Barracuda Firewall Release Notes 6.7.X

https://campus.barracuda.com/doc/44435160/

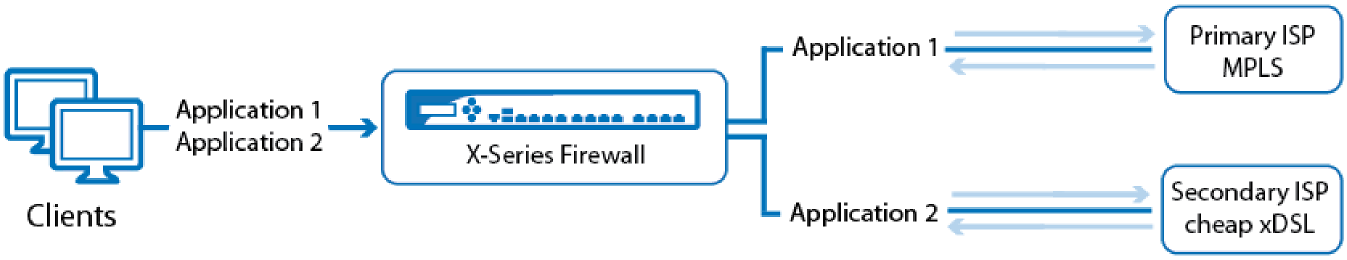
Please Read Before Upgrading

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 Firewall Version 6.7.0.022

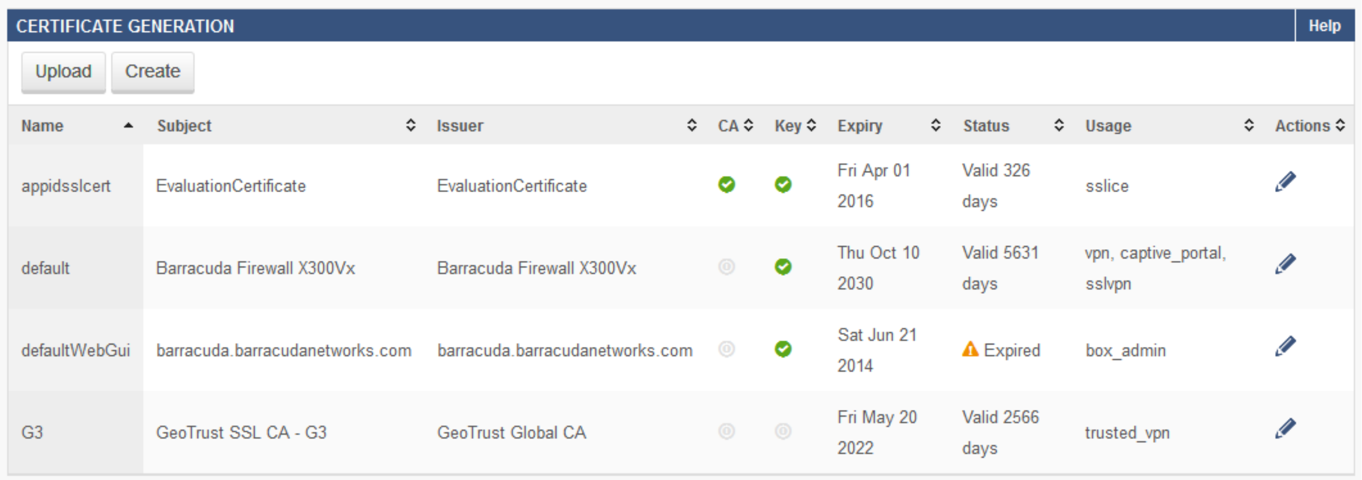
Application-Based Link Selection



Application-based connection objects allow you to select the Internet connection based on the application. Application-based link polices can be defined for individual applications or application categories. Traffic that does not match one of these policies is sent using the default connection object.

For more information, see Application Based Connection Objects.

Certificate Manager

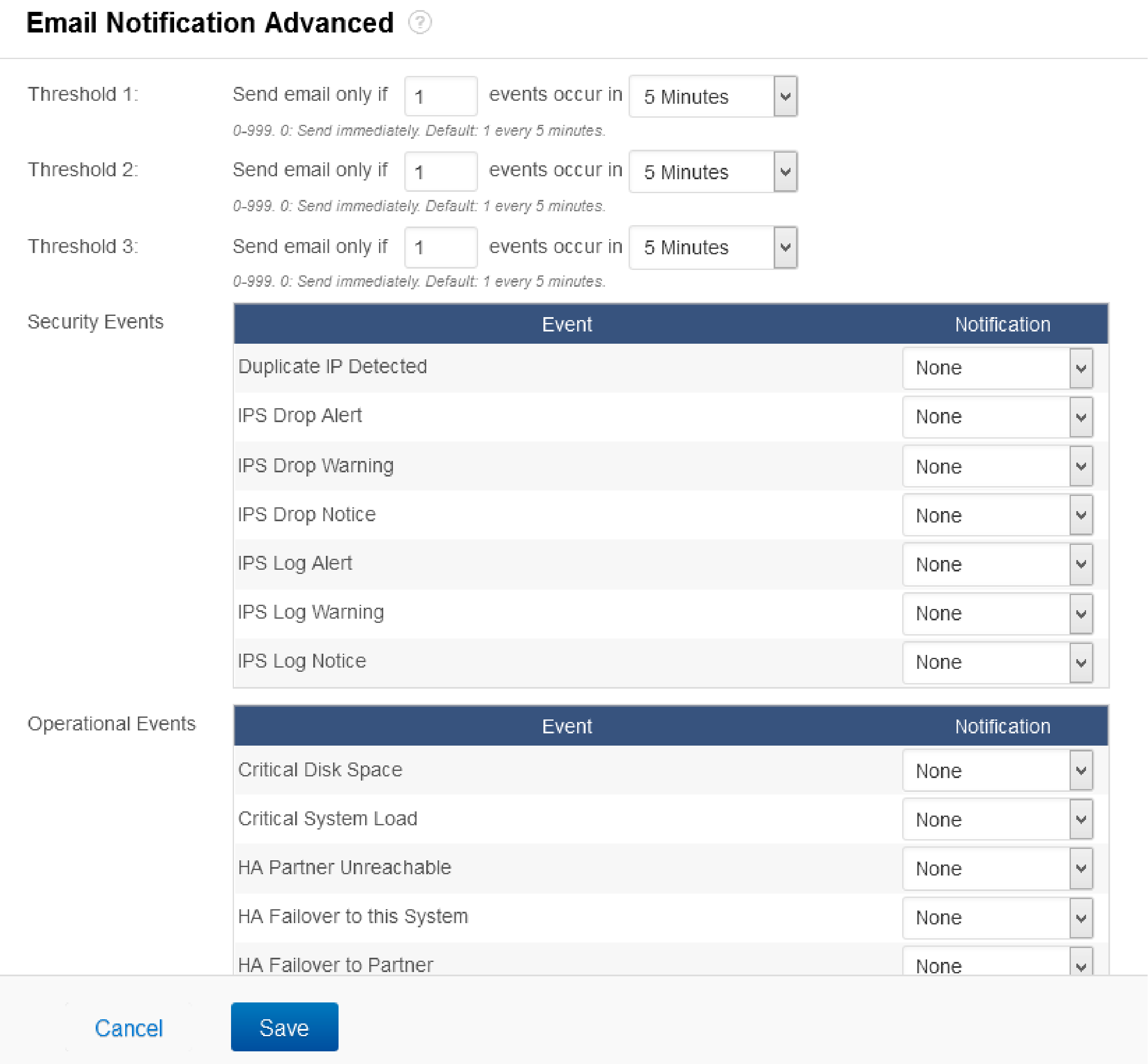


Name	Subject	Issuer	CA	Key	Expiry	Status	Usage	Actions
appidsslcert	EvaluationCertificate	EvaluationCertificate	✓	✓	Fri Apr 01 2016	Valid 326 days	sslice	✎
default	Barracuda Firewall X300Vx	Barracuda Firewall X300Vx	○	✓	Thu Oct 10 2030	Valid 5631 days	vpn, captive_portal, sslvpn	✎
defaultWebGui	barracuda.barracudanetworks.com	barracuda.barracudanetworks.com	○	✓	Sat Jun 21 2014	⚠ Expired	box_admin	✎
G3	GeoTrust SSL CA - G3	GeoTrust Global CA	○	○	Fri May 20 2022	Valid 2566 days	trusted_vpn	✎

The Barracuda Firewall uses the Certificate Manager as a central repository to manage all X.509 certificates on the device. You can create self-signed certificates or upload your own certificates. All certificates are available for all Barracuda Firewall services, as long as they meet the requirements for that service.

For more information, see How to Use and Manage Certificates with the Certificate Manager.

Email Notification



Email Notification Advanced

Threshold 1: Send email only if 1 events occur in 5 Minutes

0-999. 0: Send immediately. Default: 1 every 5 minutes.

Threshold 2: Send email only if 1 events occur in 5 Minutes

0-999. 0: Send immediately. Default: 1 every 5 minutes.

Threshold 3: Send email only if 1 events occur in 5 Minutes

0-999. 0: Send immediately. Default: 1 every 5 minutes.

Security Events

Event	Notification
Duplicate IP Detected	None
IPS Drop Alert	None
IPS Drop Warning	None
IPS Drop Notice	None
IPS Log Alert	None
IPS Log Warning	None
IPS Log Notice	None

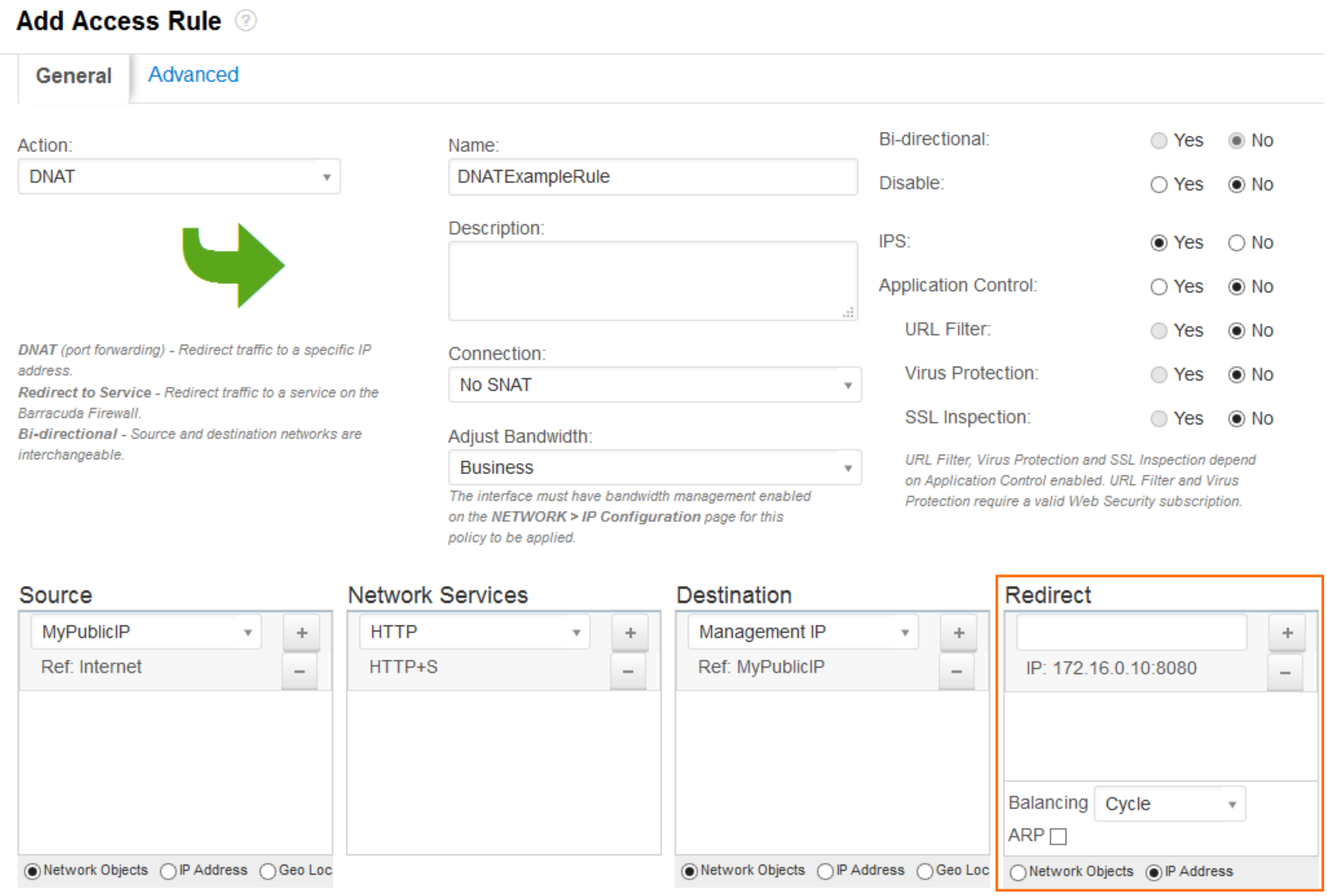
Operational Events

Event	Notification
Critical Disk Space	None
Critical System Load	None
HA Partner Unreachable	None
HA Failover to this System	None
HA Failover to Partner	None

The Barracuda Firewall can alert the administrator of important system events by sending notification emails. You can configure a notification email policy for each event. To limit the number of emails for frequently occurring events, you can define up to three thresholds. Thus, the administrator will receive an email only when the number of events exceeds the threshold set in the timespan. The following events can trigger email notifications:

For more information, see How to Configure Email Notifications.

Destination NAT Load Balancing



Add Access Rule

General | Advanced

Action: DNAT

DNAT (port forwarding) - Redirect traffic to a specific IP address.
Redirect to Service - Redirect traffic to a service on the Barracuda Firewall.
Bi-directional - Source and destination networks are interchangeable.

Name: DNATExampleRule

Description:

Connection: No SNAT

Adjust Bandwidth: Business

The interface must have bandwidth management enabled on the NETWORK > IP Configuration page for this policy to be applied.

Bi-directional: ○ Yes ● No
Disable: ○ Yes ● No
IPS: ● Yes ○ No
Application Control: ○ Yes ● No
URL Filter: ○ Yes ● No
Virus Protection: ○ Yes ● No
SSL Inspection: ○ Yes ● No

URL Filter, Virus Protection and SSL Inspection depend on Application Control enabled. URL Filter and Virus Protection require a valid Web Security subscription.

Source: MyPublicIP, Ref: Internet — ● Network Objects ○ IP Address ○ Geo Loc

Network Services: HTTP, HTTP+S

Destination: Management IP, Ref: MyPublicIP — ● Network Objects ○ IP Address ○ Geo Loc

Redirect: IP: 172.16.0.10:8080 — Balancing: Cycle — ARP □ — ○ Network Objects ● IP Address

To redirect to more than one server in cycle (round robin) or fallback mode, you can enter multiple IP addresses or use a network object containing multiple IP addresses for DNAT access rules. It is also possible to redirect to a different port by appending the port after the IP address.

For more information, see Firewall Rules and Example - Configuring a DNAT Access Rule.

Inline Editing of Firewall Objects

Barracuda Firewall firmware 6.7.0 adds the option of editing or creating objects directly in the UI element they are referenced from. For example, you can now create a network object in a second popover when creating an access rule without having to break the workflow.

Usability Improvements for DHCP Server Configuration

The DHCP server configuration has been reworked to improve useability. The DHCP server subnet list now also shows which port is used by the DHCP subnet.

Authoritative DNS Server Improvements

The DNS server now allows you to distinguish between internal, external, and combined zones on a per-domain basis and automatically creates PTR records when creating A records.

For more information, see Authoritative and Caching DNS.

VPN Split Tunnel Mode

Enabling the split tunnel mode for a Client-to-Site VPN allows only the client access to the networks published for the Client-to-Site VPN. This feature is available only for Windows clients using the full-featured Barracuda Network Access Client.

SSL VPN Mobile Portal

The Barracuda Firewall SSL VPN mobile portal provides a user-friendly interface with a service bar where users can launch available web resources that have been made accessible by the Barracuda Firewall. Users can navigate through the resources and add shortcuts to a favorites list.The Barracuda Firewall SSL VPN mobile portal supports most commonly used devices, e.g., Apple iOS, Android and Blackberry.

For more information, see SSL VPN for the Barracuda NextGen Firewall X, Mobile Portal User Guide and Supported Mobile Devices.

Local Disk Backup and Restore

The Barracuda Firewall now automatically creates up to 24 hourly backups directly on the local disk of the unit. These backups can be restored directly via Web UI or from the recovery console.

For more information, see How to Backup and Restore the Barracuda NextGen Firewall X.

Firmware Improvements

- Improved stability of the virus scanner engine during pattern updates. (BNF-5175)
- Using the URL Filter when accessing heavy, interactive websites now works as expected. (BNF-5276)
- You can now block just a subset of a URL. (BNF-5269)
- The SIP Proxy now reacts gracefully when failing to open additional dynamic ports. (BNF-5220)
- Custom application objects are now displayed correctly in the **Application** and **Details** columns on the **BASIC > Active** and **Recent Connections** pages. (BNF-5193)
- A warning popup is displayed when an SNMP source IP address is not a part of the Management ACL. (BNF-4881)
- Added popup to advise user to enable TCP Stream reassembly when enabling virus scanning in the Firewall. (BNF-4859)
- DC Agent authentication now works as expected. (BNF-4845)
- It now possible to use * wildcards when filtering on the **BASIC > Active** and **Recent Connection** pages. (BNF-4723)

- MSAD authentication now supports multi-domain login management by enabling **Check Domain Names** in the MSAD configuration. (BNF-4690)
- Yahoo Japan (yahoo.jp), Yahoo Mail Japan, and AOL Japan (aol.jp) are now detected by Application Control. (BNF-4683)
- The support tunnel now reliably starts when triggered via the WebUI. (BNF-4644)
- Editing service objects now works as expected. (BNF-4598)
- The **Directory Browser** now correctly displays error messages. (BNF-4565)
- Reverse Lookup zones are automatically created when adding an A-type DNS record. (BNF-4252)
- Filtering for information contained in the **Info** column on the **Recent Connections** page now works as expected. (BNF-4217)
- Added a validation check to avoid the HA partner from being excluded by the **Management ACL**. (BNF-4148)
- In an HA cluster the Wi-Fi ticketing information is now synced to the secondary box. (BNF-3733)
- When using Barracuda Cloud Control, the secondary unit of an HA cluster now mirrors the behavior of standalone secondary units. (BNF-2636)
- PPTP clients now show the username in the **Name** column on the **VPN > Active Clients** page. (BNF-1386)

Important Migration Steps

- If you are using an intermediary certificate bundled with a root certificate or a certificate chain as the SSL Inspection root certificate the certificate is not migrated to the new certificate manager. You must reupload the complete certificate bundle to the new certificate manager.
- Replace all certificates with a expiration date after 01.01.2038 before updating to 6.7.0. Please note that certificates with an expiration date after 01.01.2038 are not supported by this firmware version.
- If the **VPN Certificate Pool** on the **VPN > Settings** page is set to **default** make a dummy change to the **VPN > Client-to-Site VPN** configuration.

Known Issues and Limitations for 6.7.0.022

- In some cases certificates with a expiration date after 01.01.2038 are unusable after updating from 6.6.2 to 6.7.0.
- Smaller Barracuda Firewall models may take up to 10 minutes to verify the update package causing a browser timeout. Login again to apply the update.
- The SIP proxy can not be used for external Barracuda Phone appliances. Use Access rules to open the necessary ports instead.
- If appending a port to the first target IP address of a DNAT access rule, the port is applied to all target IP addresses.
- Barracuda Report Creator is only available for Windows 7, 8 and 8.1.
- Creating / Editing Firewall Access Rule: In the “Connection” portion the inline creation only allows to create a regular connection object, not an application based connection object.
- Inline edit of connection objects is not possible for application based connection objects.
- Application based connection objects can not be renamed.
- Application based connection objects must be saved before adding link policy objects.

- Certificate manager and application based connection objects currently can not be configured via the Barracuda Control Center.
- In rare cases, using the Ping, Telnet, or Dig commands in Advanced > Troubleshooting results in an empty pop-up window. Clicking Reload in the Basic > Administration tab resolves this issue.

Figures