Release Notes 6.1.1

https://campus.barracuda.com/doc/46203690/

Before installing or upgrading to the new firmware version, back up your configuration and read the release and migration notes. If you are updating from a version earlier than 6.0.x, all migration instructions for 5.x and 6.0 also apply.

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, depending on your current firmware version and other system factors. If the process takes longer, please contact Barracuda Networks Technical Support for further assistance.

In these Release Notes:

General

If you want to update an existing system:

- When updating from an earlier version to 6.1, the following update path applies: **4.2 > 5.0 > 5.2 > 5.4 > 6.0 > 6.1.**
- Barracuda NG Firewall F100 and F101 models using the ClamAV Virus Scanner may not have enough free disk space for updating. For more information, see Migrating to 6.1.
- Do not upgrade Barracuda NG Firewalls or NG Control Centers using Xen HVM images to 6.1.0.

For more information, see Migrating to 6.1.

GPL Compliance Statement

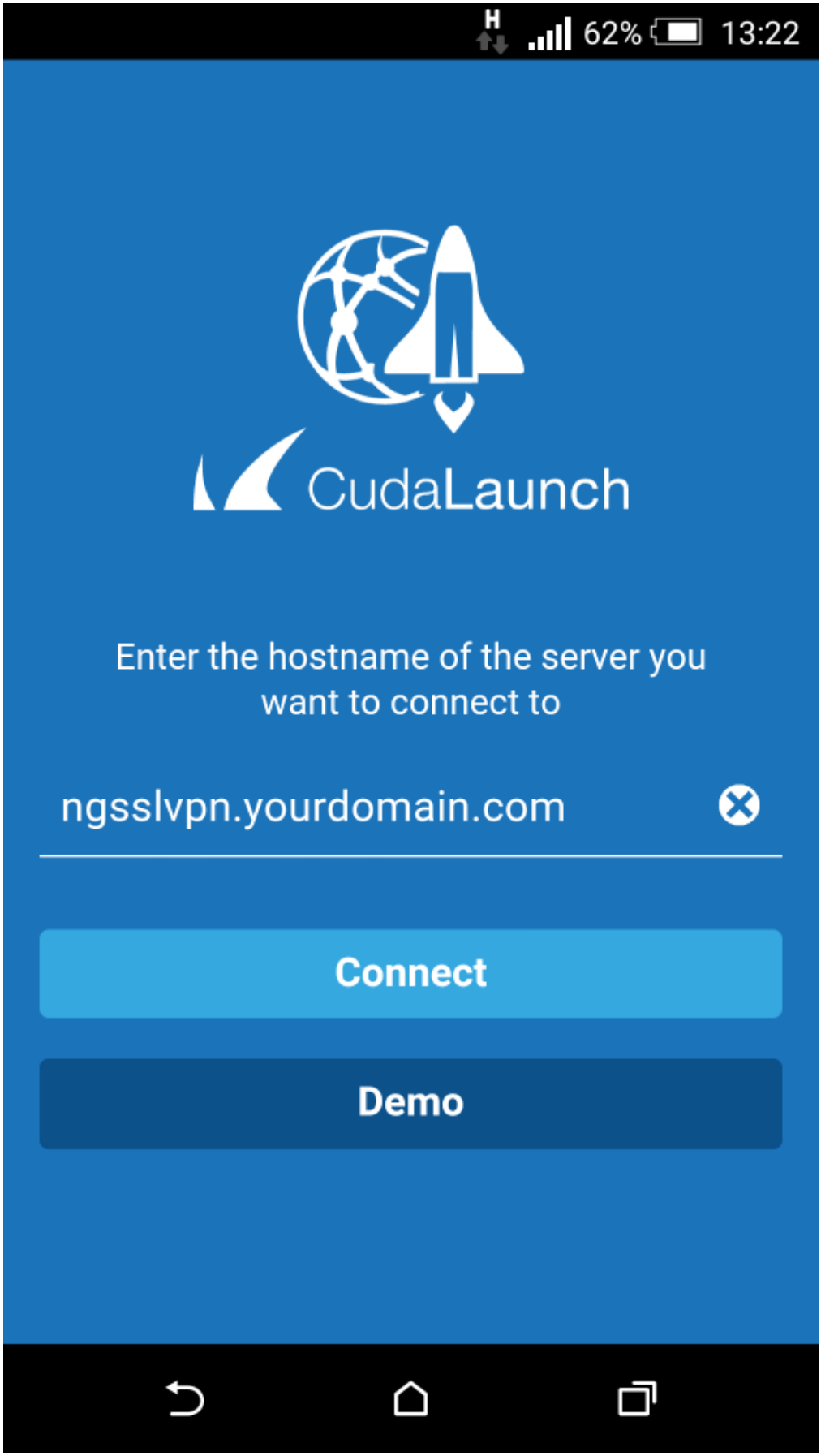
This product is in part Linux-based and contains both Barracuda Networks proprietary software components and open source components in modified and unmodified form. Some of the open source components included underlie either the GPL or LGPL, or other similar licensing, which requires all modified or unmodified source code to be made freely available to the public. This source code is available at http://source.barracuda.com.

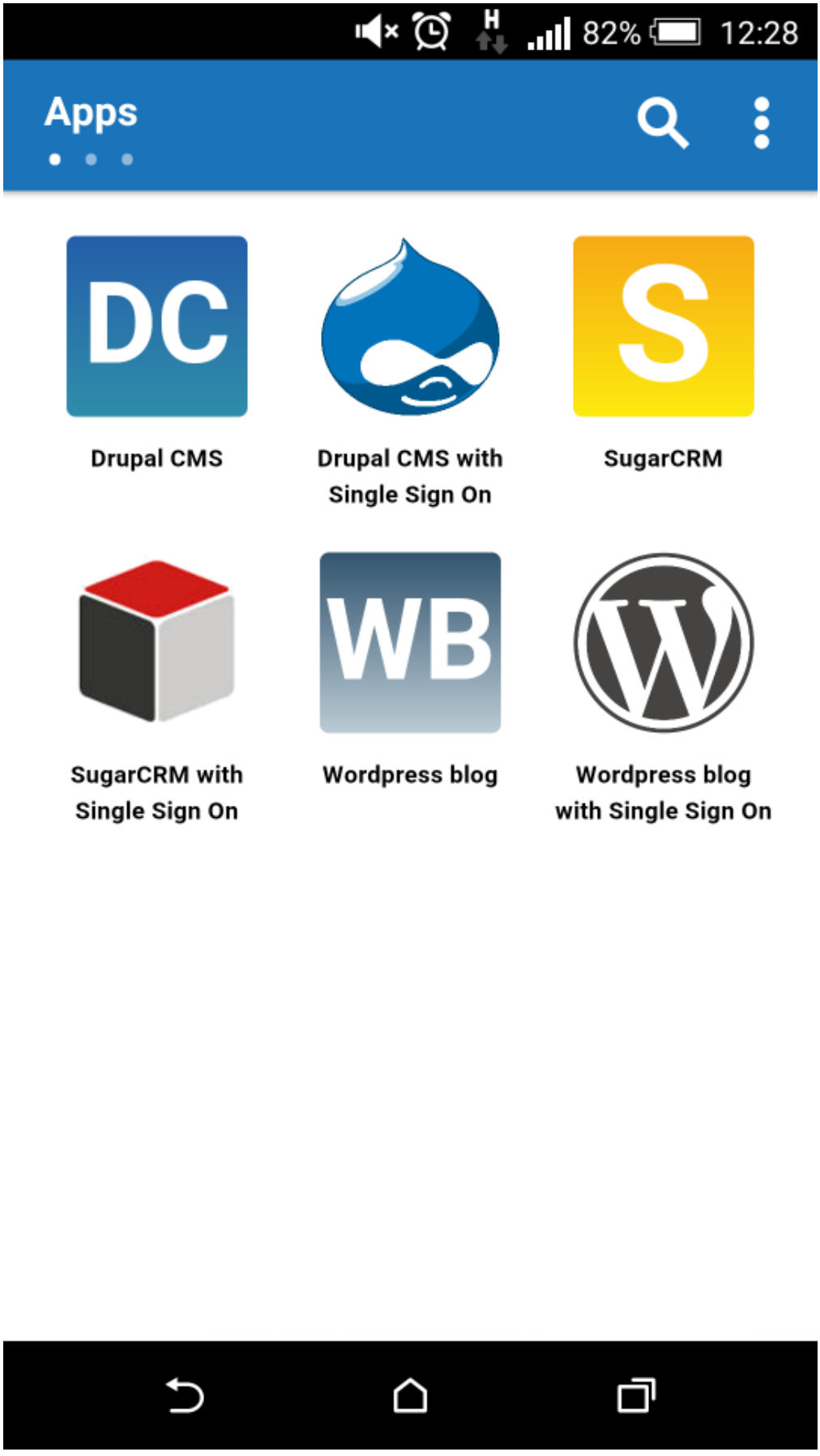
Hotfixes Included with Barracuda NG Firewall Version 6.1.1

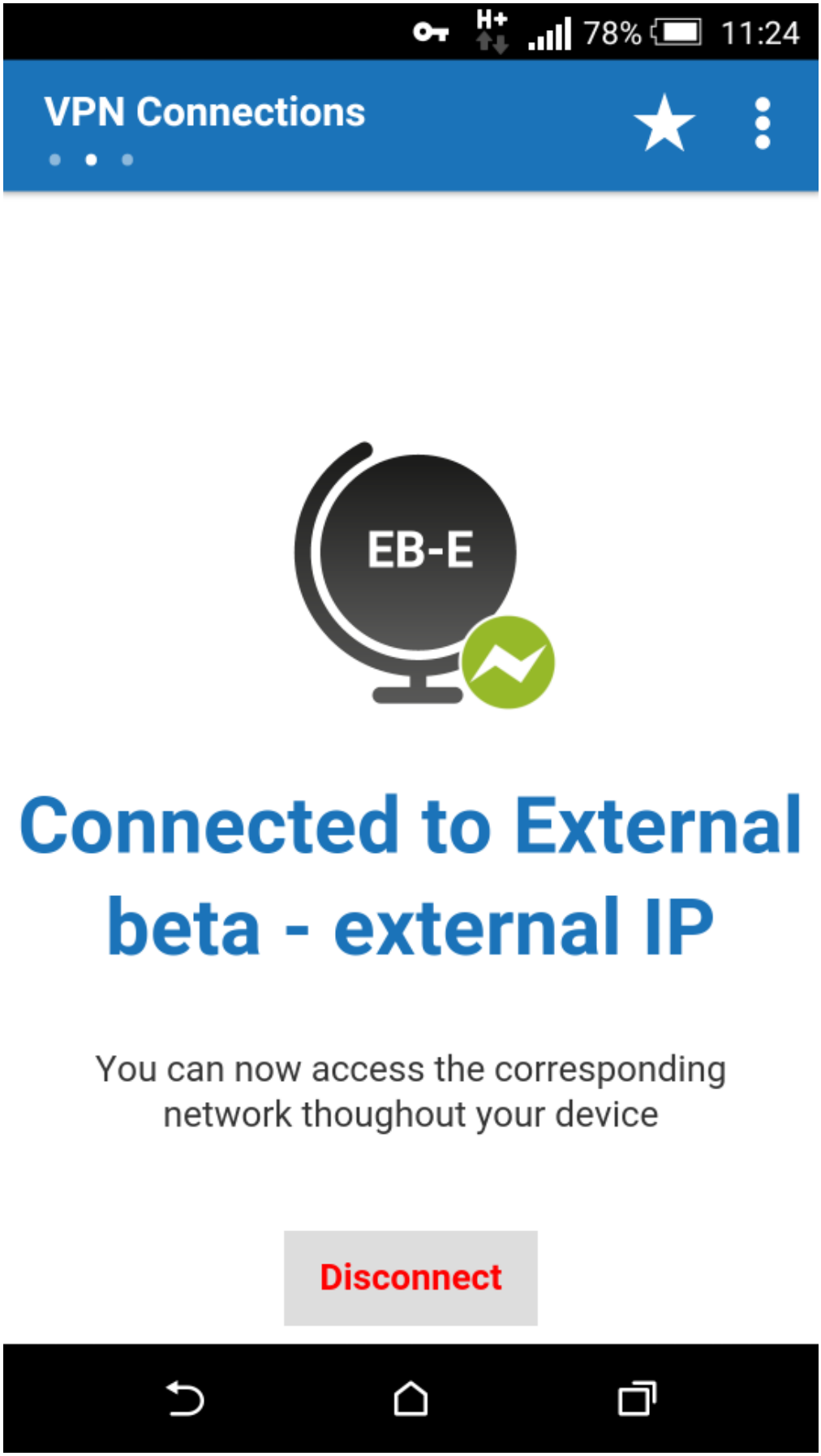
- Hotfix **686**: Wi-Fi Access Point Authentication
- Hotfix **687**: SSL VPN Generic Web Forwards
- Hotfix **693**: Leap Second Update 2015
- Hotfix **697**: DHCP Server Restart Policy
- Hotfix **699**: Azure Public Cloud Detection

What´s New in Barracuda NG Firewall Version 6.1.1

CudaLaunch


62%
13:22
CudaLaunch
Enter the hostname of the server you want to connect to
ngsslvpn.yourdomain.com
Connect
Demo

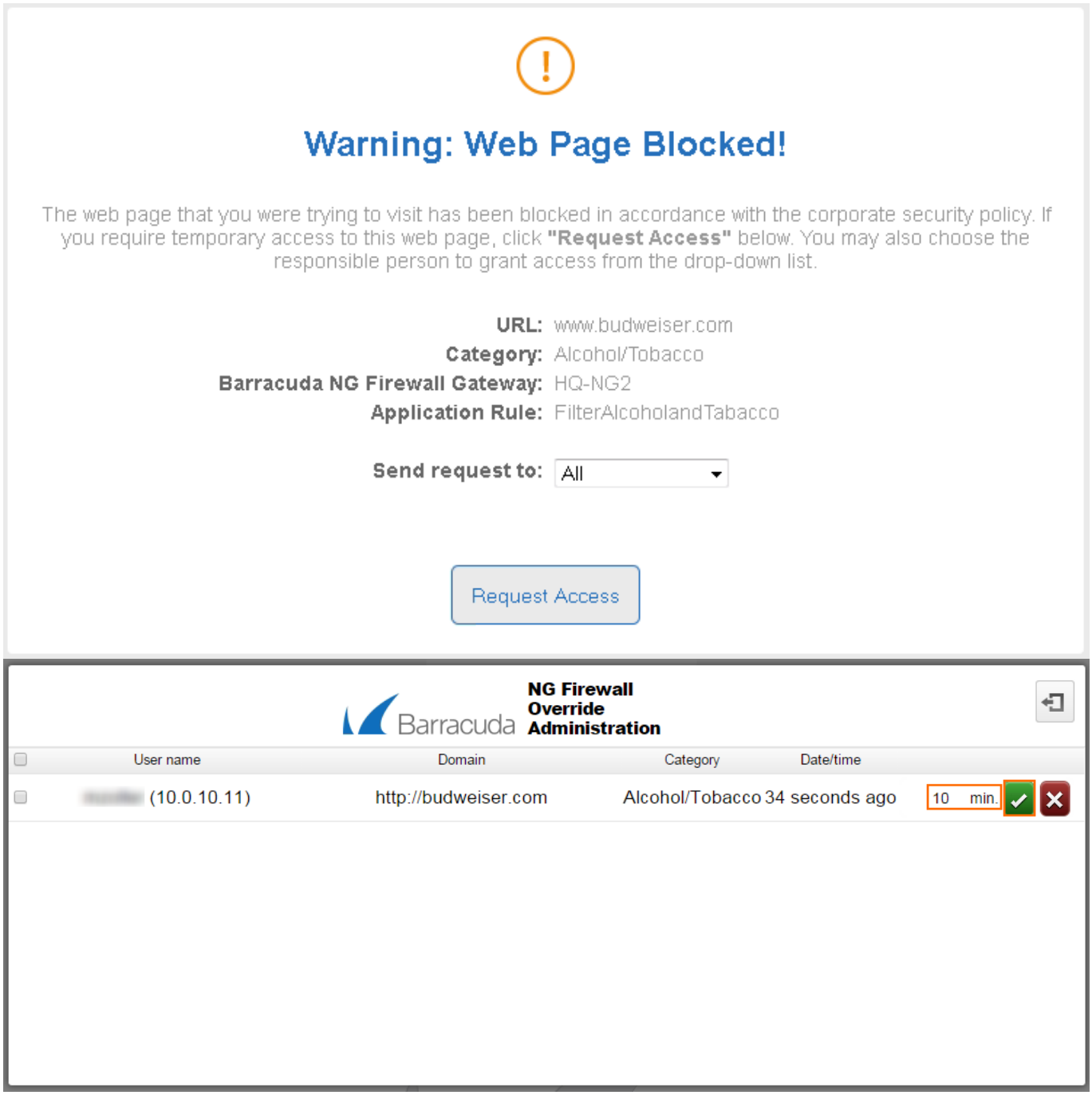

82%
12:28
Apps
DC
Drupal CMS
Drupal CMS with Single Sign On
S
SugarCRM
SugarCRM with Single Sign On
WB
Wordpress blog
Wordpress blog with Single Sign On


78%
11:24
VPN Connections
EB-E
Connected to External
beta - external IP
You can now access the corresponding
network thoughout your device
Disconnect

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. CudaLaunch on Android uses the TINA VPN protocol; the iOS app manages the built-in IPsec VPN client.

For more information, see CudaLaunch and NG Firewall Configuration for CudaLaunch.

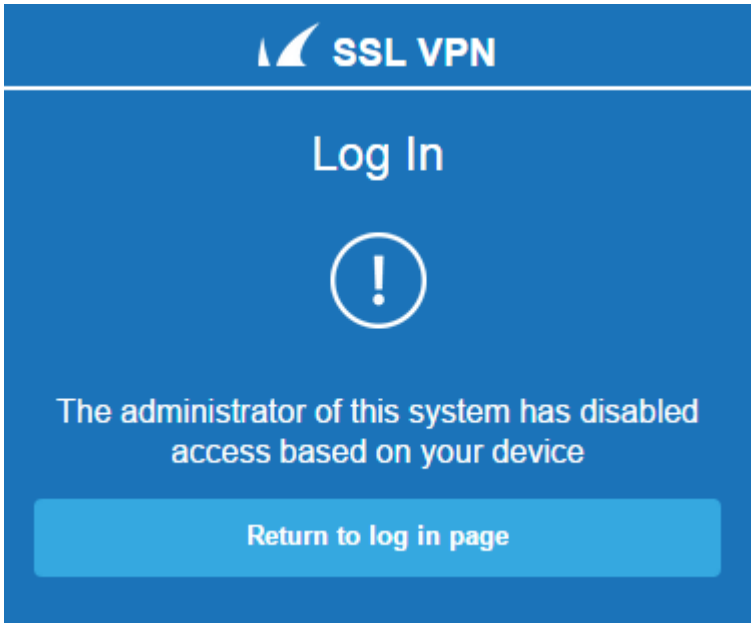
URL Filter Overrides



The Override feature of the URL Filter grants temporary access to otherwise blocked URL categories. URL categories that are set to the **override** policy redirect the user to the customizable Override Block page of the URL Filter. The override admin must grant the request for a specified time. When the request has been granted, the user is automatically forwarded to the website. Overrides are always granted for the entire URL category.

For more information, see How to Configure URL Filter Overrides and How to Grant URL Category Overrides - User Guide.

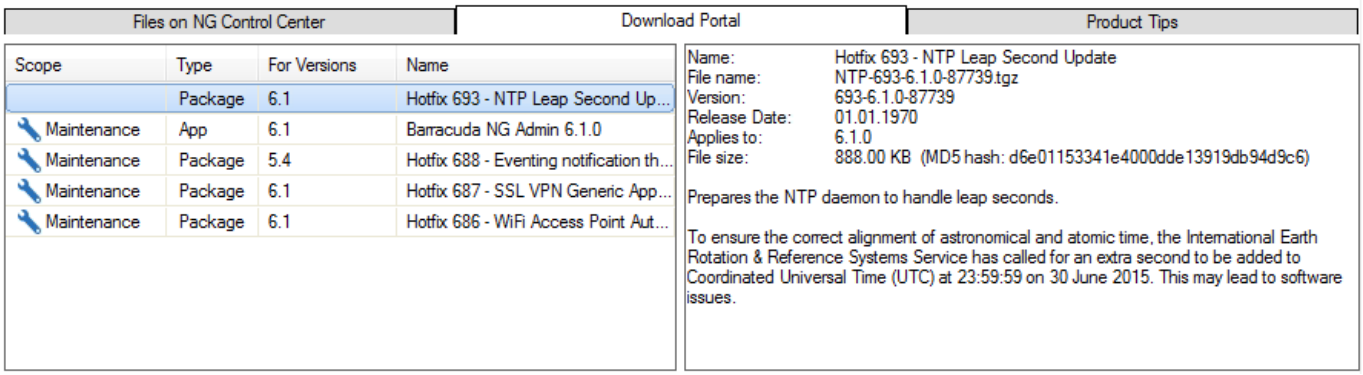
NAC for SSL VPN and CudaLaunch



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.

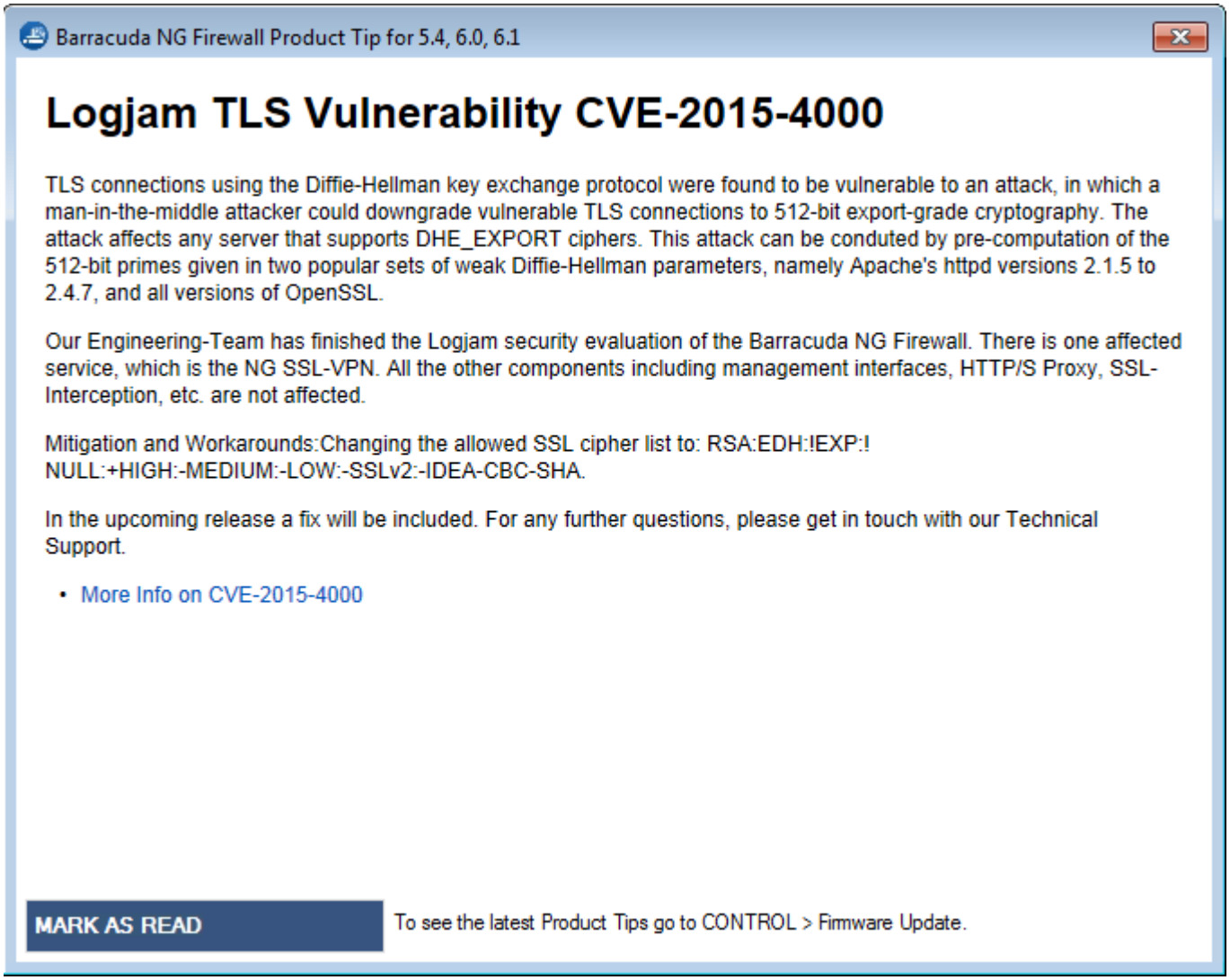
Firmware Update Management on the NG Control Center



Similar to standalone units, the Barracuda NG Control Center Firmware Update page is now tied in with the new Barracuda Download Portal. The **Download Portal** tab displays dependencies for updates and hotfixes as well as detailed information for each download. On the box level of the NG Control Center, go to **CONFIGURATION > Configuration Tree > Advanced Configuration > Firmware Update** to enable the **Download Products** tab.

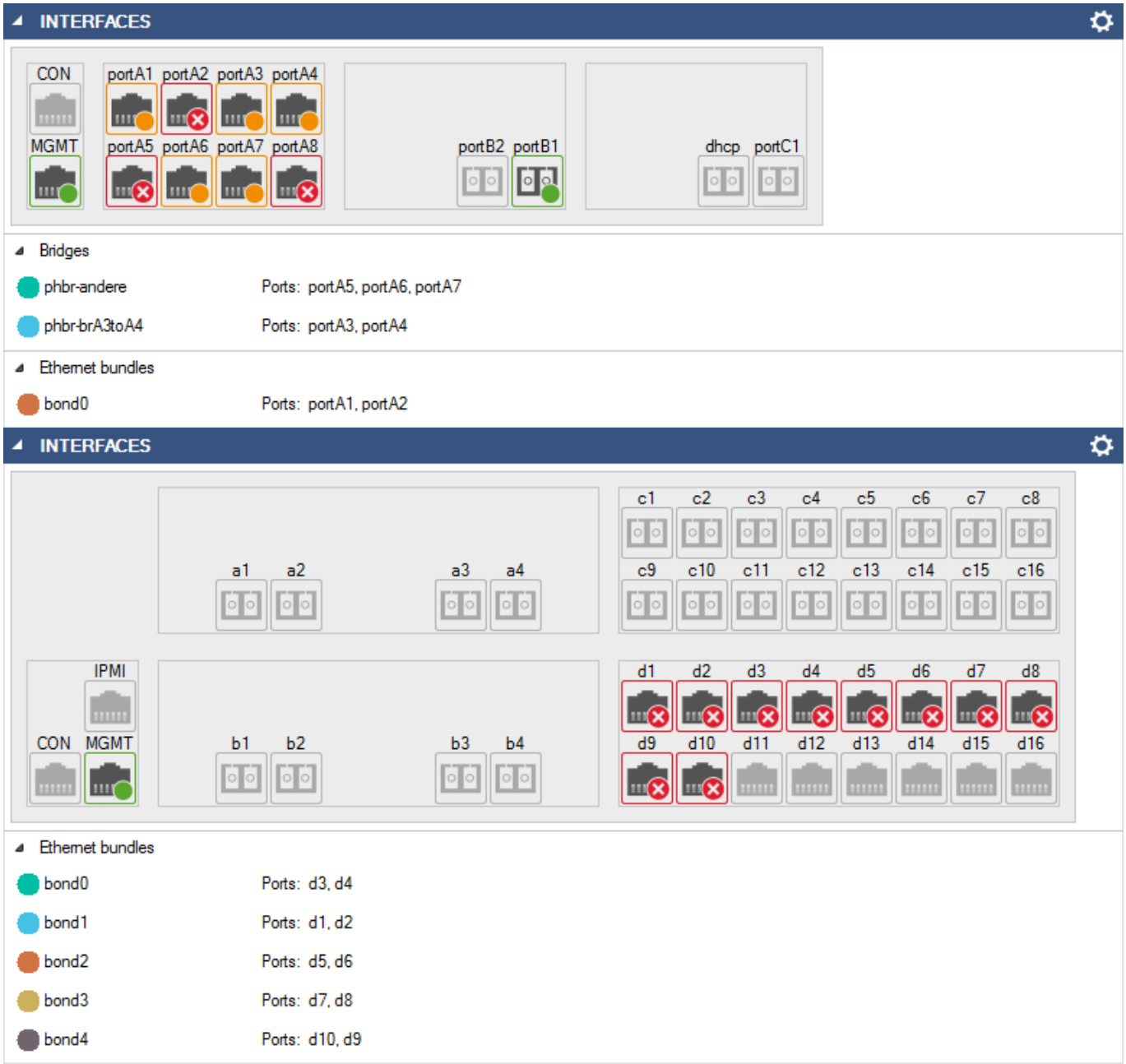
For more information, see How to Update Barracuda NG Control Center Managed Systems.

Product Tips on the NG Control Center



Barracuda Networks can now inform customers of important issues such as security vulnerabilities or other important messages concerning the Barracuda NG Firewalls managed by the NG Control Center. These notifications are displayed in the **Product Tips** element on the **Dashboard**. On the box level of the NG Control Center, go to **Box > Advanced Configuration > Message Board** to enable **Product Tips**.

Interface Dashboard Element



The **Interface** element shows the port configuration for your Barracuda NG Firewall. All ports are displayed in the same location and with the same port names as on the physical appliance.

For more information, see DASHBOARD General Page.

Updated Available Instance Types for Barracuda NG Firewalls in AWS and Azure

When deploying the Barracuda NG Firewall in Azure or AWS, you can now choose from an updated list

of Instance sizes and types. In Azure, it is now possible to use any Instance size, as long as the license level matches the number of available CPU cores. AWS Instance types have been updated to use the new generation of AWS Instances. These changes apply to both BYOL and PAYG (Hourly) images.

For more information, see Public Cloud Hosting.

Improvements Included in Barracuda NG Firewall Version 6.1.1

Barracuda NG Admin

- The Firmware update element no longer causes NG Admin to crash on systems that are located in a time zone with a negative offset. (BNNGF-30967)
- Improved error handling when receiving invalid responses from the Barracuda Servers while downloading licenses. (BNNGF-30618)
- Changed the input validation of the **YouTube for Schools Token** to allow underlines. (BNNGF-31421)
- Downloading update via the firmware update element now works as expected. (BNNGF-30094, BNNGF-30824)
- Entering **Networks** for Site-to-Site tunnels is no longer required. This is required for an OSPF over VPN configuration. (BNNGF-31444)
- Changed input validation for **Site Specific Objects** to allow all characters also allowed for Forwarding Firewall Objects. (BNNGF-31040)
- Generating system reports now works as expected. (BNNGF-31181)
- The access rule dialog now handles larger system text sizes. (BNNGF-31068)
- NG Admin no longer crashes in unconfigured GTI Editor. (BNNGF-29676)
- Session details now contain the **URL Category** and **Application Context**. (BNNGF-31665)
- Copying/Paste and cloning of Schedule objects now work as expected. (BNNGF-31630)
- **Switch to Advanced View** is visible again on the **Box > Administrators** page. (BNNGF-31449)
- The IPsec tunnel statuses are now displayed on **CONTROL > GeoMaps** and **CONTROL> Status Map.** (BNNGF-24002)
- NG Admin now works as expected on Windows Vista. (BNNGF-30495)
- Added check to ensure names for GTI Editor groups are unique. (BNNGF-30431)
- Added column for the **serial number** to the NG Control Center **CONTROL > Status Map**. (BNNGF-29850)
- Using range regular expressions for filtering in NG Admin now works as expected. (BNNGF-20283)
- Licenses that are about to expire are now displayed in yellow on the **CONTROL > Licenses** page. (BNNGF-13807)
- RCS now works as expected on the **Security Policy** and **Response Messages** pages. (BNNGF-29819)
- RCS now works as expected on the **Network** page when a UMTS/3G modem is configured. (BNNGF-21274)

- The eventing service is now included in the status displayed on the **CONTROL > Status Map** page. (BNNGF-29674)
- Changed input validation to allow **-** (dash) and **_** (underscore) in the shell script editor on the **CONTROL > Remote Execution** page. (BNNGF-31551)
- The Firmware Update element now also works with SF licenses. (BNNGF-30056)
- Pressing delete key repeatedly no longer temporarily removes list items without a page lock. (BNNGF-30091)
- Exporting the **Trusted Root Certificate** to the clipboard on the **Security Policy** page now works as expected. (BNNGF-29936)
- **Rate-Max** for inbound traffic shaping rates larger than 2047 Mbit on the **FIREWALL > Shaping** page are now displayed correctly. (BNNGF-28993)
- Icons in the **CONTROL > Network > ARP** are now displayed correctly. (BNNGF-27948)
- Changing the welcome message for the Access Control Service now works as expected.(BNNGF-24005)

Barracuda OS

- Increased the number of supported DHCP WAN connections to twelve. (BNNGF-31523)
- After updating, **controld** now restarts if necessary. (BNNGF-30455)
- Updated libcurl to fix several security vulnerabilities. (BNNGF-39894, BNNGF-30108)
- **installUpdate** now writes to the **box_Release_update.log** file. (BNNGF-31305)
- Fixed potential issues caused by leap seconds. (BNNGF-31167, BNNGF-31160)
- Improved event handling for events not reaching the Notification Threshold defined for one week. (BNNGF-28795)
- Added rpm signature checks to hotfix files and **PhionRelCheck**. (BNNGF-30551)
- For Wi-Fi AP authentication, it is now possible to define a subnet or an individual IP address as the access point source network. (BNNGF-30126)
- Improved memory management of the **MSAD DC Client** authentication. (BNNGF-29964)
- Updated default values for the general firewall configuration parameters. (BNNGF-31425)
- Updated OpenSSL to version 0.9.8zf. (BNNGF-21059)
- Users authenticating the first time via an Aerohive Wi-Fi access point are no longer assigned a wrong IP address. (BNNGF-30080)
- It is now possible to migrate virtual servers to VF2000 or higher. (BNNGF-30051)
- Removed option to use wildcards in the pre-authentication value patterns. (BNNGF-26436)
- The control daemon now automatically monitors and restarts ntpd. (BNNGF-29702)
- Product Tips and Firmware Update Element now generate events when new items are available. (BNNGF-29447)

Firewall

- YouTube for Schools now works as expected when accessing YouTube via HTTPS. (BNNGF-31370)
- Changes to the forwarding firewall ruleset no longer terminate sessions allowed due to a firewall plugin. (BNNGF-25686)
- The FTP plugin now handles EPRT ftp commands correctly. (BNNGF-30323)
- YouTube SafeSearch can no longer be deactivated when using the Chrome browser.

(BNNGF-30268)
- Added IP addresses for **dlportal.barracudanetworks.com** (64.235.151.85 and 95.172.71.5) to the **Barracuda Update Servers** network object. (BNNGF-29445)
- The **Authentication Timeout** when accessing the Barracuda Web Security Service (Flex) is now configurable. (BNNGF-31510)
- Internal access rules not accessible for the user no longer generate events. (BNNGF-26014)
- Client-to-Site VPN traffic is no longer blocked when a MAC-based access rule is located before the client-to-site access rule in the ruleset. (BNNGF-29862)
- The number of network objects that can contain hostnames is no longer limited to 383. (BNNGF-30590)

Distributed Firewall

- Using application objects in the application ruleset now works as expected. (BNNGF-31430)

HTTP Proxy

- The progress bar popup now works as expected. (BNNGF-31782)
- Handling of URL categorization in the HTTP Proxy service now works as expected. (BNNGF-31126)
- Files analyzed by ATD are no longer cached by the HTTP Proxy. (BNNGF-27131)

Virus Scanner

- Improved handling of RAR files no longer cause high CPU loads. (BNNGF-29816)
- Virus patterns are now updated immediately after installing an update or hotfix containing the virus scanner rpm. (BNNGF-29152)
- Using legacy phion pool licenses in combination with Avira now works as expected. (BNNGF-30304)

DHCP Server

- The DHCP server now listens on both LAN and Wi-Fi interfaces if DHCP subnets are served over both interfaces. (BNNGF-29780)

VPN Server

- Encapsulation for IPsec tunnels using NAT-T is now set correctly. (BNNGF-29755)
- L2TP tunnels now work as expected when a referenced firewall object is used for the static IP address of the user. (BNNGF-31052)
- To avoid excessive logging, the default **Log Level** for WAN Optimization is now set to **0**. (BNNGF-30784)

SSL VPN

- Checking documents in and out on a SharePoint 2010 server now works as expected.

(BNNGF-517)
- The password attribute value is no longer visible in the browser page source. (BNNGS-1001)
- You can now remove all permissions from the custom VPN profiles. (BNNGS-999)
- SSL tunnels associated with generic applications are now correctly scoped to the respective Application. (BNNGF-30333, BNNGS-983)
- Writing to log file while loading a Web Forward now works as expected. (BNNGS-936)
- Single Sign-On via JavaScript authentication now works as expected. (BNNGS-935)
- Tapping **Logout** now works as expected on iOS and Windows Phone devices. (BNNGS-930)
- Added input validation to ensure the **Allowed Host filter path** is unique. (BNNGS-748)
- Saving and displaying text for **User Attributes** using the **TextArea** format now works as expected. (BNNGS-368)
- Clicking **Login** button repeatedly after logging in no longer results in a JavaScript error. (BNNGS-240)

FTP Gateway

- Added option to limit the **Maximal Workers per Peer** to avoid high system load. (BNNGF-21237)
- Changed the maximum number allowed for **Maximal Allowed Workers** to 255 and the default value to 128. (BNNGF-30574)

OSPF/RIP/BGP Service

- BGP weight changes now work as expected. (BNNGF-30028)

Azure

- A MAC address change because of a reboot no longer invalidates the license on managed Barracuda NG Firewalls in Azure. (BNNGF-31497)

Xen

- Xen HVM images now work as expected. (BNNGF-28214)
- Xen HVM images now use the **xen-netfront** network driver by default if possible. (BNNGF-27392)

NG Control Center

- Managed NG Firewalls running on a Xen hypervisor report their serial number correctly. (BNNGF-31701)
- Setting **Enforce password strength** to **No password enforcement** for NG Control Center admins now works as expected. (BNNGF-27960)
- NG Control Center admins assigned to an Administrative Role that disallows **Create PAR File** can no longer create system reports containing PAR files. (BNNGF-21496)
- Box level configuration for Firmware Update Element and Products tips is now accessible through **Set Area Config** on the **CONTROL > File Upload** page on the NG Control Center. (BNNGF-29443)

Known Issues

6.1.1

- Product Tips: A NG Admin session may temporarily freeze when the Barracuda Update servers are unreachable.
- Product Tips: Product Tips on the NG Control Center are enabled, even though the **Enabled** is set to **No** in the **Set Area Config** for **Product Tips** on the **CONTROL > File Update** page. Do a dummy change set the configuration. This settings also applies to all NG Firewalls managed by the NG Control Center.
- Opensource Xen HVM: Opensource (Linux) Xen HVM images are currently not supported for firmware 6.1.1.
- Interface Element: In some cases the interface element may not work correctly on virtual NG Firewalls.
- Firewall Plugin: The DCERPC firewall plugin module is disabled.
- Azure: During the update to 6.1.1 the ssh key is regenerated replacing the existing ssh key.
- Barracuda NG Control Center C610: Verification of the raid rpm signature included in the extra update archive fails, causing phionRelCheck to show a dirty release state.
- Application Control 2.0: The URL Category **Search Engine** may not be set to **override** when URL Filtering is used in combination with SafeSearch.
- HTTP Proxy: Custom block pages do not work for the HTTP Proxy when running on the same NG Firewall as the Firewall service. This issue does not occur when running the HTTP proxy service on a second NG Firewall behind the NG 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: The mobile navigation bar is missing from servers entered in the **Allowed Hosts**.
- 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 in to YouTube when cookies are disabled.
- Safe Search: Safe search is not enforced by Bing when using HTTP.
- VPN Routing: When a duplicate route to an already existing VPN route in the main routing table is announced to the NG Firewall 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.

Miscellaneous

- 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 NG Control Centers deployed using NG

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.
- Firewall: It is not possible to join a **join.me** session if SSL Interception and Virus Scanning is enabled in the matching access rule.
- Firewall: Using SSL Interception in combination with URL Filtering and category exemptions may result in degraded performance.
- NG Admin: SPoE does not work if an IPv6 virtual server IP address is used.
- 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 2.0 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 2.0 and Virus Scanning: If the Content-Length field in HTTP headers is missing or invalid, the **Large File Policy** may be ignored.
- Application Control 2.0 and Virus Scanning: It is not currently possible to perform virus scanning for chunked transfer encoded HTTP sessions such as media content streaming. Barracuda Networks recommends excluding such traffic from being scanned.
- Application Control 2.0 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 2.0 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.**
- High Availability: IPv6 network sessions might not be established correctly after an HA failover.
- Barracuda OS: Restoring units in default configuration with par files created on an NG Control Center may result in a corrupt virtual server. Instead, copy the par file to */opt/phion/update/box.par* and reboot the unit.
- VPN: Rekeying does not currently work for IPsec Xauth VPN connections. The VPN tunnel terminates after the configured rekeying time and needs to be re-initiated.

Figures

1. cudalaunch_RN.png
2. CudaLaunch11.png
3. CudaLaunch05.png
4. WF_Override_UserGuide03.png
5. WF_Override_UserGuide02.png
6. NAC-RN.png
7. CC-FWUP-RN.png
8. CC_ProductTips_RN.png
9. interface01.png
10. interface02.png