

How to Configure VPN Group Policies in the SSL VPN

<https://campus.barracuda.com/doc/96026104/>

By adding group-policy-based VPN group policies to your CloudGen Firewall SSL VPN resources, you can let end users self-provision the VPN clients on their Windows, macOS, or iOS devices. Users then only need to log into their desktop or mobile portal and click the provisioning link. By default, the VPN group policy uses session and user attributes for single sign-on. The downloaded file automatically configures the Barracuda VPN client or iOS VPN client, depending on the operating system. Currently, VPN files containing personal license files (*.lic) cannot be uploaded.

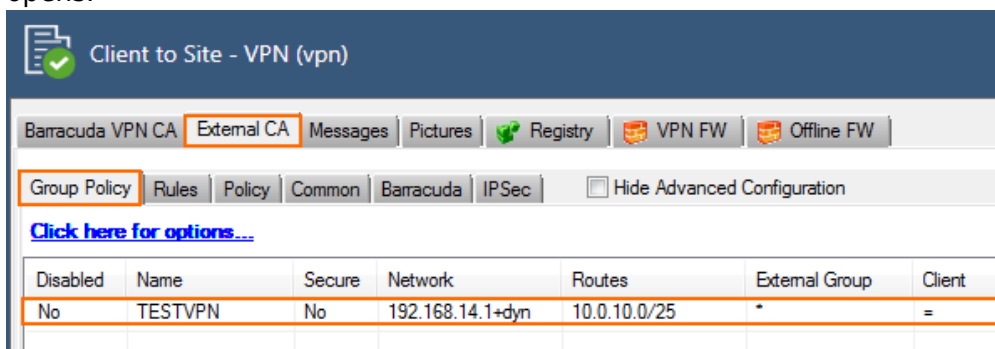
Before You Begin

- Configure a Client-to-Site VPN group policy. For more information, see [Client-to-Site VPN](#).
- (macOS X and Windows only) Install the Barracuda VPN Client. For more information, see [Installing the Barracuda Network Access/VPN Client for Windows](#).

Step 1. Export the Client-to-Site VPN Group Policy

Download the VPN group policy (*.vpn) file from the Client-to-Site configuration.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > Client-to-Site**.
2. Click the **External CA** tab.
3. In the **Group Policy** tab, double-click on the VPN group policy. The **Edit Group Policy** window opens.



4. Click **Export to file**. The **Export VPN Profile** window opens.

09 Subject	Cert Policy / OID	Peer	
	/ =		

Export to file ... OK Cancel

5. Enter a new **Description**.
6. Enter the IP address of the **VPN Server**.
7. Click **OK**.

Export VPN Profile

Description: C2S_VPN_Template

Prompt for credentials	No
Remember User name	No
Subject	
Transport Mode	Reliability (TCP)
Use Access Control Service	No
Use MS Credential Manager	No
VPN Server	62.99.0.222
Virtual Adapter Configuration IPv4	Direct assignment

OK Cancel

8. **Save** the file.

Step 2. Create a VPN Group Policy Resource

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > SSL-VPN**.
2. In the left menu, select **VPN Group Policy**.
3. Click **Lock**.
4. Click **+** to add a new **VPN Group Policy**.
5. Enter a **Name** and click **OK**. The **VPN Group Policy** window opens.
6. Enter the **Display Name**.
7. (optional) To restrict access to the VPN files by user group, replace the * entry in the **Allowed User Groups** list. Click **+** to add new user groups.
8. Click **Ex/Import** and select **Import from File**.
9. Select the VPN group policy file you exported in step 1.
10. (SSO only) Enter a session or user attribute for the **Username** and **Password**. For more information, see [How to Use and Create Attributes](#).

Uploaded VPN Group Policy Files

Active	<input checked="" type="checkbox"/>	
Display Name	<input checked="" type="checkbox"/> Client to Site VPN	
Allowed User Groups	<div><div></div><div></div></div>	
.VPN File	<input checked="" type="checkbox"/> Ex/Import DATA set	
Custom Icon	<input type="checkbox"/> Ex/Import No data set	
Username	<input type="text" value="{session.username}"/>	
Password	<input type="text" value="{session.password}"/>	

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

VPN Self-Provisioning

To configure the VPN clients on their desktop or iOS device, users can access the VPN group policies through either the SSL VPN web portals or CudaLaunch. Clicking on the VPN group policy resource adds the policy to the VPN client installed on the device. For CudaLaunch on mobile devices, the VPN connection is fully managed by the app, including updating the VPN profile if the VPN file attached to the group policy in the SSL VPN is changed. For Windows and macOS devices, the VPN connection for the Barracuda VPN Client can be downloaded directly from CudaLaunch or the web portal, but VPN configuration changes are not synced.

- [CudaLaunch](#)
- [Self-Service VPN Provisioning for iOS Devices](#)
- [Self-Service VPN Provisioning on Microsoft Windows](#)
- [Self-Service VPN Provisioning on macOS](#)

Figures

1. vpnfiles00.png
2. vpnfiles01.png
3. vpnfiles02.png
4. vpnfiles03.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.