How to Configure SSL VPN VPN Apps

https://campus.barracuda.com/doc/79462856/

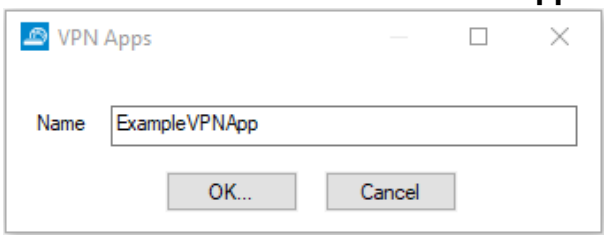
VPN Apps for the SSL VPN are used to allow users to connect to internal web applications not suitable for SSL VPN Web Apps or native apps. CudaLaunch transparently opens a client-to-site VPN tunnel and then opens the resource in the default browser. Depending on your requirements, you can restrict the VPN connection to be available only for VPN Apps. For Windows clients, both CudaLaunch and the Barracuda VPN client must be installed; for iOS and Android, CudaLaunch is required.

Before You Begin

- Configure both SSL VPN and client-to-site VPN:
  - Configure a client-to-site VPN group policy. For more information, see How to Configure a Client-to-Site VPN Group Policy.
- Configure a VPN group policy for the SSL VPN. For more information, see How to Configure VPN Group Policies in the SSL VPN.

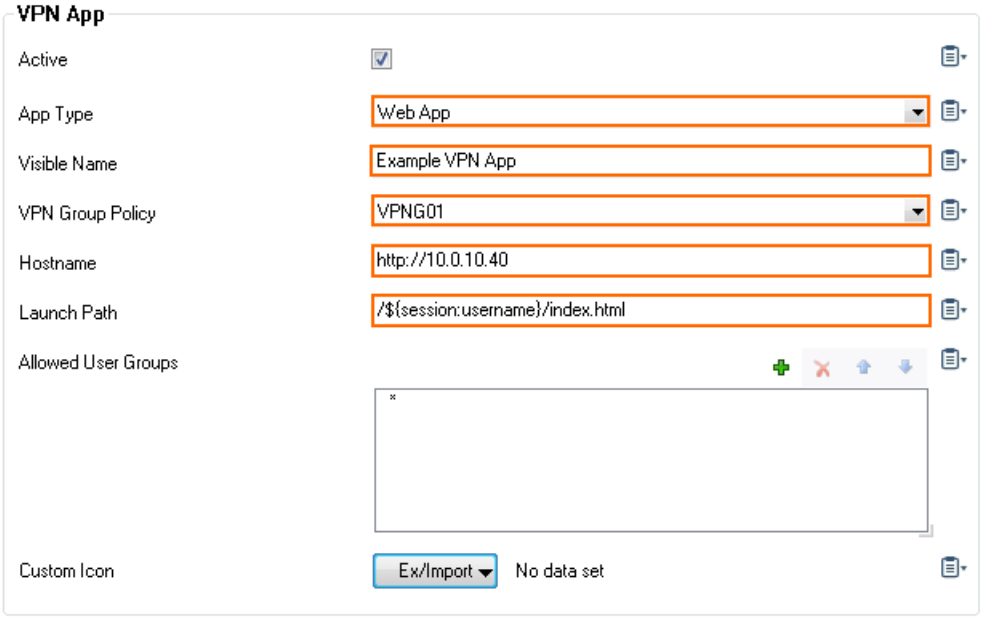
Step 1. Configure a VPN App for SSL VPN

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > SSL-VPN**.
2. Click **Lock**.
3. In the left menu, select **VPN Apps**.
4. In the **VPN Apps** section, click **+** to add a VPN App to the list.
5. Enter a **Name** and click **OK**. The **VPN Apps** window opens.



6. Configure the VPN App:
   - **App Type** – Select **WebApp**.
   - **Visible Name** – Enter the user-facing name for this app.
   - **VPN Group Policy** – Select the VPN group policy. This policy must already be uploaded as a VPN group policy for the SSL VPN service. For more information, see How to Configure VPN Templates in the SSL VPN.
   - **Hostname** – Enter the hostname for the internal web application in the following format: Protocol type (`http://` or `https://`) followed by the FQDN or IP address of the web server. E.g., `http://your.domain.com` or `https://10.10.10.10`
     Launch Path – Enter "/" followed by the path and file name you want to request when

starting the VPN App. Hash characters (#) in the launch path must be replaced by `[hash]`. You can also include user or session attributes in the launch URL. E.g., `/wiki/${session:username}/ or /lunchmenu/${user:location}/index.php` For more information on attributes, see How to Use and Create Attributes.

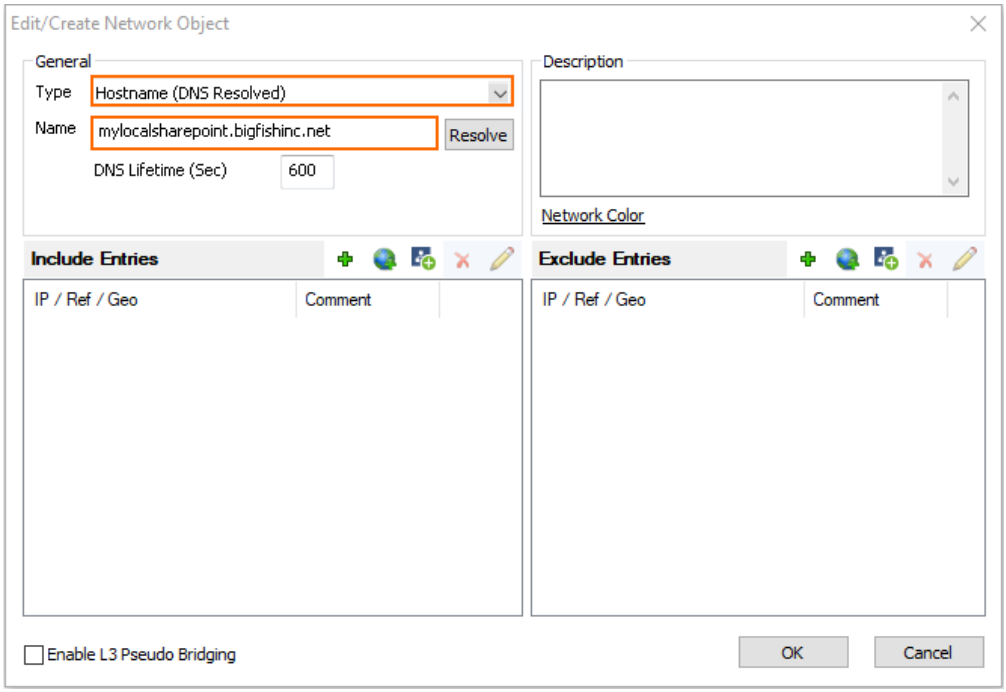


7. (optional) To restrict access to the web app by user group, replace the * entry in the **Allowed User Groups** list. Click **+** to add new user groups.
8. (optional) Click **Ex/Import** to upload a custom icon.
9. Click **Send Changes** and **Activate**

Step 2. Create a Network Object for the VPN App Resources

Create a network object containing all IP addresses, hostnames, and networks containing the servers and services that the user needs access to when accessing the VPN resource.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. In the left menu, click on **Networks**.
3. Click **Lock**.
4. Right-click the table and select **New**. The **Edit/Create Network Object** window opens.
5. For each VPN App, create a network object containing all IP addresses, hostnames and networks required by the VPN App.
   - **Type** – Select **List of IPv4 Addresses** or **Hostname (DNS resolved).**
   - **Name** – For hostname network objects, enter the FQDN; for a list of IPv4 addresses, enter the name.
   - **Include Entries** – For each IP address, click **+** to add it to the list.



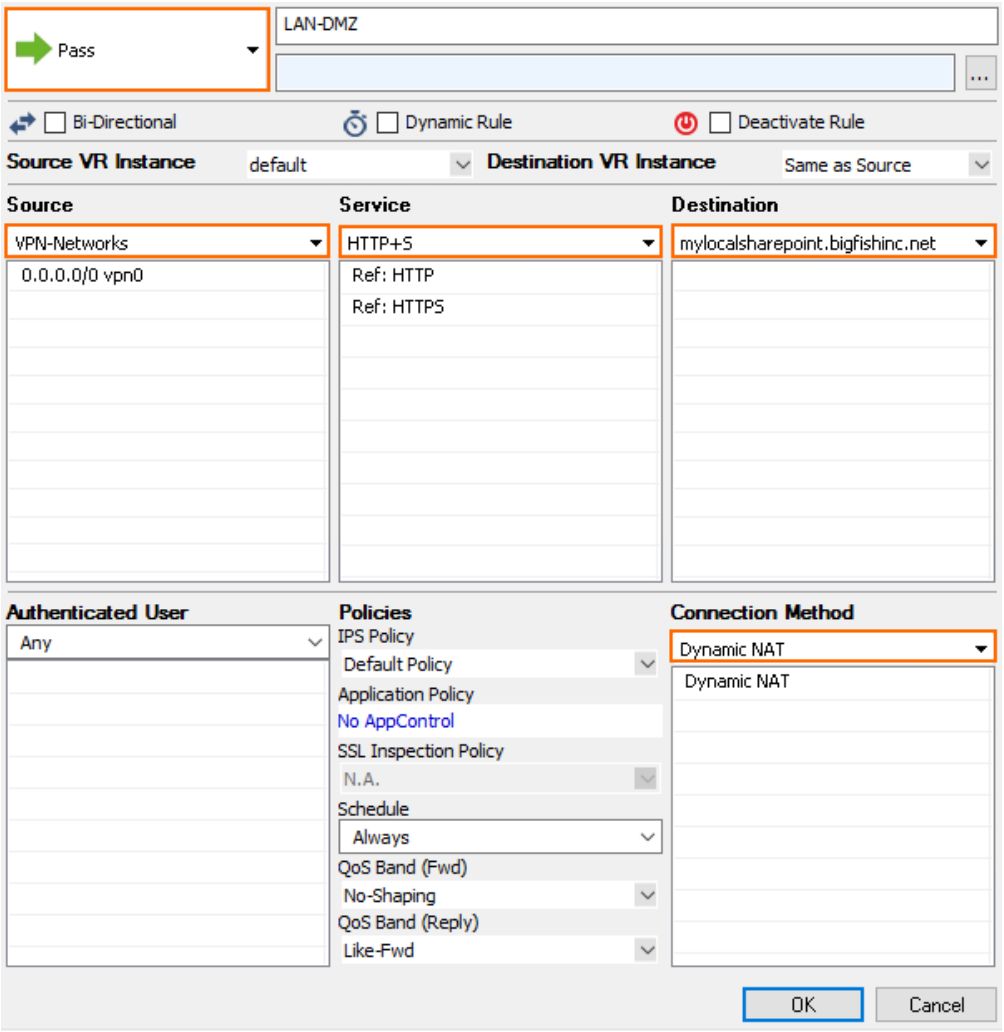
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

Step 3. Add Access Rules for VPN App Resource

Add access rules to allow connections from the client-to-site VPN to the internal resource that is accessed through the VPN App. Since the user has access to all resources allowed via access rules when connected to the client-to-site VPN, these access rules should be as restrictive as possible.

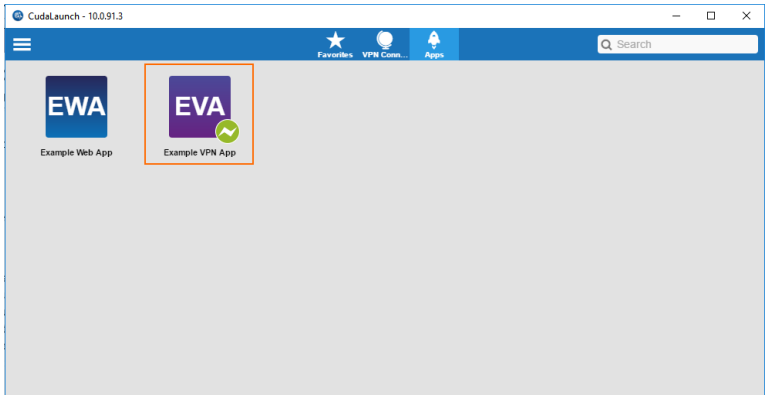
1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Either click the plus icon (**+**) at the top right of the ruleset, or right-click the ruleset and select **New > Rule**.

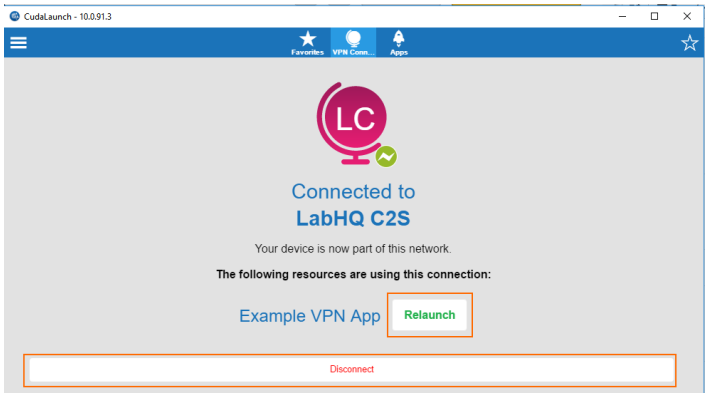
4. Select **Pass** as the action.
5. Enter a name for the rule.
6. Specify the following settings that must be matched by the traffic to be handled by the access rule:
    - **Source** – Select the network object containing the VPN client network.
    - **Service** – Select **HTTP+S**.
    - **Destination** – Select the network object configured in Step 2.
    - **Connection Method** – Select **Dynamic NAT**.



7. Click **OK**.
8. Drag and drop the access rule so that it is the first rule that matches the traffic that you want it to forward. Ensure that the rule is located *above* the BLOCKALL rule; rules located below the BLOCKALL rule are never executed.
9. Click **Send Changes** and **Activate**.

The users can now access the internal resource by clicking on the VPN App in CudaLaunch for Windows, iOS, or Android. After the connection is established, the web application is opened automatically in an external browser window. Go to the **VPN Connections** tab to disconnect from the client-to-site VPN.


CudaLaunch - 10.0.91.3
Favorites
VPN Conn...
Apps
Search
EWA
Example Web App
EVA
Example VPN App


CudaLaunch - 10.0.91.3
Favorites
VPN Conn...
Apps
LC
Connected to
LabHQ C2S
Your device is now part of this network.
The following resources are using this connection:
Example VPN App
Relaunch
Disconnect

Figures

1. vpnapp_01.png
2. vpnapp_02.png
3. vpnapp_03.png
4. FW_Rule_Add01.png
5. vpnapp_04.png
6. vpnapp_05.png
7. vpnapp_06.png