling a Wi-Fi access no longer requires you to enter a passphrase. (BNF-6041)
- Generating certificates on smaller appliances no longer times out. (BNF-6039)
- Removing VPN certificates now works as expected. (BNF-5994)
- Restoring a backup to a unit with a different serial number now works as expected. (BNF-5987)
- Deleting entries with capital letters in the Authoritative DNS configuration now works as expected. (BNF-5889)
- Management web interface now uses the following cipher string: **HIGH:!aECDH:!ADH:!3DES:!MD5:!DSS:!RC4:!EXP:!eNULL:!NULL:!aNULL**. (BNF-5913)

Migration

- Existing SSL VPN web forwards are automatically migrated to generic web forwards during the update. Verify the functionality of the web forwards and, if necessary, recreate the web forwards. For more information, see How to Configure an Outlook Web Access Web Forward, How to Configure a SharePoint Web Forward, and How to Configure a Generic Web Forward.

Figures

1. av_mail_traffic.png
2. virus_protection_ftp_68_01.png
3. dhcp_relay_01.png
4. cudalaunch_RN.png
5. CudaLaunch11.png
6. CudaLaunch05.png
7. NAC-RN.png
8. Bild 049.png