



Barracuda NG Firewall



Migration Instructions

Version 5.2



- General 4**
 - GPL Compliance Statement 4
- Prerequisites 5**
 - Supported Hardware 5
 - Minimum System Requirements 6
 - Update Matrix 7
- What’s New with Barracuda NG Firewall 5.2? 7**
- Known Issues 7**
- Bugfixes Included with Barracuda NG Firewall 5.2 8**
 - Barracuda NG Admin 8
 - Barracuda NG Install 10
 - Barracuda NG Firewall 10
 - Barracuda NG Network Access Client 13
- Determine Your Update Scenario 18**
 - Combining Barracuda NG Control Center 5.2 with 5.0 and/or 4.2 Boxes 20
 - Solving Update and Installation Failures 20
- Updating Unmanaged Boxes or Control Centers 21**
 - Updating Boxes or Control Centers using SSH 21
- Updating HA-Synced Boxes or HA-Synced Control Centers 22**
- Updating Control Center Managed Boxes 24**
- Migrating Cluster / Range Config to 5.2 26**
- Updating Standard Hardware from 4.2.x to 5.2 27**
 - General 27
 - Updating Procedure 27

Warning



Read this document **before** updating your system

Please pay special attention to Known Issues, *Known Issues* and Hardware Restrictions

General

This is the official firmware release version 5.2 for the Barracuda NG Firewall.


You can use all of your existing licenses with this new firmware.


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. A certain number of the included open source components underlie the GPL or LGPL or other similar license conditions that require the respective modified or unmodified source code to be made freely available to the general public, this source code is available on <http://source.barracuda.com>.

Please also refer to the chapter *Warranty and Software License Agreement* of the Barracuda NG Firewall 5.2 Administrator's Guide documentation located in the documentation section on www.barracuda.com and on each accompanying USB thumb drive.

Prerequisites

Caution  As soon as a box has been updated to firmware version 5.2 and, subsequently, any new features were configured using Barracuda NG Admin 5.2, **no configuration changes must be made anymore using older versions of Barracuda NG Admin!** Doing so could destroy the configuration.
Always use Barracuda NG Admin 5.2 together with Barracuda NG Firewall 5.2.

Caution  In case you need to newly install a box from scratch, the default password for the `root` user is always:
`ngflr3wall`

Supported Hardware

Table 1–1 Barracuda Networks Appliances Supported By Barracuda NG Firewall 5.2

Barracuda Networks Appliances Supported by Barracuda NG Firewall 5.2
Hardware Appliances: F10, F15, F100, F200, F300, C400, C610, F400, F600, F800, F900
Virtual Appliances: VC400, VC610, VC820

Table 1–2 Legacy Appliances and Standard Hardware Supported By Barracuda NG Firewall 5.2

Legacy Appliances and Standard Hardware Supported by Barracuda NG Firewall 5.2
Legacy Hardware Appliances*: netfence edge Rev. B, sintegra XS Rev. B, sintegra S Rev. B, sintegra SR Rev. B, netfence S, netfence SR, netfence E, netfence XL, MR, M1, M3 Rev. A, M3 Rev. B, sintegra XS, sintegra S, sintegra S Rack, netfence edge Rev. A, netfence 140, netfence 240, netfence 240 Rack, netfence 421, netfence 431, netfence 780, netfence 850, S6 Rev. A, S6 Rev. B, S16, M50, L2000, industrial appliance
Standard Hardware: This refers to hardware which is neither a Barracuda Networks nor a legacy phion appliance. Please follow the instructions given in the chapter Updating Standard Hardware from 4.2.x to 5.2, page 27 .

* See the [Barracuda NG Firewall 5.0 Migration Instructions](#) for important information on updating restrictions appearing with certain legacy appliances.

Minimum System Requirements

Caution



If you are upgrading standard hardware to Barracuda NG Firewall 5.2, please ensure that at least **2 GB of free storage space** is available on the root partition. If this minimum amount of space is not available, Barracuda Networks highly recommends to re-install the system with a larger root partition instead of upgrading. On appliances with hard disk, the upgrade package requires additionally **another 2 GB** of free storage space on the `/phion0` partition for storing temporary data. This additional space is not necessary on Flash based appliances.

Caution



On flash appliances, please remove all USB devices except the installation USB thumb drive before initiating the installation process. Otherwise, the following error message may occur:

An error occurred finding the installation image on your hard drive. Please check your images and try again.

Table 1–3 Minimum system requirements for Barracuda NG Firewall

Operation Systems	Included (Barracuda OS)
Disk space	15 GB on a dedicated harddisk for gateway installation on harddisks 4 GB for gateway installation on a CF flash card with 1.5 GB of free space 30 GB on a dedicated harddisk for Barracuda NG Control Center installation 2 GB of free storage space on the root partition 2 GB of free storage space on the <code>/phion0</code> partition 50 MB of free storage space on the dedicated boot partition. 1 GB on an USB thumb drive for new installations.
RAM	512 MB
Processor	400 MHz, i686 compatible The CPU must support the TSC and CMOV instructions. Installing or updating systems with older CPUs will exit with an error.
Networking	1 network interface required
Partitioned space	The dedicated boot partition must have a size of at least 50 MB. Updating a system with a smaller boot partition size exits with an error. Therefore, Barracuda Networks recommends to perform a fresh installation instead of updating, as with a fresh installation the partition size will automatically be adjusted correctly.

Table 1–4 Minimum system requirements for Barracuda NG Admin / Barracuda NG Install

Operation Systems	Windows XP, Windows Vista (32-bit, 64-bit), Windows 7 (32-bit, 64-bit) with Microsoft .NET Framework 3.5 SP1 or Microsoft .NET Framework 4.0 or later
Disk space	30 MB
RAM	1 GB
Processor	1 GHz

Update Matrix

Table 1–5 Update matrix - supported and not supported update cases

	Target Version			
	5.0	5.0.1	5.0.2	5.2.0
4.2.10 and earlier	-	-	-	-
4.2.11	✓	✓	✓	-
4.2.13	✓	✓	✓	-
4.2.14	✓	✓	✓	-
4.2.15	✓	✓	✓	-
5.0	-	✓	✓	✓
5.0.1	-	-	✓	✓
5.0.2	-	-	-	✓

What's New with Barracuda NG Firewall 5.2?

Related Docs



See the **Barracuda NG Firewall 5.2 Release Notes** for a comprehensive list of the new software features included with firmware 5.2.

Note



Upcoming release dates will be announced by Barracuda Networks at <https://login.barracudanetworks.com/>.

Known Issues

Note



Advice about known issues is available at <http://www.barracuda.com/kb>.

Bugfixes Included with Barracuda NG Firewall 5.2

Barracuda NG Admin

Table 1–6 Barracuda NG Admin

Description
Under certain circumstances, it could happen that opening a System Settings node within the Repository failed, generating the following error message: Node [path]) - path not found This issue was fixed.
In rare cases, the Send Changes button was erroneously disabled within the Personal Firewall Rules Configuration . This issue was fixed.
A readability issue appearing on a button within the NAC Policy Configuration window was fixed.
A remote management tunnel within the VPN Configuration could not be re-enabled once it had been disabled. This issue was fixed.
It was not clearly visible within Barracuda NG Admin Configuration whether it was disconnected or not. This issue was fixed.
The Open Details dialog window was erroneously positioned far left on the screen. This issue was fixed.
The Statistics Viewer used to crash frequently when the Show button was clicked. This issue was fixed.
The Status Map erroneously displayed orange instead of red icons in Tiles , Icon and List view modes. This issue was fixed.
The Edit window used during the process of setting up an administrator account erroneously asked for entering the password repeatedly. This issue was fixed.
Within the Admin Overview window it was not visible whether an administrator account had been disabled or not. This issue was fixed.
Whitespace characters within the password had erroneously been allowed during creation of administrator accounts. This issue was fixed.
In network objects of Connection type, Weight type entries were erroneously not displayed. This issue was fixed.
Barracuda NG Admin crashed when the search tool was used within a forwarding rule set. This issue was fixed.
The sorting of proxy ARPs was not possible within Control > Network . This issue was fixed.
The Group Policy dialog erroneously displayed the wrong assigned network. This issue was fixed.
In External CA > Group Policy > Group VPN Settings > Preauthentication Details > LDAP Attributes > Enter Name within the VPN configuration, it was erroneously not possible to enter an asterisk (' * ') character. This issue was fixed.
The preselected value within the Redirect field in the Firewall Rule editor was incorrect. This issue was fixed.
On dual-screen systems, Barracuda NG Admin used to freeze when the second monitor was disconnected while the firewall rule editor was displayed there. This issue was fixed.
Barracuda NG Admin used to crash occasionally on systems running Microsoft .NET version 3.5 SP1. This issue was fixed.
With live updating enabled, the log viewer content did erroneously not scroll automatically to the most recent entry. This issue was fixed.
It was not possible to define the network module bay configuration for multi-bay appliances within the box creation wizard. This issue was fixed.

Table 1-6 Barracuda NG Admin

Description
When trying to create a service on a secondary box in an HA environment without activating emergency override mode first, Barracuda NG Admin locked up in reappearing popup messages containing the following error message: Error while loading ConfigWorkspace SetupConfScript: ConfScript failed! This issue was fixed.
A bug within the Copy to Clipboard function and the sorting of elements in input fields of the "collection" type in conjunction with references was erroneously removing references from copied elements. This issue was fixed.
In rare cases, the firewall rule editor crashed on dragging and dropping items within. This issue was fixed.
Refreshing the screen within Box > Control > Network was under certain circumstances erroneously causing the duplication of network routes. This issue was fixed.
Within Box > Control , the Authentication Level dropdown list was erroneously not filled with data. This issue was fixed.
Barracuda NG Admin in disconnected state erroneously showed the last received status data on the status map. This issue was fixed.
Barracuda NG Admin allowed logons to boxes by entering random text additionally to the valid password in certain combinations. Although this was not by any means critical in terms of security because the valid password was always needed, this issue has been fixed.
The IPSec Remote Address field within the Site-2-Site VPN settings was erroneously expecting inverted CIDR notation. This issue was fixed.
Clusters with names starting with "10" were not visible within a range named "1". This issue was fixed.
A rendering issue within certain table headers was fixed.
The Firewall Access Cache did erroneously not remember the sort order in grouped view after the screen was refreshed. This issue was fixed.
Barracuda NG Admin did erroneously not allow the slash ("/") character to be entered into the Plugin field of a firewall service object. This issue was fixed.
Barracuda NG Admin used to crash occasionally on systems running Microsoft .NET version 3.5 SP1. This issue was fixed.
The side bar was erroneously missing within the personal firewall rules screen. This issue was fixed.
In rare cases, refreshing the firewall history screen using the F5 key did not work as intended. This issue was fixed.
A bug prevented the opening of a new log file within the log viewer if the maximum amount of 31 open tabs had been reached and one tab had been closed before. This issue was fixed.
Within the Serial Number field in the Box Configuration , it was erroneously possible to enter the has ("#") character. This issue was fixed.
The Lock / Unlock button did not work as intended within the Box Properties . It was not possible to unlock subsequently to locking. This issue was fixed.
Under certain configuration combinations of local and box time zones, Barracuda NG Admin erroneously generated the following error message: Failed to get local time zone information This issue was fixed.
Cycling through more than 12 open tabs using the << and >> buttons did occasionally not work as intended. This issue was fixed.
Closed sessions were erroneously not removed from the Windows 7 taskbar preview. This issue was fixed.
In certain fields, such as the Domain name of the host on which the service is running field of the Service of Server (SRV) dialog within the DNS Service configuration, it was erroneously not possible to enter a fully qualified domain name. This issue was fixed.
Scrolling through logs in the log viewer did sometimes not work as intended. The position within the log would not change. This issue was fixed.

Barracuda NG Install

Table 1–7 Barracuda NG Install

Description
Barracuda NG Install used to fail when the autorun.inf file could not be written onto a USB pen drive during the installation process. This issue was fixed.

Barracuda NG Firewall

Table 1–8 Barracuda NG Firewall

Module	Description
<i>Access Control Service</i>	The Access Control Service was occasionally restarting without the need to do so, which in turn caused clients to interrupt their health validation. This issue was fixed.
<i>Access Control Service</i>	Firewall offline authentication was not functional when the password contained special characters. This issue was fixed.
<i>Barracuda OS</i>	After an unclean shutdown of a flash-based appliance, syslog files could occasionally not be written anymore after restarting the system. This issue was fixed.
<i>Barracuda OS</i>	On boxes not controlled by a Barracuda NG Control Center and therefore not using centralized time synchronisation, the NTP service could erroneously not synchronize with the time servers provided through pool.ntp.org. There was no time synchronisation available unless an IP address was configured for direct access to a specific time server. This issue was fixed.
<i>Barracuda OS</i>	In release versions prior to 5.0.2 it was erroneously not possible to change the appliance model during server migration. This issue was fixed. It is now possible to change the server model. The only restriction is that flash-based appliances can only be changed to other flash-based appliances, and harddisk-based appliances can only be changed to other harddisk-based appliances.
<i>Barracuda OS</i>	Under certain circumstances, the NTP daemon needed the IP address used for accessing the NTP server having a bind to UDP port 123. This issue was fixed.
<i>Barracuda OS</i>	An issue regarding the system connectivity of USB UMTS modems was fixed.
<i>Barracuda OS</i>	On appliances with LCD, the appliance's serial number was erroneously not shown on the display. This issue was fixed.
<i>Barracuda OS</i>	A problem with the watchdog service was in rare cases causing unwanted reboots. This issue was fixed.
<i>Barracuda OS</i>	The LCD and keypad panel was erroneously not working as intended on certain legacy netfence SR appliances.
<i>Barracuda OS</i>	An issue regarding remote command execution was fixed.
<i>Barracuda OS</i>	Blocked services were under certain circumstances erroneously shown in Started state within SNMP.
<i>Control Center</i>	After clicking Disconnect within the <i>Firewall Audit</i> module, it was not possible anymore to reconnect. This issue was fixed.
<i>Control Center</i>	On C610 appliances, a popup window triggered by the boxnet configuration was repeatedly bothering users with the erroneous message that a different appliance type was detected. This issue was fixed.
<i>Control Center</i>	Non-root administrators were not able to create new administrator users because the <i>New Entry</i> button erroneously was disabled. This issue was fixed.
<i>Control Center</i>	In rare cases, the routing cache on a Control Center could exceed its maximum amount of entries, leading to system instability and the need to reboot the box. This issue was fixed.

Table 1–8 Barracuda NG Firewall

Module	Description
DHCP Service	In very rare occasions, the DHCP service failed when starting and then generated the following error message into the log file: Fatal +0100 /bin/logsetup2 not found, contact support! This issue was fixed.
Firewall	The <code>EPRT</code> FTP command was in rare cases causing a kernel panic. This issue was fixed.
Firewall	Fallback IPs defined in Connection Objects did not work as intended as soon as a route was not available, e.g. because of an interface being down. This issue was fixed, invalid routes are now handled just like disabled routes.
Firewall	An unclear error message was generated into the log file whenever the ACPF module failed to unload: unloading module - FATAL: Module _ not found. This issue was fixed.
Firewall	On boxes with high load it could occasionally happen that packets belonging to active sessions were dropped after a certain uptime until the <code>acpf</code> service was restarted. This issue was fixed.
Firewall	High amounts of firewall sessions passed through the firewall could lead to a blocking effect on FTP sessions after a certain amount of time. It was not possible anymore then to initiate FTP sessions through the firewall. This issue was fixed.
Firewall	The firewall landing page did not work as intended in conjunction with certain URLs. This issue was fixed.
Firewall	Within the firewall's access cache, the names of kernel or accelerated rulesets that had no match were erroneously not listed. Instead, there were entries generated only saying <code><nomatch></code> . This issue was fixed.
Firewall	In rare cases, Traffic Shaping was in conjunction with the HTTP Proxy service causing a kernel panic. This issue was fixed.
Firewall	In rare cases, forwarded inbound TCP packets were incorrectly handled by the firewall, causing a connection reset. This issue was fixed.
FTP Gateway	The FTP Gateway did erroneously not accept groupname strings containing wildcards or partial strings for authentication. This issue was fixed.
FW Audit Log Service	Logging of interface statistics erroneously stopped after a certain amount of entries. This issue was fixed.
HTTP Proxy	Firewall inline authentication had problems authenticating through the proxy. This issue was fixed.
HTTP Proxy	On usage of group ACLs for authentication, the groups were erroneously cached until the proxy service was restarted manually. Therefore, changes to the group ACLs did not become effective after clicking Activate . This issue was fixed.
HTTP Proxy	In rare cases, proxy users did not have groups associated to them due to a database problem. This issue was fixed.
HTTP Proxy	In rare cases and under heavy load, it happened that the proxy memory usage increased far above an acceptable level. This issue was fixed.
VPN Service	The OWA Options button was not accessible in conjunction with a Microsoft Exchange 2010 server. This issue was fixed.
Network	Under certain circumstances, the assignment of routes to a PPP device failed after the modem was reset. This issue was fixed.
Network	Under certain circumstances, a bug prevented the boxnet module to correctly handle country code settings. This issue was fixed.
Network	A missing whitespace in <code>make_box</code> generated a boxnet error message. This issue was fixed.
Network	Network interface bonding stopped working in 5.0.1 if VLAN interfaces were contained within the bond. This issue was fixed.

Table 1–8 Barracuda NG Firewall

Module	Description
<i>Network</i>	It was erroneously not possible to increase the MTU for a VLAN interface. This issue was fixed.
<i>Network</i>	The control daemon crashed when more than 7 multipath gateways were configured. This issue was fixed.
<i>Network</i>	The NTP daemon erroneously did not use the VIP IP table for the synchronizing process. This issue was fixed.
<i>Network</i>	An issue regarding TACACS authentication was fixed.
<i>Secure Web Proxy</i>	A problem in minor release 5.0.1 prevented the filtering of user groups during the authentication process. This issue was fixed.
<i>VPN Service</i>	Due to a bug in the authentication database handler, it could in rare occasions happen that the system became unstable after performing a big amount of firewall authentication processes. This issue was fixed.
<i>VPN Service</i>	Under certain circumstances, broken VPN transports were not appropriately terminated and could therefore crash the VPN service. This issue was fixed.
<i>VPN Service</i>	On standard hardware equipped with newer Intel (Westmere) CPUs it was not possible to use AES256 encryption. This issue was fixed.
<i>VPN Service</i>	The Remote Desktop Java applet erroneously displayed the mouse cursor in black color on certain versions of Windows Terminal Server. This issue was fixed.
<i>VPN Service</i>	Erroneously, it was not possible to use SSL VPN in conjunction with legacy phion SECURE licenses on Barracuda appliances. This issue was fixed.
<i>VPN Service</i>	Boxes having only a low amount of unused RAM left or having strongly fragmented RAM due to intensive system usage were occasionally not able anymore to establish compressed VPN tunnels. This issue was fixed.
<i>VPN Service</i>	Under certain circumstances, Transport Balancing did not work as intended in conjunction with routing mode tunnels. This issue was fixed.
<i>VPN Service</i>	Under certain circumstances, client-to-site VPN sessions were erroneously terminated. This issue was fixed.
<i>VPN Service</i>	An issue regarding the memory consumption of the SSLV VPN engine erroneously increasing over time was fixed.
<i>VPN Service</i>	In rare cases, big amounts of active VPN tunnels could lead to a kernel trace due to a problem with data integrity validation based on the security parameter index (SPI). This issue was fixed.

Barracuda NG Network Access Client

Table 1–9 Barracuda NG Network Access Client

Description
Under certain circumstances it occasionally happened that secure routes were lost. This issue was fixed.
Rendering issues in the client software concerning visual selections after a screen refresh were fixed.
In rare cases, the virtual adapter reconnected using an erroneous IP address after it had attended sleep mode. This issue was fixed.
Due to a problem with socket handling, it occasionally happened that the health agent crashed. This issue was fixed.
The health validator occasionally crashed during the VPN authentication process in conjunction with erroneous initialization of the authentication process through the Access Control server. This issue was fixed.
In rare cases, a problem with the VPN Access Control server regarding source NAT occurred. This issue was fixed.
An issue regarding x509 in conjunction with current user store certificates was fixed.
After disconnecting and then reconnecting to a different VPN server without network access protection, the health agent used an erroneous IP address list for reconnecting which could result in connecting attempts to the wrong Access Control server. This issue was fixed.
The VPN client erroneously requested the Access Control server's IP address before the internal VPN state engine was finished with NATting the Access Control server. This issue was fixed.
Erroneously appearing password retrieval dialogs were removed.
With the <i>Use Access Control Service</i> option set to Yes in a profile of a Barracuda NG Network Access Client VPN-only installation it was only possible to establish one successful connection unless the client was unloaded and restarted. This issue was fixed.
An issue regarding fast VPN reconnecting was fixed.
In 64-bit versions of Microsoft Windows, the configuration object for the VPN client profiles was not displayed within the system's control panel. This issue was fixed.
Reconnecting the VPN client was not correctly visualized by the tray icon. This issue was fixed.
In rare cases, certain devices could not bind to UMTS interfaces. This caused malfunctions of the personal firewall in conjunction with these devices. The issue was fixed.
Under certain circumstances it could happen that the automatic deinstallation of clients that had been installed in unattended mode was not possible. This issue was fixed.
An issue with the health agent generating an <code>Access violation</code> error was fixed.
Health validation was erroneously using too much bandwidth over slow VPN connections. This issue was fixed.
In rare cases, the health agent crashed with an application error during the system shutdown. This issue was fixed.
The 32-bit and 64-bit versions of the client had problems with the removal of host routes on Windows Vista and Windows 7 systems. This issue was fixed.
Occasionally, client errors appeared in conjunction with the reading of certain x509 certificates. This issue was fixed.
Occasionally it happened that terminating a VPN connection needed more time than necessary. This issue was fixed.
The client was erroneously not able to create or modify its registry entries when running without administrator rights. This issue was fixed.
In rare cases, the health agent was freezing. This issue was fixed.
With two manually assigned IP addresses for Access Control servers of which the first one was not reachable, the health agent displayed the wrong health state although the fallback mechanism itself worked as intended. This issue was fixed.
Occasionally, the VPN client displayed an error dialog saying <code>No Certificate loaded</code> after typing the password followed by clicking Connect . This issue was fixed.

Table 1–9 Barracuda NG Network Access Client

Description
The VPN client used to freeze after pressing the Alt key for a minimum of two times while left-clicking into the side bar. Restoration was possible by clicking the client's instance within the task bar. Furthermore, the Connect and Close buttons were not displayed as intended after pressing the Alt key. These issues were fixed.
Erroneously, it was not possible to validly choose Blowfish as encryption method within the client. This issue was fixed.
The client in VPN-only mode was under certain circumstances consuming more CPU time than necessary due to the installation of unneeded components. This issue was fixed.
An issue regarding the client's checking for the Access Control server connection while in offline mode was fixed.
A parse error occasionally appeared in the system report in conjunction with the client's virus checking engine. This issue was fixed.
Up to now there was no health validation performed on the client subsequently to adapter changes. This issue was fixed.
After locking the client system followed by entering a wrong password to unlock it again, the wrong password was under certain circumstances internally used by the credential provider, generating unwanted behavior. This issue was fixed.
The closure process of the tray icon of the client triggered by a system logout or shutdown caused the watchdog service to restart the tray icon which in turn produced unwanted results such as the "Force Shutdown?" system dialog or shutdown-and-restart loops of the tray icon. This issue was fixed.
In rare cases it could happen that the client service was hanging during system startup. Under certain circumstances, this was causing several other system malfunctions mainly on Windows Vista. This issue was fixed.
An issue regarding the uninstallation of certain drivers was fixed.
The Firewall Always On checkbox did not work as intended. This issue was fixed.
The personal firewall's rule editor did erroneously not display IP addresses and subnets within destination dropdowns. This issue was fixed.
Right-clicking to open the context menu within an existing VPN profile was in certain cases crashing the client. This issue was fixed.
Under certain circumstances, custom MOTD images were not displayed within the client. Instead, the default image showed up. This issue was fixed.
An issue that could lead to a crash during the deinstallation of a component was fixed.
When externally linked x509 certificates were used, the client crashed whenever it was closed and then re-opened, followed by cancelling the password request dialog of the x509 certificate and clicking on My Account . This issue was fixed.
Under certain circumstances, x509 certificates created using Barracuda NG Admin couldn't be used with the client. This issue was fixed.
Personal firewall plugins were erroneously not checked for an empty plugin name definition. This issue was fixed.
There was no firewall check for captured firewall packets. This issue was fixed.
The client's tray icon menu performed slow under Windows 7 with enabled visual effects. This issue was fixed.
Barracuda NG Access Client installed on Windows XP in VPN-only mode generated the following error event into the system's application error log at every restart: Error while open I/O to phionvpn.sys (ErrorNr=2) The System can't find the stated file Although this did not affect operations by any means, this issue was fixed.
The health agent erroneously displayed error messages if a Access Control server was not reachable, although fallback servers worked as intended. This issue was fixed.
Although No Access Control Server was set in a profile, a route to a Access Control server was introduced. This issue was fixed.
The transparent agent did erroneously not support the <code>-version</code> command. This issue was fixed.
Certain issues regarding the adding of Access Control server routes and the connecting and disconnecting speed of the client were fixed.

Table 1–9 Barracuda NG Network Access Client

Description
Locally configured VPNs using proxy ARP did under certain circumstances erroneously prevent the client from establishing a connection. This issue was fixed.
The client's registry check erroneously failed when a certain registry key was missing. This issue was fixed.
Dead gateways erroneously remained within the client's internal connection map. This issue was fixed.
The process of initializing a VPN connection through the client was too slow due to an issue with the Access Control server validation. This issue was fixed.
The health agent was due to a problem with the internal database in rare cases exiting with an access violation error. This issue was fixed.
Access Control server triggered blocking processes within the client could in certain cases lead to an authentication dialog although no authentication was necessary. This issue was fixed.
With multiple anti-virus scanning engines installed, the health agent was in certain cases erroneously immediately revalidating the system's health state. This issue was fixed.
In very rare cases in conjunction with a certain NIC type, the health monitor could crash on startup. This issue was fixed.
In certain cases, it was erroneously not possible to deactivate the personal firewall on-the-fly if the client system had been rated as untrusted by the health agent. This issue was fixed.
Opening the ruleset selector within the personal firewall was in rare cases freezing the application window. This issue was fixed.
The client was erroneously trying to reconnect while e.g. system checks were performed. This issue was fixed.
The client was erroneously not checking the connectivity during reconnection processes in conjunction with one-time passwords. This issue was fixed.
The registry monitoring direct access mode was erroneously not capable of being disabled at runtime. This issue was fixed.
Domain checks were erroneously only performed for the default VPN profile. This issue was fixed.
The VPN Service could occasionally not locate UDP ports 53 and 5355 within the internal UDP list. This issue was fixed.
The tray icon menu description in VPN-only mode was not correctly displayed. This issue was fixed.
Due to the fact that during VPN shutdown both an adapter reset and a system check is performed and interfered with each other, the termination process was erroneously slowed down. This issue was fixed.
Users for profiles without user authentication were erroneously remembered by the client. This issue was fixed.
Certain checks for installed client components were missing. This issue was fixed.
Ethernet headers were missing in incoming packets from certain WWAN adapters. This issue was fixed.
Certain pop-up dialogs generated by the tray icon were not hideable by the user. This issue was fixed.
Disabled virtual adapters were under certain circumstances erroneously causing disabled tray icon menu items. This issue was fixed.
The registry monitor did erroneously not recognize changes to the registry flags <code>VPNAdapterAlwaysON</code> and <code>tcpdump</code> . This issue was fixed.
In certain cases, the OS was not forward DNS requests to the virtual adapter. This issue was fixed.
An issue regarding blocking IPs and adapter monitoring was fixed.
The client was after reconnecting not always able to resolve DNS entries. This issue was fixed.
A popup regarding quarantining was displayed although the health agent was configured to not notify the user in such cases. This issue was fixed.
Dynamic adapter handling was in certain cases erroneously fed with incorrect IP addresses. This issue was fixed.
An issue regarding the local storage of x509 keys was fixed.

Table 1–9 Barracuda NG Network Access Client

Description
When a VPN was active without making use of a Access Control server, then the local Access Control server validation was not working as intended. This issue was fixed.
The 64-bit version of the health agent did in version 2.0 SP2 under certain circumstances not work as intended. This issue was fixed.

Note



Further minor bugfixes may exist that have been fixed but are not listed here.

Determine Your Update Scenario

Caution As soon as a box has been updated to firmware version 5.2 and, subsequently, any new features were configured using Barracuda Ng Admin 5.2, **no configuration changes must be made anymore using older versions of Barracuda NG Admin!** Doing so could destroy the configuration.
Always use Barracuda NG Admin 5.2 together with Barracuda NG Firewall 5.2.



Caution On flash appliances, please remove all USB devices except the installation USB thumb drive before initiating the installation process. Otherwise, the following error message may occur:



An error occurred finding the installation image on your hard drive. Please check your images and try again.

Caution If the update is performed remotely, Barracuda Networks strongly recommends to **be prepared for on-site access to the box** in case the update process fails. The person on-site should have access to the appliance via a serial console or a prepared USB stick in order to start a system recovery.



Note



Updating to Barracuda NG Firewall 5.2 is possible from release version 5.0 and newer. Direct updating from release versions prior to 5.0 is not possible. Update to 5.0 first.




Note



In order to use Microsoft Exchange 2010 via SSL VPN after updating to Barracuda NG Firewall 5.2, it is necessary to perform **Activate** at least once within the **SSL VPN** settings in Barracuda NG Admin to correctly apply the update to the SSL VPN engine.

Before beginning the updating process, you should clarify which types of hardware and administrative configuration you have. Barracuda NG Firewall 5.2 allows different administrative configurations. Please follow those update instructions applying to your configuration.

Table 2–10 Different Administrative Configurations

Administrative Configuration Type	Applicable Update Instructions
<p>Unmanaged Box or Control Center</p> 	<p>If you want to update either an unmanaged box or a Control Center, then proceed to Updating Unmanaged Boxes or Control Centers, page 21.</p>
<p>Control Center Managed Box</p> 	<p>If you want to update a box that is managed by a Control Center, then proceed to Updating Control Center Managed Boxes, page 24.</p> <p>If you also need to update a cluster or a range of CC-managed boxes, proceed subsequently to Migrating Cluster / Range Config to 5.2, page 26.</p>
<p>Box or Control Center combined with HA Box</p> 	<p>If you want to update a box or a Control Center (that is combined with a High Availability (HA) box), then proceed to Updating HA-Synced Boxes or HA-Synced Control Centers, page 22.</p> <p>If you also need to update a cluster or a range of CC-managed boxes, proceed subsequently to Migrating Cluster / Range Config to 5.2, page 26.</p>

Note



See **Supported Hardware, page 5** to determine whether your Barracuda hardware qualifies for a supported installation of or a supported update to Barracuda NG Firewall 5.2.

If you are going to update so-called "standard hardware" from a firmware version prior to 5.0, please follow the instructions given in [Updating Standard Hardware from 4.2.x to 5.2, page 27](#).

Combining Barracuda NG Control Center 5.2 with 5.0 and/or 4.2 Boxes

The table below shows compatibility between the firmware's major versions.

Table 2–11 Firmware compatibility

		Barracuda NG Control Center Version			
		netfence management centre 4.2	Barracuda NG Control Center 4.2	Barracuda NG Control Center 5.0	Barracuda NG Control Center 5.2
Box Version	netfence 4.0	✓	-	✓	✓
	netfence 4.2	✓	-	✓	✓
	Barracuda NG Firewall 4.2	-	✓	✓*	✓*
	Barracuda NG Firewall 5.0	✓**	✓**	✓	✓
	Barracuda NG Firewall 5.2	-	-	✓**	✓

* Already existing boxes only; introduction of new boxes, especially new Barracuda appliances is not possible.

** Configuration sent from the Barracuda NG Control Center to the box is automatically migrated on the box. Newly introduced features of the respective release can't be configured. The managed box migrates the configuration automatically by itself and sets initial default values for newly introduced configuration items.

Solving Update and Installation Failures

If a box does not boot into normal operation mode after update or installation, certain BIOS settings might be misconfigured. In this case, reset the BIOS configuration by performing the following steps:

- **Establish a serial console connection to the box (19200 bit/s).**
- **Switch the appliance on and hold the *Del* key during the boot-up RAM test. Wait until the BIOS screen appears.**
- **If the BIOS screen does not appear, hold *ALT* and simultaneously press *0* on the numeric keyboard. Then, release *0* again while still holding *ALT* and, again simultaneously, press *9* on the numeric keypad, followed by releasing *9* and finally also releasing *ALT*. The BIOS screen should appear.**
- **Within the BIOS menu, select and execute *Set to optimal defaults*.**
- **Save the new settings, exit the BIOS and reboot the appliance.**

Updating Unmanaged Boxes or Control Centers



Updating Boxes or Control Centers using SSH

Best Practice



For speed reasons, Barracuda Networks recommends using this method of updating for all appliances in general, especially for those based on a flash drive or slower hardware.

Step 1: Copy

Before copying the package onto the box as described below, make sure that there is no old minor release or patch package lurking within the `/var/phion/packages/` directory. The directory must not contain any files.

Although the `/var/phion/packages/` directory must be empty, it still contains the subdirectories: `kl`, `os`, `ph`, `sa`, `tgz`. These don't affect the updating process. Furthermore, there must not be a whitespace character within path or file name of the package.

- **Copy the update package onto your firewall system into the `/var/phion/packages/` directory of the respective box.**

To get the file onto the box, you may use the [Send File](#) button within the built-in SSH client of Barracuda NG Admin. Don't forget to change the directory first using `cd /var/phion/packages/`.

Step 2: Update

Start the update sequence by executing `phionUpdate` from the shell.

No more interaction is necessary. Wait until the update is finished. Depending on the hardware, it will need from 15 minutes on the fastest appliances up to 60 minutes on the flash appliances.

Warning



Do not interrupt the update procedure. During update, the box boots several times and due to this, the connection will be terminated. Indicators that the update process has been finished are the following output on the console:
Barracuda NG Firewall release 5.2.0-xxx, or the operativeness of logging in again using SSH or Barracuda NG Admin.

Updating HA-Synced Boxes or HA-Synced Control Centers



In the instructions below, the term "primary box" refers to the box used for regular operation, while "HA box" refers to the secondary box used as a failover system.

Caution



If you plan on updating only either the primary or the HA box, not both ones, then please ensure that the box not to be updated is running 5.0.x. Firewall and Configuration HA synchronizing is not possible between release version 5.2 and release versions below 5.0.

Barracuda Networks strongly recommends to follow the procedure for updating HA systems exactly as described below in order to minimize any operational drop outs.

Step 1: Prepare the HA Box

- **Log-in to the HA box using Barracuda NG Admin.**
- **Block the (standby) server on the HA box within [Control > Server](#).**

Step 2: Update the HA Box

- **Update the HA box using SSH as delineated in [Updating Boxes or Control Centers using SSH, page 21](#).**

No more interaction with the HA box is necessary. Wait until the update is finished. Depending on the hardware, it will need from 15 minutes on the fastest appliances up to 60 minutes on the flash appliances.

Warning



Do not interrupt the update procedure. During update, the box boots several times and due to this, the connection will be terminated. Indicators that the update process has been finished are the following output on the console:
Barracuda NG Firewall release 5.2.0-xxx, or the operativeness of logging in again using SSH or Barracuda NG Admin.

Step 3: Switch Servers to the HA Box and Prepare the Primary Box

- **Log-in to the primary box using Barracuda NG Admin.**

Proceed after having assured that the HA box is fully functional.

- **Unblock the (standby) servers on the HA box by clicking [Stop Server](#) within [Control > Servers](#).**
- **Log-in to the primary box using [Barracuda NG Admin](#).**
- **Switch all servers from the primary to the HA box and verify for correct operability. Therefore, [Block all Servers](#) on the primary box.**

You may leave the primary box in standby mode until correct operability of the HA box has been verified. Click [Stop Server](#) on the primary box in order to achieve this. If functional errors occur on the HA box, you may switch servers back to the primary box.

Step 4: Update the Primary Box

- **Update the primary box using SSH as delineated above in [Updating Boxes or Control Centers using SSH](#), page 21.**

No more interaction with the primary box is necessary. Wait until the update is finished. Depending on the hardware, it will need from 15 minutes on the fastest appliances up to 60 minutes on the flash appliances.

Warning



Do not interrupt the update procedure. During update, the box boots several times and due to this, the connection will be terminated. Indicators that the update process has been finished are the following output on the console:
Barracuda NG Firewall release 5.2.0-xxx, or the operativeness of logging in again using SSH or Barracuda NG Admin.

Step 5: Switch Servers Back to the Primary Box

- **Log-in to the respective primary box using [Barracuda NG Admin](#).**

Proceed after having assured that the primary box is fully functional.

- **Re-enable all servers on the primary box by clicking [Stop Server \(Control > Server\)](#) on each.**
- **Log-in to the HA box using [Barracuda NG Admin](#).**
- **Block all the servers on the HA box by clicking [Block Server \(Control > Server\)](#).**

Proceed after having assured that the primary box is fully functional.

- **Set all the servers on the HA box back to standby by clicking [Stop Server \(Control > Server\)](#).**

The update process is finished.

Updating Control Center Managed Boxes



To make use of the multi-release capabilities of Barracuda NG Control Center, all boxes within one cluster must run under the same software major release version. Migration of the CC configuration is only available for all boxes, servers and services of a cluster simultaneously.

Step 1: Import the Update Package into the Control Center

- **Log-in to the Barracuda NG Control Center using Barracuda NG Admin.**
- **Navigate to *Control > Firmware Update* and click *Import...***
- **Select the update package within the file browser.**

Step 2: Select Boxes to Update and Send them the Update

- **Choose the desired *Range, Cluster or Box*.**
- **Select the previously copied update within the *Files* list.**
- **Click *Create Task...***
- **Choose *Immediate Execution* from the *Scheduling* drop-down menu and click *OK*.**

Step 3: Execute the Copied Update

- **Navigate to *Control > Update Tasks*.**
- **Verify if the update package was successfully copied, which is indicated by a green icon within the Σ column.**
- **Right-click the desired box and select *Perform Update* followed by choosing *Immediate Execution* from the *Scheduling* drop-down menu and clicking *OK*.**

No more interaction with the box is necessary. Wait until the update is finished. Depending on the hardware, it will need from 15 minutes on the fastest appliances up to 60 minutes on the flash appliances.

Warning

Do not interrupt the update procedure. During update, the box boots several times and due to this, the connection will be terminated. Indicators that the update process has been finished are the following output on the console:



Barracuda NG Firewall release 5.2.0-xxx, or the operativeness of logging in again using SSH or Barracuda NG Admin.

Note

Take a look into the box log file at **Box > Logs > Box\Release\update** after the update process has been finished. In case of a not succeeded update please consult **Box\Release\update_hotfix** for a detailed log.



Migrating Cluster / Range Config to 5.2

Note that cluster migration must be completed before features inherent to Barracuda NG Firewall 5.0 can be administered by the CC. So, only **after all boxes of a specific cluster have been updated** to Barracuda NG Firewall 5.0, configuration migration may be executed on the Control Center.

The minimum administration entity in a multi-release environment is a cluster, thus the migration process must be performed in one step for at least one whole cluster within a range.

Step 1: Lock Cluster or Range

- ***Lock the cluster or range to update.***

The context menu of the locked range or cluster now offers an entry named *Migrate Range/Cluster*.

Step 2: Select Migrate Range or Migrate Cluster

- ***Choose either Migrate Range or Migrate Cluster.***
- ***Subsequently to selecting this, select release version 5.0 within the following dialogue window.***

After confirming by clicking **OK**, the selected cluster or range is migrated.

Note



Especially for large clusters or ranges it may take more time to perform all migration steps.

Step 3: Review and Activate Future Configuration

Configuration nodes that are going to be changed during the migration process are tagged with a "Changed" icon. Configuration nodes that are going to be deleted will be tagged with a "Deleted" icon.

- ***Carefully review the changes before activating them in the next step.***
- ***Click **Activate** to activate new configuration.***

The migration process is finished.

Updating Standard Hardware from 4.2.x to 5.2

General

Due to a kernel version change between 4.2.x and 5.2 (linux kernel 2.4 was changed to linux kernel 2.6), the enumeration of NICs may on some hardware sort the ethX devices in a different order, resulting in a loss of management access.

Therefore, a procedure has now been implemented to rename the interfaces after upgrading to 5.2 to stay identically with the 4.2.x interface names. This is done by creating an interface mapping table using the eth device's MAC addresses as identifiers.

The following procedure **must be performed on every single box separately** due to the fact the MAC addresses are different per box and so will be the mapping table.

If you find out later that your server is not affected by the resorting issue, then you may delete the mapping configuration subsequently. The network activation log will then contain the following message:

```
No difference found between configured and detected MAC to interface mapping
```

- ***Update is possible on standalone as well as on CC-managed boxes from firmware 4.2.0 onwards to major release version 5.0. No direct updating to 5.2.x is possible!***
- ***Updates from a base release in the range from 4.2.0 to 4.2.14 requires a hotfix to be installed. 4.2.15 includes the functionality and no hotfix is required.***
- ***It is recommended to evaluate the process on a system with physical access or in a lab environment in case the upgrade fails.***
- ***The procedure is compatible with user defined interface mappings. If a user defined interface mapping is found, it will be applied after the MAC-to-eth mapping procedure.***
- ***If you add additional NICs after upgrading to 5.0, the mapping may fail. Therefore, do not use MAC mapping in this case any longer but switch to user defined interface mapping. The problem may occur if linux detects the new NICs before it detects the old ones.***

Updating Procedure

Step 1: Prepare the Standard Hardware For the Update

- ***If the box runs on firmware 4.2.14 or below, you must install the hotfix `boxnet_mac2ifmapping-386-4.2.14`.***

Step 2: Generate the Mapping Data

- **Log-in to the box via ssh as root and issue the following command:**
`CreateMACMapping`
Running this program multiple times will do no harm.
- **Copy the output lines of the program beginning with `CM` and those beginning with `CI` to the clipboard.**

Step 3: Apply the Mapping Data

- **On standalone boxes, open the [Box Network Configuration](#) within Barracuda NG Admin.**
On CC-managed boxes, open the [Box Network Configuration](#) within Barracuda NG Admin on the respective Barracuda NG Control Center.
- **Paste the content of the clipboard to [Network > Interfaces > MAC Mapping](#) (only visible in [Advanced configuration mode](#)).**
- **Set [Use Assignment](#) to [yes](#).**
- **Click [Send Changes](#) followed by [Activate](#).**

Step 4: Proceed to the Update

- **Upgrade the box following the 5.0 upgrade procedure as described in the separately available [Barracuda NG Firewall 5.0 Migration Instructions](#). Please download this document from <http://www.barracudanetworks.com/ns/support/documentation.php>.**
- **Subsequently, you may update from 5.0 to 5.2 following the procedures as described in [Determine Your Update Scenario](#), page 18.**

When the update process is finished, please verify if all interfaces are correctly mapped.

Note



In case the linux kernel 2.4 assigned the interfaces in the same order as the linux kernel 2.6 did, the following message will be generated into the 5.0 box network activation log:

```
No difference found between configured and detected MAC to interface mapping
```

In this case you may disable MAC mapping. This will make the configuration hardware-independent, providing you with more flexibility in case hardware will be changed somewhere in the future.

Note



Further advice about updating standard hardware is available through the Barracuda Networks support.

