How to Install the Barracuda NAC Light

https://campus.barracuda.com/doc/46206646/

Installed in NAC 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 Access Monitor to be installed on the client machines.

Before You Begin

On the 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 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, including the full list of possible parameters, see Partially Preconfigured Unattended Remote 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. S elect **Barracuda VPN Client** as the only feature to be installed.
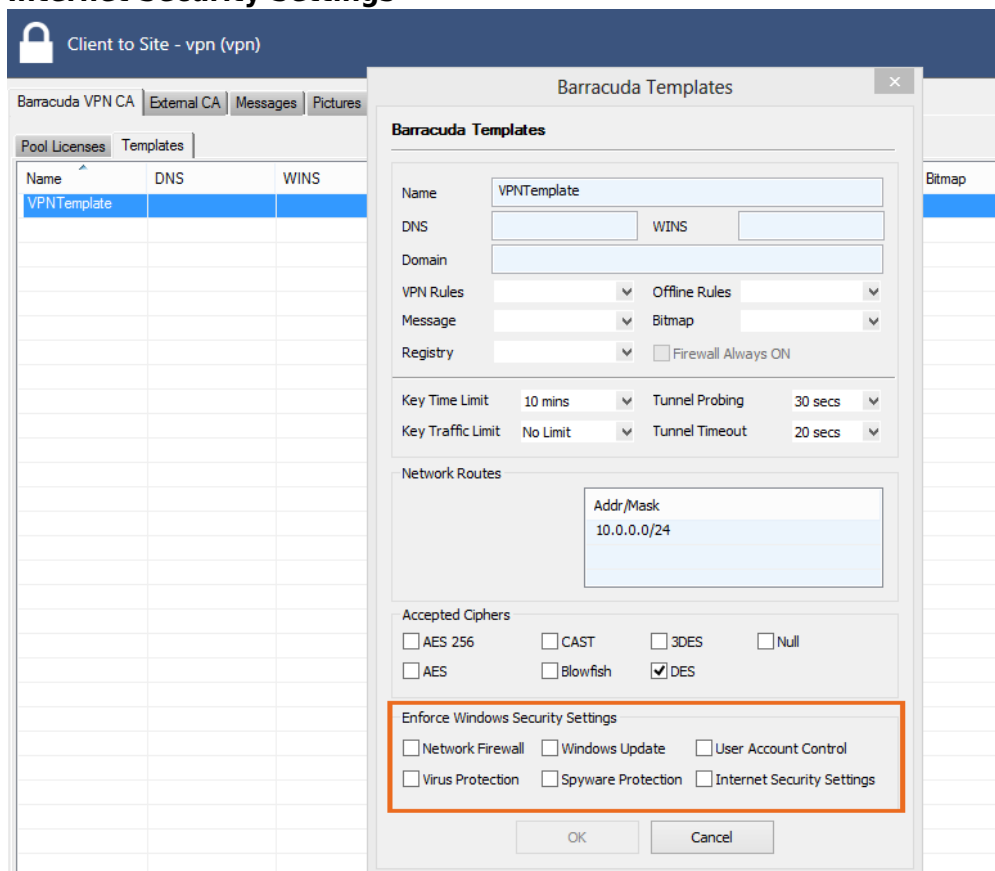
Step 2. Select the Windows Security Settings to Enforce

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 > Virtual Servers > *your virtual server* > 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**

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.
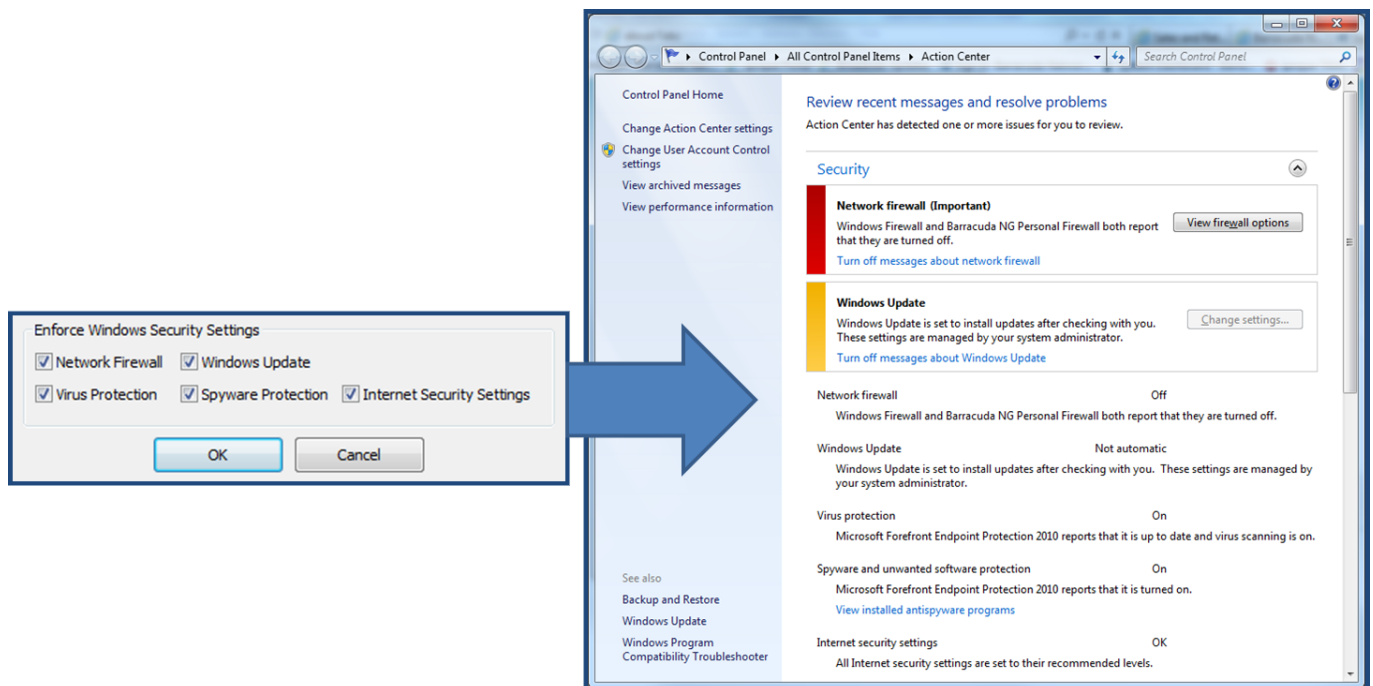
The Windows Security option "Windows Update" will only check if Windows updates are configured to be installed automatically on the client machine. It does not consider any information regarding the installation status of certain updates or the overall update status of the system. As the Windows Update 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.

Figures

1. nac_light01.png
2. nac_light02.png