How to Create an SSL Tunnel

https://campus.barracuda.com/doc/39814215/

An outgoing SSL tunnel protects TCP connections that your local computer forwards from a local port to a preconfigured destination IP address and port, reachable by the Barracuda SSL VPN that the user is connected to. To use the tunnel, the application or browser connects to a random listener port on the 127.0.0.1 or 127.0.0.2 localhost address. The encrypted tunnel ends at the SSL VPN, all connection beyond the SSL VPN are not secure. If you want other computers on the same network to share a SSL tunnel, use a network IP address instead of the 127.0.0.1 localhost address as the source address.

Step 1. Create a SSL tunnel

1. Log into the SSL VPN web interface.
2. Go to the **RESOURCES > SSL Tunnels** page.
3. In the **Create SSL Tunnel** section, select the desired database from the **User Database** drop down list.

   If you are a Super User in the Global View and you want to apply this SSL tunnel across more than one User Database, select *Global View* as the User Database to list the Policies across all the User Databases.
4. Enter a unique name for the tunnel in the **Name** field.
5. In the **Destination Host** field, enter the name or IP of the resource you want to access.

   The *${}* indicates that replacement variables can be used. Clicking this icon will load the replacement variables that are available. The *session* variables are values taken from the current session. The *userAttributes* variables are values taken from user-defined attributes for the currently logged on user.
6. In the **Destination Port** field, enter the port number on the destination host. If you have a client application running on the destination host that for example listens at port 5900 for VNC, enter 5900.
7. Select *Yes* for **Add to My Favorites** if the tunnel should be added to the default **Resource Category**.
8. Double-click on your desired policies from the **Available Policies** list to send them to **Selected Policies** list.
9. Click **Add** to create the SSL Tunnel.

The SSL tunnel is now visible in the **SSL Tunnel** section.

Step 2. (Optional) Configure advanced tunnel settings

You can configure additional settings such as **auto launch**, **multiple port ranges** or **tunnel type**

by editing the SSL tunnel configuration:

1. In the **SSL Tunnels** section, click the **Edit** link associated with the tunnel. The **Edit Tunnel** page opens.
2. Configure the settings as required.
3. Click **Save**.

Step 3. Test the SSL tunnel

To test the SSL tunnel, click the name of the SSL Tunnel your just created or the **Launch** link associated with it. Make sure that you also test a user account that has the appropriate access rights with a connection outside your intranet.