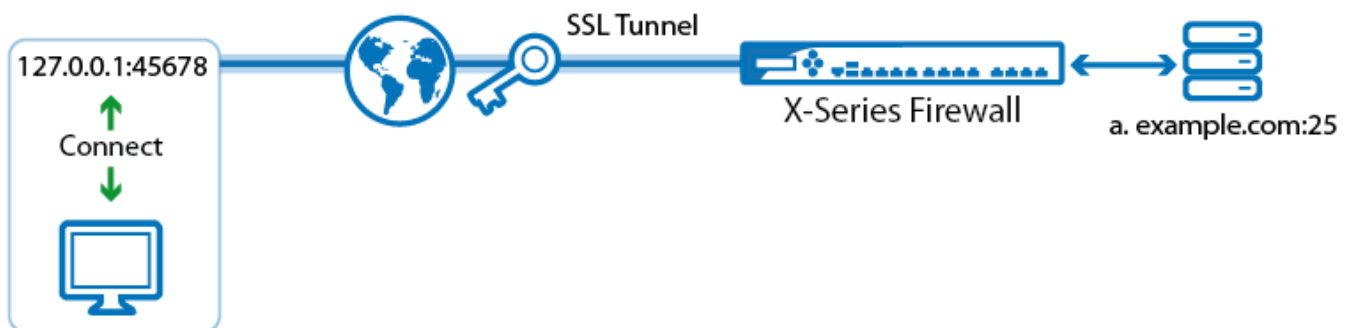


How to Configure SSL Tunnels

<https://campus.barracuda.com/doc/50266389/>

After you enable and configure the SSL VPN, you can add SSL tunnels. SSL tunnels are used to encrypt data for client/server applications that normally do not use encryption. An outgoing SSL tunnel protects TCP connections that a computer forwards from a local port to a preconfigured destination IP address and port that the user is connected to. To use SSL tunnels you must have a Remote Access Premium subscription.



Before you begin

Enable the SSL VPN service and CudaLaunch. For more information, see [How to Enable SSL VPN and CudaLaunch](#).

SSL tunnels

Configure a resource containing one or more SSL tunnels that forward the TCP traffic of the remote service. Access to tunnel resources can be limited via the user groups.

1. Go to **VPN > SSL VPN** and click the **Resources** tab.
2. In the **SSL Tunnels** section, click **Add SSL Tunnel**.
3. In the **Add SSL Tunnel** window, set **Enable** to **Yes**.
4. (optional) Click **Browse** to upload a PNG file for the web portal, less than 30 kB and not larger than 80x80 pixels.
5. In the **Name** field, enter the visible name for the tunnel resource. This is the name used in the web portal for this resource.
6. In the **Tunnels** section, configure the SSL tunnel:

1. Enter the **Name** of the SSL tunnel.
2. Enter the tunnel destination IP address in the **Address** field.
3. Enter the port on the loopback interface that the user connects to in the **FWD Port** field and the **Local Port** of the service tunneled by the SSL VPN. To use a random port, enter 0 (default).
4. (optional) To restrict access to the SSL tunnel by user group, remove the * entry in the **Allowed User Groups** list. Enter the user groups that can access the tunnel, and click + after each entry. If no groups are added, the SSL tunnel cannot be accessed. Use question marks (?) and asterisks (*) as wildcard characters.

Add SSL Tunnel

Enable: ☒ Yes ☐ No

Icon:
PNG File, less than 30kB and not bigger than 80x80 pixel.

Name:
Name displayed in the SSL-VPN portal page

Tunnels

Name	Address	FWD Port	Local Port	
<input type="text" value="WebSSL"/>	<input type="text" value="10.0.10.50"/>	<input type="text" value="5900"/>	<input type="text" value="80"/>	<input type="button" value="+"/>
WebSSL	10.0.10.50	5900	80	<input type="button" value="-"/>

Use zero as local loopback port to use a randomly chosen port.

Allowed Groups:

<input type="text" value="cn=vpnusers*"/>	<input type="button" value="+"/>
<input type="text" value="cn=vpnusers*"/>	<input type="button" value="-"/>



Use * as a wildcard





7. Click **Save**.


Tunnels in CudaLaunch

Tunnels are available only in CudaLaunch. To enable or disable the tunnel, go to the **Tunnels** tab and click the tunnel icon. The gray or green status icon shows the state of the tunnel.


State	Icon
-------	------

Tunnel inactive	 Generic Tunnel Example
Tunnel active	 Generic Tunnel Example





Generic Tunnel
Example



Generic Tunnel Example

Destination	Local
10.0.10.44:8080	127.0.0.1:58045

Disconnect

Figures

1. generic_ssl_tunnel.png
2. ssl_res01.png
3. sslvpn_gen_tunnel_05.png
4. sslvpn_gen_tunnel_04.png
5. sslvpn_gen_tunnel_07.png
6. sslvpn_gen_tunnel_06.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.