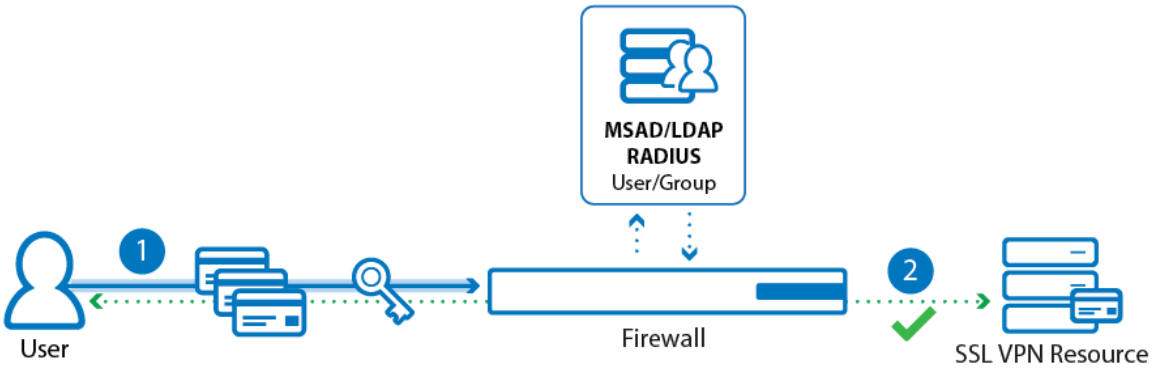
How to Configure Access Control Policies for Multi-Factor and Multi-Policy Authentication

https://campus.barracuda.com/doc/68358839/

Multi-Policy Authentication (MPA) is a configurable combination of Access Control Policies (ACPs) that are evaluated upon login. Multi-Policy Authentication contains group memberships, SSL VPN Network Access Control (NAC) criteria, and authentication schemes. To use Multi-Factor Authentication (MFA), add multiple authentication schemes to the Access Control Policy. The Access Control Policy must be active and added to the login configuration of the SSL VPN. The user can then choose between the available Access Control Policies when accessing the SSL VPN service via web portal or CudaLaunch. The 'Use Identity' scheme will use the authentication scheme set as the identity scheme in the login configuration page.



Before You Begin

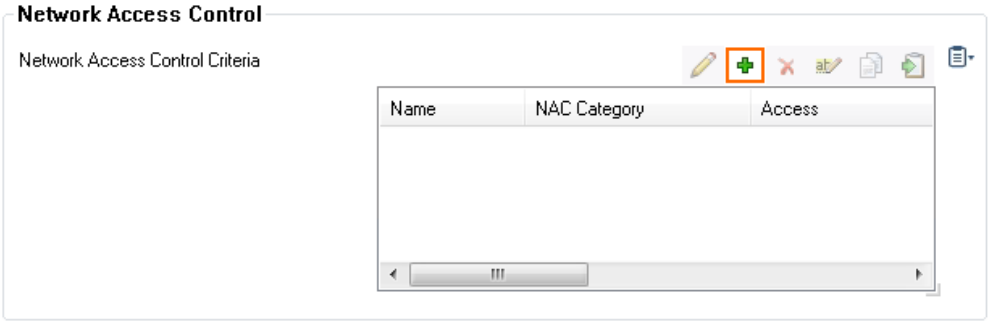
- Configure authentication schemes for your external authentication services. For more information, see Authentication.
- Configure the SSL VPN service. For more information, see How to Configure the SSL VPN Service.

Step 1. (optional) Configure Network Access Control Criteria

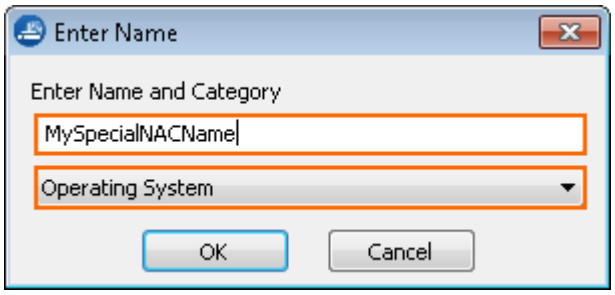
Define NAC criteria to be used in the Access Control Policies .

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Service > VPN-Service > SSL-VPN**.
2. In the left menu, click **Access Control Policies**.
3. Click **Lock**.

4. For each **Network Access Control** criterion:
    1. Click **+** to add a **Network Access Control** criterion.



    2. Enter the name for the NAC criterion.
    3. Select the category from the list:
        - **Operating System**
        - **Browsers**
        - **Browser Plugins**
        - **CudaLaunch Access**



    4. Click **OK**.
    5. Configure the Network Access Control Criteria:
        1. **Operating System** as category (Currently applies only to browser access, not CudaLaunch access):
            - **Active** – Select the check box.
            - **Access** – Select **Allow** or **Block**.
            - **Operating System Type** – Select the operating system to allow or block from the list.
            - (optional) **Version** – Select the version number.
        2. **Browser** as category:
            - **Active** – Select the check box.
            - **Access** – Select **Allow** or **Block**.
            - **Browser Type** – Select browser type from the list.
            - (optional) **Version** – Select the version number.
        3. **Browser Plugin** as category:
            - **Active** – Select the check box.
            - **Access** – Select **Allow** or **Block**.
            - **Plugin Type** – Select **All**, **Flash**, **Java**, or **Silverlight**.
            - (optional) **Version** – Select the version number.
        4. **CudaLaunch Access** as category:
            - **Active** – Select the check box.

- **Access** – Select **Allow** or **Block**.

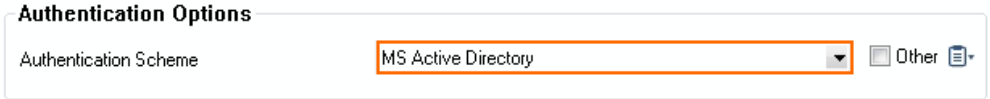
5. Click **OK**.
6. Click **Send Changes** and **Activate**.

Step 2. Configure Access Control Policy

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Service > VPN > SSL-VPN**.
2. In the left menu, click **Access Control Policies**.
3. Click **Lock**.
4. Click **+** to add an **Access Control Policy**.
5. The **Access Control Policies** window opens.
6. Enter the name for the Access Control Policy.
7. Click **OK**.
8. In the **Access Control Policy** section, select the **Active** check box to activate the authentication scheme.

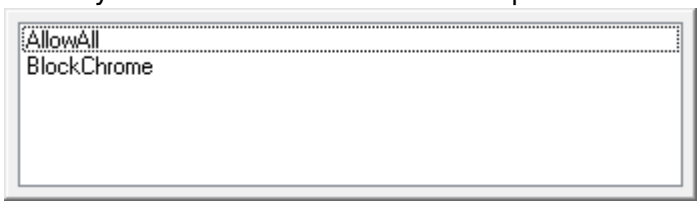
9. In the **Group Access** section, click **+** to add **Allowed Groups** and **Blocked Groups**.
   In **Allowed Groups**, either add an asterisk (*) to have the **Access Control Policy** processed for all groups, or enter a group name. Note that an empty box blocks the **Access Control Policy**.
   In **Blocked Groups**, enter a group name for groups to be blocked.
10. For each Access Control Policy, define one or more authentication schemes:
    1. Click **+** to add an **Authentication Scheme**.

    2. In the **Authentication Schemes** window, select the **Authentication Scheme**.



    3. Click **OK**.
11. (optional) Define SSL-VPN NAC criteria:
    - In the **Network Access Control** section, click **+**.

- Select your NAC criteria created in step 1.



12. Click **OK**.
13. Click **Send Changes** and **Activate**.

Step 3. Set the Login Access Control Policy

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Service > VPN-Service > SSL-VPN**.
2. In the left menu, click **Login**.
3. For each Access Control Policy you want to add to the SSL VPN service:
   1. Click **+** to add your access control policy to the list of **Access Control Policies**.

   2. Select the access control policy from the pop-up menu.
4. (optional) Configure the following settings as needed:
   - **Use Max Concurrent Users** – Enable to limit the number of simultaneous users using the SSL VPN service.
   - **Max Concurrent Users** – Enter the maximum number of users that can be simultaneously connected to the SSL VPN service.
   - **Session Timeout (Min)** – Enter the session timeout in minutes.
   - **Authentication Request Timeout (sec)** – Enter a value up to 20 seconds if you are using multi-factor authentication.
   - **Deny Remember Me** – Set to **yes** to remove the **Remember me** check box on the login page.
5. Customize the login messages and logos:
   - (optional) Import a 200 x 66 PNG or JPG image to customize the **Logo**.
   - (optional) Enter a plain text **Login Message**. E.g, `Welcome to the Barracuda`

`NextGen Firewall SSL VPN`.
- (optional) Enter an HTML **Help Text**.

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

Figures

1. auth_01.png
2. add_nac_entry_00.png
3. specify_nac_name_cat_00.png
4. activate_auth_scheme_00.png
5. add_authentication_scheme_00.png
6. add_auth_scheme_msad_00.png
7. add_nac_to_access_control_policy_00.png
8. select_from_popupmenu_nac_00.png
9. add_access_control_policy_00.png