
How to Install the Barracuda NACv50 Light

<https://campus.barracuda.com/doc/75696512/>

Installed in NACv50 Light mode, the Barracuda VPN Client can enforce Windows Security Center settings on client machines running Windows 7, Windows 8, or Windows 10, so that only healthy clients are allowed to connect. The client security settings are validated via the Barracuda CloudGen Firewall VPN service without requiring the Barracuda Personal Firewall or the Barracuda Health Agent to be installed on the client machines.

Before You Begin

On the Barracuda CloudGen Firewall, create and configure a VPN service for client-to-site VPN connections. For instructions, see [Client-to-Site VPN](#). You will select the Windows Security settings via the Barracuda CloudGen Firewall VPN service.

Step 1. Install the Barracuda VPN Client on the Client Machines

On the client machines to be managed, install the Barracuda VPN Client with one of the following methods:

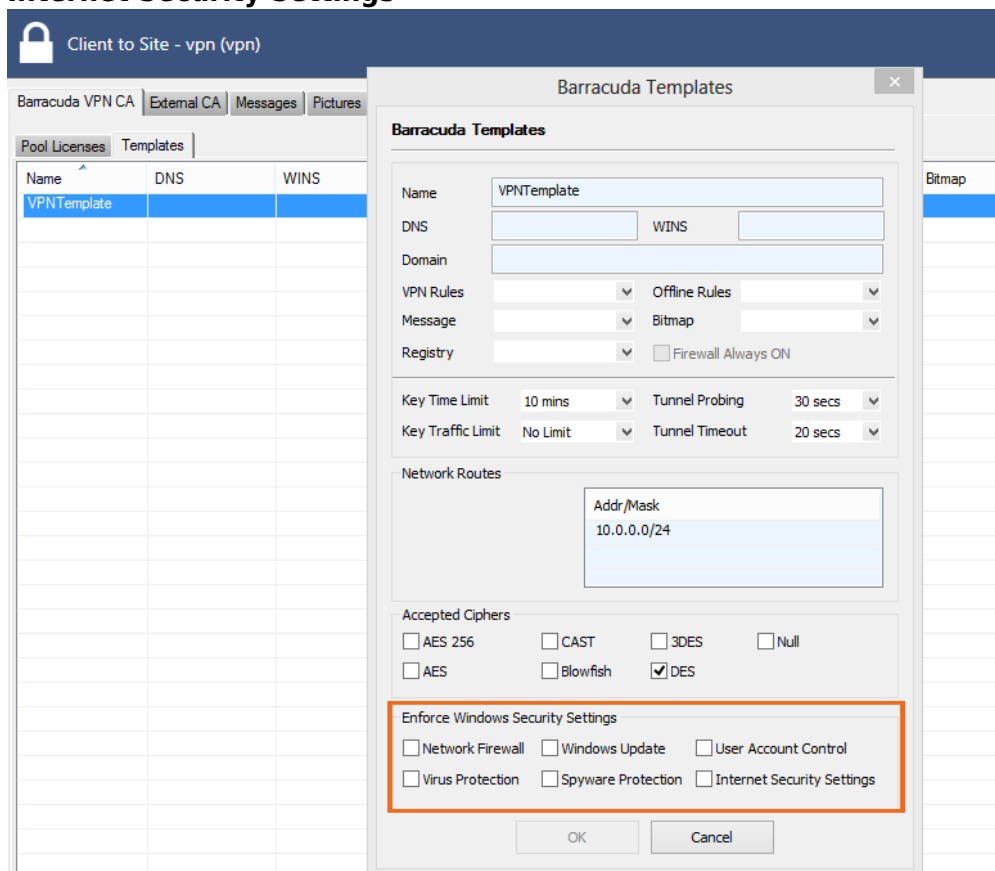
- **Preconfigured Remote Custom Installation** – For instructions, see [Fully Preconfigured Custom Installation](#).
Use at least this parameter:
 - **PROGTYPE=VPN** – Selects the VPN-only installation mode.
- **VPN-Only Installation** – The interactive standard installation process. For instructions, see [How to Install the Barracuda Network Access/VPN Client for Windows](#). Select **VPN Client** as the only feature to be installed.

Step 2. Select the Windows Security Settings to Enforce

In your client-to-site VPN template, select the Windows security settings to enforce on client machines.

1. In Barracuda Firewall Admin, go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > your VPN service > Client to Site**.
2. From the **Barracuda VPN CA** tab, click the **Templates** tab.
3. Click **Lock**.

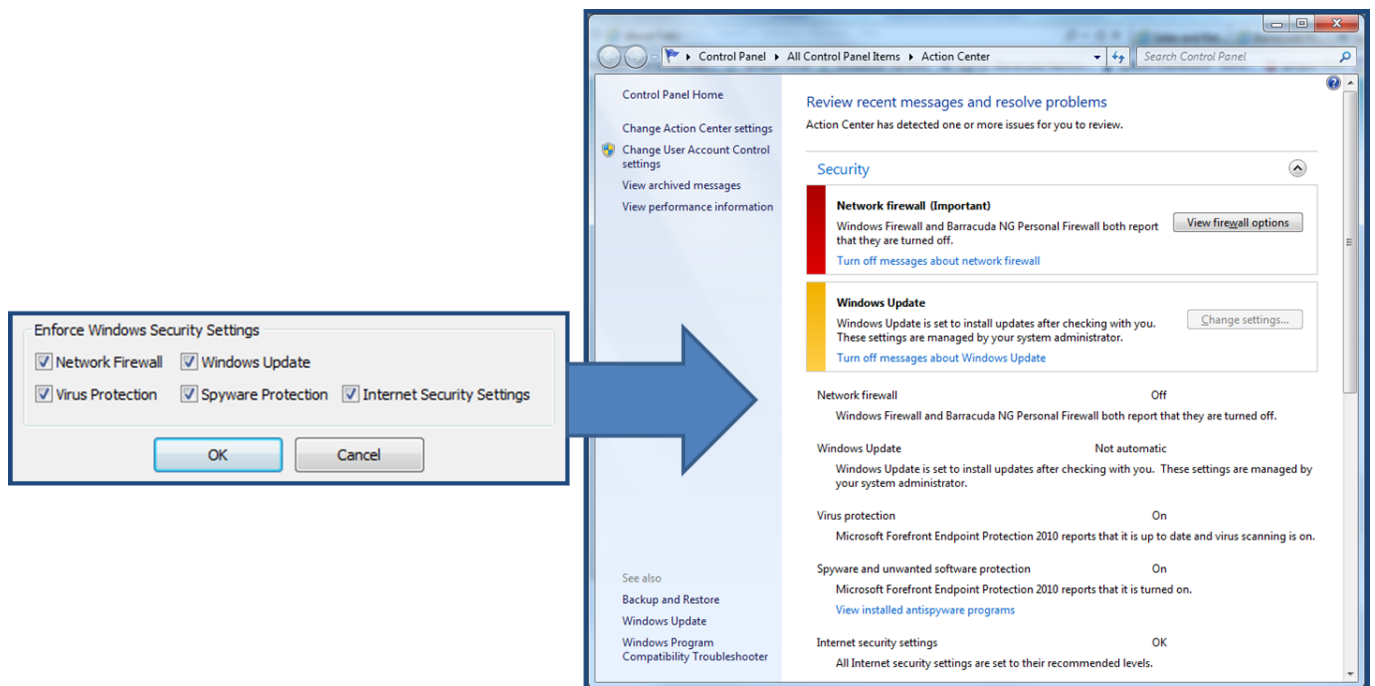
4. Double-click the template.
5. In the **Enforce Windows Security Settings** section of the **Barracuda Templates** window, select the security settings that you want to enforce:
 - **Network Firewall**
 - **Windows Update**
 - **User Account Control**
 - **Virus Protection**
 - **Spyware Protection**
 - **Internet Security Settings**



The screenshot shows the Barracuda VPN Client interface. The 'Barracuda Templates' window is open, displaying various configuration options. The 'Enforce Windows Security Settings' section is highlighted with an orange box. This section contains six checkboxes: Network Firewall, Windows Update, User Account Control, Virus Protection, Spyware Protection, and Internet Security Settings. The 'Accepted Ciphers' section shows that AES, Blowfish, and DES are selected. The 'Network Routes' section shows a single route for 10.0.0.0/24. The 'Key Time Limit' is set to 10 mins, and the 'Key Traffic Limit' is set to No Limit. The 'Tunnel Probing' is set to 30 secs, and the 'Tunnel Timeout' is set to 20 secs. The 'Firewall Always ON' checkbox is unchecked.

6. Click **OK**.
7. Click **Send Changes** and **Activate**.

The next time that the Barracuda VPN Client connects to your server, it will query the client machine's Windows Action Center settings while initiating the connection. The connection will only be established if these settings meet the Windows Security settings that you configured in the VPN service.



The Windows Security option "Windows Update" will only check if Windows updates are configured to be installed automatically on the client machine. It does not consider any information regarding the installation status of certain updates or the overall update status of the system. As the Windows Update configuration option "Never check for updates" is no longer available on Windows 10, enforcing the "Windows Update" option will not have any effect on client machines running Windows 10.

The Windows Security option "Spyware Protection" can no longer be used starting with Windows 10, version 1607, as the status for anti-spyware is no longer tracked by Windows.

Figures

1. nac_light01.png
2. nac_light02.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.