Barracuda SSL VPN Release Notes 2.4

https://campus.barracuda.com/doc/2458468/

Before installing any firmware version, be sure to make a backup of your configuration and read all release notes that apply to versions more recent than the one currently running on your system.

Do not manually reboot your system at any time during an upgrade, unless otherwise instructed by Barracuda Networks Technical Support. The update process typically takes only a few minutes after the update is applied. The appliance web interface for the administrator will usually be available a minute or two before the SSL VPN user interface. If the process takes longer, please contact Technical Support for further assistance.

Upgrading to Version 2.x

- **When upgrading from version 2.3 (or earlier) firmware:**
  - Backups taken from earlier firmware versions will NOT restore properly with the new backup/restore functionality found starting in version 2.4. Make new backups after the firmware update.
- **Mapped Drives:**
  - WebDAV is now the default method for providing Mapped Drives and configuration settings have been changed accordingly. Windows 7 and Vista 64-bit clients will be prompted to uninstall the current Dokan driver and also given the option to increase the maximum file download size to 2GB when launching Mapped Drives.
  - Client Certificates will need to be disabled when launching WebDAV Mapped Drives.
  - Version 2.3.1.013 is not compatible with systems that are clustered.
- **When upgrading from version 2.1 firmware:**
  - Replacement Proxy Web Forwards for OWA that were created prior to version 2.2 are no longer supported. If you have one, you will need to replace it using the new OWA Template. Go to the RESOURCES > Web Forwards page and delete the old Web Forward. Then create a new one using the Mail Web Forward category.
  - When configuring Barracuda Network Connector on Macintosh systems, note that DNS insertion and Up/Down commands are mutually exclusive.

What's new with the Barracuda SSL VPN Version 2.4.0.13

- Fix: High severity vulnerability: non-persistent XSS, unauthenticated [BNSEC-1546 / BNVS-4210]
- Fix: Medium severity vulnerability: non-persistent XSS, [BNSEC-2660 / BNVS-47759]
- Fixed Java jar signing to conform to security in Java 1.7u51 [BNVS-4787]

What's new with the Barracuda SSL VPN Version 2.4.0.12

- Fix: Clustering on new systems [BNVS-4678]
- Fix: High severity vulnerability: non-persistent XSS [BNSEC-2802 / BNVS-4542]
- Fix: High severity vulnerability: persistent XSS [BNSEC-2697 / BNVS-4543]
- Fix: Unknown severity vulnerability: [BNSEC-380]
- Fix: Unknown severity vulnerability: [BNSEC-335]

What's new with the Barracuda SSL VPN Version 2.4.0.10

- Fix: External access blocked for non SSH ports [BNVS-4152]
- Fix: The most recent Scheduled Backup files are retained [BNVS-4614]
- Fix: High severity vulnerability: Unauthenticated, non-persistent XSS [BNSEC-1546 / BNVS-4210]
- Fix: High severity vulnerability: Unauthenticated, non-persistent XSS [BNSEC-1542 / BNVS-4211]
- Fix: High severity vulnerability: Clickjacking [BNSEC-509 / BNVS-4024]
- Fix: Med severity vulnerability: Cross Site Request Forgery (CSRF) [BNSEC-1247 / BNVS-4079]
- Fix: Med severity vulnerability: URL Redirection [BNSEC-727 / BNVS-3665]
- Fix: Low severity vulnerability: Requires a man in the middle, url redirection [BNSEC-1399 / BNVS-4147]
- Fix: Low severity vulnerability: Requires authentication, non-persistent XSS [BNSEC-1239 / BNVS-4078]
- Fix: Low severity vulnerability: Cross Site Request Forgery (CSRF), HTTP header injection, non-persistent X SS [BNSEC-1144 / BNVS-4026]

What's new with the Barracuda SSL VPN Version 2.4.0.9

New Features

- The Device Configuration feature allows resources and other settings configured on the Barracuda SSL VPN to be provisioned directly to a user's device.
- Improved Sharepoint functionality, including supporting Sharepoint 2013.
- Policy time restrictions are more comprehensive.
- Improved browser NAC checking.
- Download functionality for all aspects of the system works faster and more reliably.
- Increased backup and restore capabilities (from the appliance interface).

Version 2.4.0.9 Fixes:

- **Backups**
  - Show All Backups option on the ADVANCED > Backups page displays all backup files on the share [BNVS-4348]
  - Only the requested number of SMB backups is stored [BNVS-4378]
  - Status of SMB backup is reported accurately [BNVS-4376]
  - Clustering information is excluded from backups [BNVS-4382]
- **Other**
  - All Network Connector client configurations can be launched from the user interface [BNVS-4381]
  - Fixed Java applet signing to conform to new security in Java 1.7u45 [BNVS-4516]
    Note: This error may still appear if the SSLVPN doesn't have a valid SSL certificate installed. A valid SSL certificate will be required for all SSL VPN devices as of the release of Java 1.7u51

Version 2.4.0.7:

- Fix: Mapped drives time out according to the inactivity timeout setting under Profiles [BNVS-4337]
- Fix: Attempts to access hosts not in the Web Forward Allowed Hosts list displays error message [BNVS-4319]
- Fix: Can log off users with Network Connector sessions using the Sessions page [BNVS-4322]
- Fix: Set limitations on IP subnet range for PPTP and IPSec [BNVS-4325]
- Fix: Updated Code Signing Certificate
- Fix: Vulnerability - Information Disclosure [BNSEC-1839 / BNVS-4261]
- Fix: Vulnerability - Unauthenticated, XSS-Not Persistent [BNSEC-1542 / BNVS-4211]
- Fix: Vulnerability - Unauthenticated, XSS-Not Persistent [BNSEC-1546 / BNVS-4210]
- Fix: Vulnerability - Requires Man in the Middle, URL Redirection [BNSEC-1399 / BNVS-4147]
- Fix: Vulnerability - CSRF [BNSEC-1247 / BNVS-4079]
- Fix: Vulnerability - Authenticated, XSS-Not Persistent [BNSEC-1239 / BNVS-4078]
- Fix: Vulnerability - CSRF, HTTP Header Injection, XSS-Not Persistent [BNSEC-1144 / BNVS-4026]
- Fix: Vulnerability - Click Jacking [BNSEC-509 / BNVS-4024]
- Fix: Vulnerability - URL Redirection [BNSEC-727 / BNVS-3665]

Version 2.4.0.3:

- Feature: Bookmark aliases are created automatically for new and existing resources
- Fix: Server Agent service starts on Linux [BNVS-4244]
- Fix: Improved ActiveSync session disconnection handling [BNVS-4243, BNVS-4263]
- Fix: Prevent files that were in tmp directory from being deleted when they should not have been [BNVS-4188]
- Fix: Enabled uploading of certificates with PKCS #8 private keys [BNVS-4235]
- Fix: Account selection works correctly for Read Only mode Active Directory groups when using

Internet Explorer [BNVS-4217]
- Fix: My Resources filter displays correct selection [BNVS-4258]
- Fix: Creating a new Certificate Authority is possible after deleting an existing one [BNVS-4233, BNVS-4255]
- Fix: Ssladmin session information is displayed correctly on clustered systems [BNVS-4225]
- Fix: Correction to AD password expiry message [BNVS-3591]
- Fix: Improvements to Microsoft Sharepoint 2013 checkout discard in Microsoft Office 2007 and 2010 [BNVS-4184]

Version 2.4.0.2 Fixes:

- **Graphs**
  - Graphs display correctly in Internet Explorer version 10 [BNVS-4030]
- **Web Forwards**
  - Path based web forwards display large pages containing multi-byte characters accurately [BNVS-4196]
  - Web sites that switch between character encodings display extended chars (??, ??, etc.) correctly [BNVS-4102]
  - Launching a Host File Redirect Tunneled Web Forward in Windows 7 closes the Command prompt window [BNVS-4101]
  - Sharepoint 2010 documents can be edited [BNVS-4132]
- **IPsec/PPTP**
  - Timeout option added for IPsec/PPTP sessions [BNVS-4155]
  - When launching PPTP, if the connection already exists then a confirmation message is not displayed [BNVS-4194]
  - IPsec PSK can include all valid symbols [BNVS-4081, BNVS-4125]
- **Mapped Drives**
  - Webdav Mapped Drives do not timeout due to inactivity [BNVS-4090]
  - Session timeout will disconnect Mapped Drives [BNVS-4128]
  - Office 2013 documents work with Mapped Drives [BNVS-3778]
- **Sessions**
  - Password can be entered after session has been locked due to browser closure [BNVS-4144]
- **Server Agent**
  - The ADVANCED > Server Agents page refreshes correctly when an agent is enabled or disabled in Internet Explorer version 10 [BNVS-4119]
  - Zip file containing the server agent client contains the correct version [BNVS-4120]
  - Server Agent service starts on Linux [BNVS-4244]
- **Other**
  - Improved notifications message handling under heavy load [BNVS-4058]
  - NAC antivirus checking detects status of multiple installed AV products [BNVS-4099]
  - Network Connector routes can be added in macOS [BNVS-4100]
  - Authentication schemes and NAC exceptions consider policy time restrictions [BNVS-3455]

- /32 CIDR notation is handled correctly by IP authentication [BNVS-3818]