How to Configure NAC for SSL VPN

https://campus.barracuda.com/doc/73700203/

SSL VPN Network Access Control (NAC) limits access to the web portals of the SSL VPN service according to a variety of factors based on attributes of the connecting device. Users who fail the NAC check are not allowed to log in until they have a conforming system. You can define policies for each category. Configure the firewall to allow or block specific NAC categories, subtypes, and versions. NAC settings do not apply to clients connecting via CudaLaunch. The following parameters are evaluated by the SSL VPN service when the user logs in:

- Desktop operating systems
- Mobile operating systems
- Desktop browser types and versions
- Browser plugins
- Mobile browser types and versions

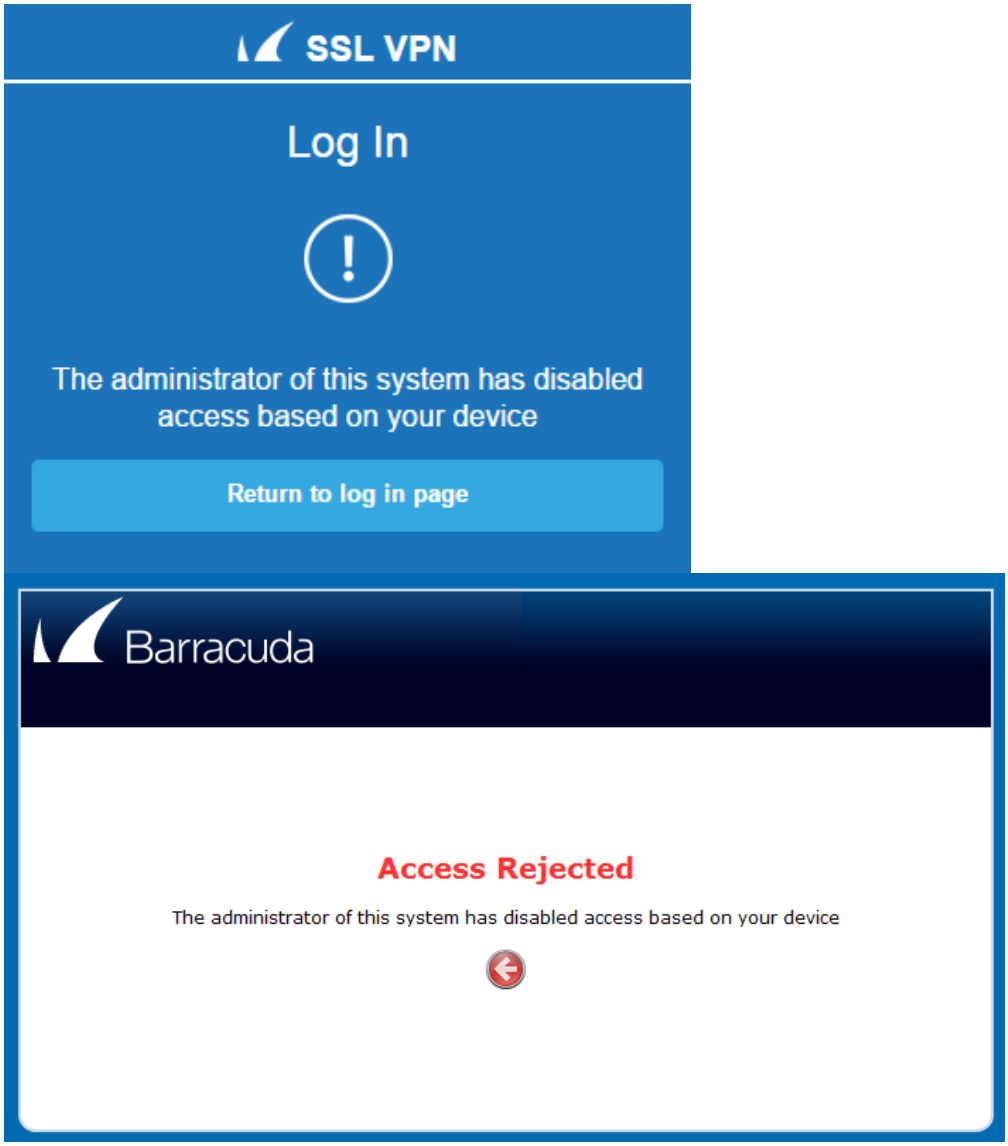
Before You Begin

Enable and configure SSL VPN on the firewall. For more information, see How to Configure the SSL VPN Service.

Configure the NAC Block List

1. Go to **VPN > SSL VPN**.
2. Click the **NAC** tab.
3. Click **Add Criteria**. The **Add Network Access Control Criteria** window opens.
4. Set **Enable** to **Yes**.
5. For each **NAC Category**, select the versions that should be blocked or allowed:
    1. Enter a **Name** for the rule.
    2. Select the **Access** policy.
    3. Select the **NAC Category**. The subtype for the selected category is displayed. For example, the mobile browser type if you selected **Mobile Browser**.
    4. Select the **Type** and **Version** for the category you previously selected.
6. Click **Save**.

All users accessing the SSL VPN web portals must now conform to the requirements set in the NAC block list. When a user logs in with a device that fails one or more of the server-side NAC checks, the following block pages are displayed:



Check the **sslvpn** log file to find out which NAC block rule caused the user to be rejected. For more information, see Logging.

Figures

1. NAC_block_mobile.png
2. NAC_block_desktop.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.