How to Configure the SSL VPN Service

https://campus.barracuda.com/doc/73700097/

Configure SSL VPN on the firewall to give end users remote access to corporate resources. It is recommended to use a signed certificate to avoid browser certificate warnings when accessing the SSL VPN portals.

Before You Begin

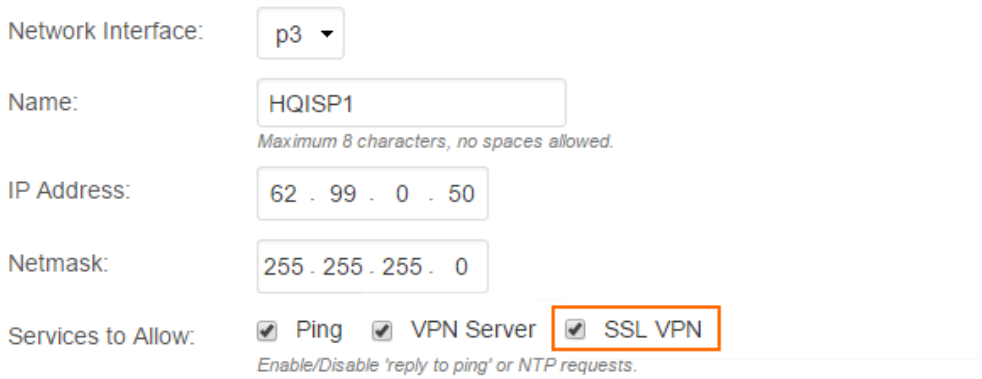
- An Advanced Remote Access subscription is required.
- If you are running a VPN server on the same public IP address, go to **VPN > Settings** and verify that **Use TCP Port 443** is set to **No**.
- Verify that you are not using DNAT access rules to redirect HTTPS traffic on the same public IP that the SSL VPN is using.

Step 1. Enable SSL VPN

When you enable the SSL VPN portal, determine if you are using a static, dynamic, or secondary IP address for the portal. Typically, the SSL VPN portal is deployed on a static public IP address with a corresponding DNS A resource record. The portal can also use a secondary IP address for internal access.

Static IP Address

1. Go to **NETWORK > IP Configuration**.
2. In the **Static Interface Configuration** section, click **Edit** to configure your static WAN interface.
3. In the **Edit Static Network Interface** window, select the **SSL VPN** check box.



If the VPN service is also enabled for this interface, go to **VPN > Settings** and verify that **Listen on Port 443** is set to **No**.

4. Click **Save**.

Secondary IP Address

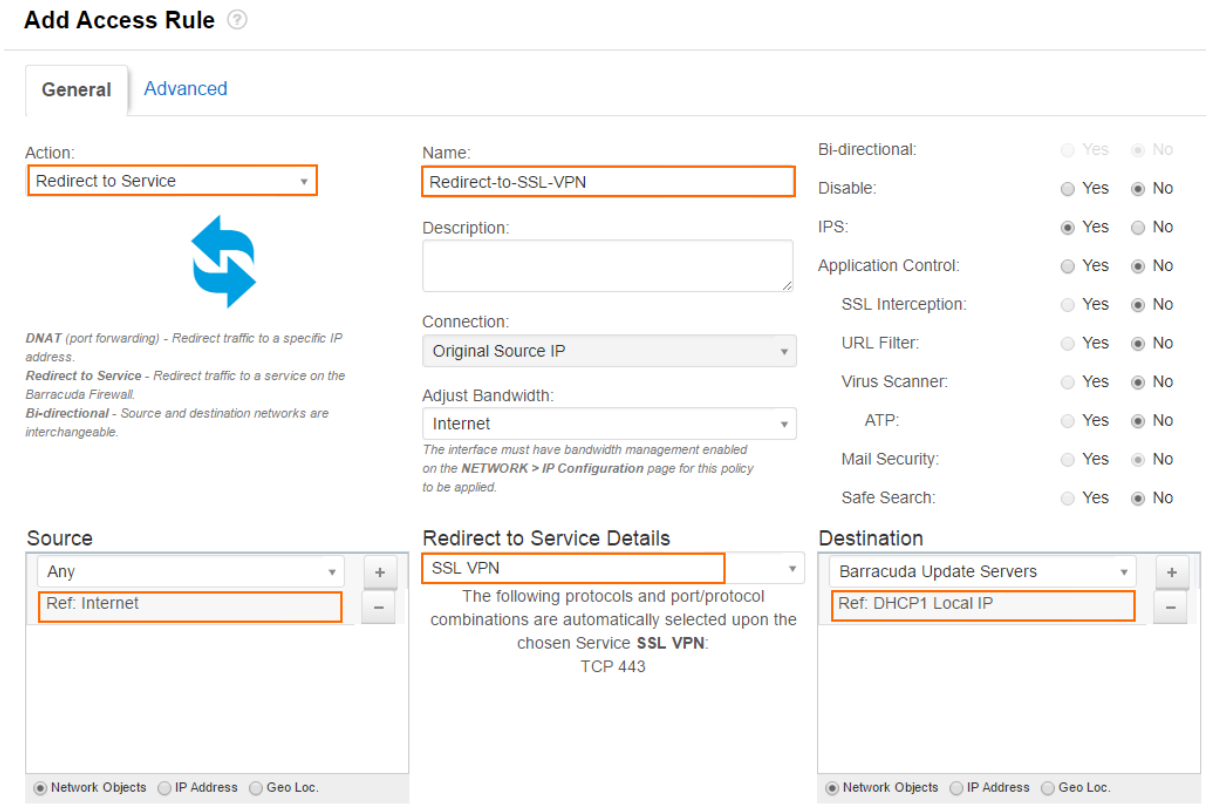
Typically, a secondary IP address is used to provide the SSL VPN portal on internal network segments.

1. Go to **NETWORK > IP Configuration**.
2. In the **Management IP Configuration** section, select the **SSL VPN** check box next to the required IP address in the **Secondary IP Addresses** table. Or,
   if the IP address resides in a configured static network interface, edit the interface in the **Static Interface Configuration** section, and select the **SSL VPN** check box.
3. Click **Save**.

Dynamic Network Interface

To use a dynamic interface to access the SSL VPN portals, redirect incoming HTTPS traffic to the SSL VPN service.

1. Go to **FIREWALL > Access Rules**.
2. Add a Redirect to Service access rule with the following settings:
   - **Name** – Enter a name for the access rule. E.g., `Redirect-to-SSL-VPN`.
   - **Action** – Select **Redirect to Service**.
   - **Source** – Select **Internet** from the list, and click **+**.
   - **Redirected To Service Details** – Select **SSL VPN**.
   - **Destination** – Select the network object representing your incoming Internet connection, and click **+**. E.g., **DHCP1-Local-IP**



3. To enable access to the SSL VPN portal via a hostname instead of only via the IP address

(because the latter may change), you can use the third-party DynDNS service.
   1. Go to **NETWORK > IP Configuration**.
   2. In **Dynamic Interface Configuration**, enable **Use Dynamic DNS** for the required interface.
4. Click **Save**.

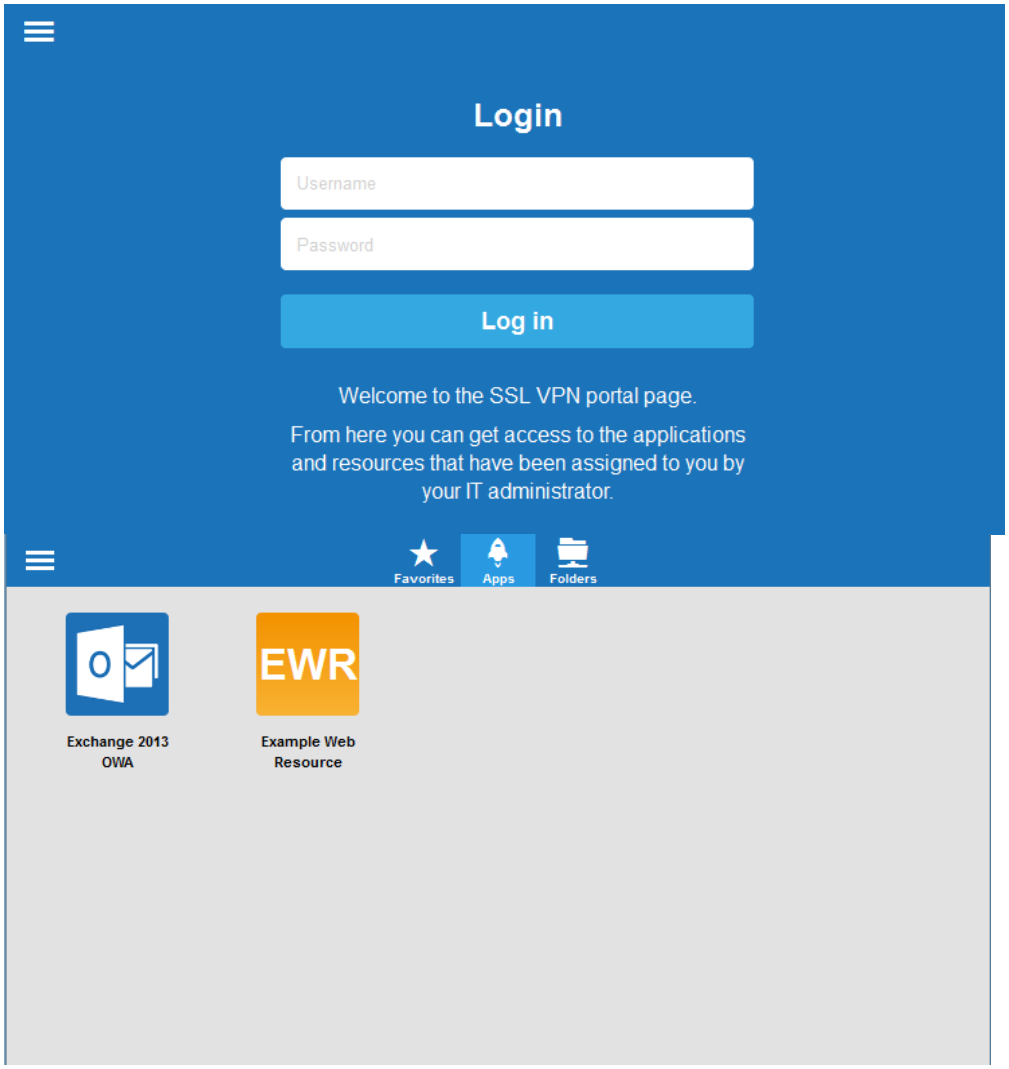
Step 2. Configure SSL VPN Settings

Configure the SSL VPN web portal and upload a certificate. End users must authenticate themselves before they can access internal resources and applications via SSL VPN. You can manage user authentication either locally on the firewall or externally with Active Directory, LDAP, or RADIUS. For instructions on how to configure local or external user authentication, see Authentication.

1. Go to **VPN > SSL VPN**.
2. Click the **Server Settings** tab.
3. Set **Enforce Strong Ciphers** to **Yes** unless you require backward compatibility with SSLv3-only clients.
4. Set **Allow SSLv3** to **No**. SSLv3 is considered unsafe.
5. Upload or create a **Certificate**. It is recommended to install a CA-trusted SSL certificate for the SSL VPN on the firewall, so that web browsers do not issue a SSL warning to end users when they access the portal. By default, the Web UI certificate is used. For instructions, see How to Use and Manage Certificates with the Certificate Manager.
6. In the **Authentication** section, select the method from the **User Authentication** list.
7. (optional) To restrict SSL VPN access by user group:
   1. Set **Group Access Restrictions** to **Yes**.
   2. Enter the user groups that can access the SSL VPN in the **Allowed Groups** list, and click **+** after each entry. Use question marks (?) and asterisks (*) as wildcard characters.
   3. Enter the user groups that are denied access to the SSL VPN in the **Blocked Groups** list, and click **+** after each entry.
8. In the **Appearance** section, customize the SSL VPN portal by uploading your company's logo, and welcome and help texts.
   Only ASCII characters are allowed in the **Welcome Message** and **Help Text** fields.
9. Click **Save**.

Next Steps

After you enable and configure the SSL VPN, end users can access the portal in their web browsers. Configure your DNS server or service to resolve sslvpn.<*yourdomain*> to the public IP address of your firewall. End users can then access the portal page by opening **https://sslvpn<*yourdomain*>**.



To add resources for your end users to the SSL VPN portal, see:

- How to Configure an Outlook Web Access Web App
- How to Configure a SharePoint Web App
- How to Configure a Generic Proxied Web App
- How to Configure Single Sign On for Proxied Web Apps

Figures

1. ssl_von_config_01.png
2. ssl_vpn_config_02.png
3. web_01.png
4. web_02.png