

## How to Configure the SSL VPN Service

<https://campus.barracuda.com/doc/41116136/>

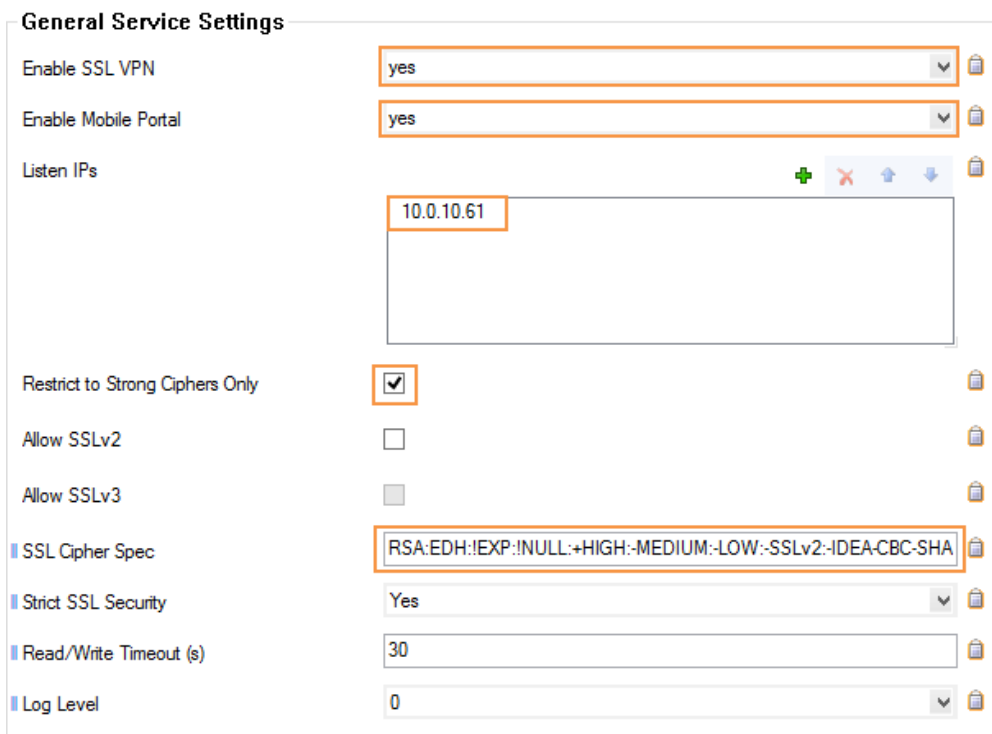
Before configuring the SSL VPN service, ensure that you have correctly created and configured a VPN service.

### In this article:

### Configure the Basic Settings

1. Open the **SSL-VPN** page (**Config > Full Config > Box > Virtual Servers > your virtual server > Assigned Services > VPN-Service**).
2. Click **Lock**.
3. Set **Enable SSL VPN** to **Yes**.
4. Click **+** to add a **Listen IP**.
5. (recommended) Enable **Restrict to Strong Ciphers Only**.

For Barracuda NG Firewalls versions 6.0.1 and below, Barracuda Networks strongly recommends to set the following custom **SSL Cipher Spec** settings to mitigate [CVE-2015-4000](#) aka. Logjam: ***RSA:EDH:!EXP:!NULL:+HIGH:-MEDIUM:-LOW:-SSLv2:-IDEA-CBC-SHA***



General Service Settings	
Enable SSL VPN	yes
Enable Mobile Portal	yes
Listen IPs	10.0.10.61
Restrict to Strong Ciphers Only	<input checked="" type="checkbox"/>
Allow SSLv2	<input type="checkbox"/>
Allow SSLv3	<input type="checkbox"/>
SSL Cipher Spec	RSA:EDH:!EXP:!NULL:+HIGH:-MEDIUM:-LOW:-SSLv2:-IDEA-CBC-SHA
Strict SSL Security	Yes
Read/Write Timeout (s)	30
Log Level	0

- Make sure that the IP address has been added to the virtual server settings. For more information, see [Virtual Servers and Services](#).
- Do not use a bind IP address of the VPN service. Otherwise the SSL VPN service cannot be started. To test if the SSL VPN is running, open `https://<listen IP>/` in your web browser

If the VPN server has enabled a listening socket on port 443, the SSL VPN service will not be able to start. This is indicated with the following SSL VPN log message: `http_listener: failed to listen on <IP address>@443`. Go to **VPN Settings > Server Settings** and set **Use Port 443** to **No**.

6. In the **Service Identification** section, configure the certificates and private keys that are used by the SSL VPN.
7. From the **Identification Type** list, select one of the following options:
  1. **Self-Signed-Certificate** - Create the **Self-Signed Private Key** and the **Self-Signed Certificate**.
  2. **External-Certificate** - Import the CA-signed **External Certificate** and the **External-Signed Private Key**.
  3. **Generated-Certificate** - The certificate and the private key is created by the Barracuda NG Firewall.
8. Generate or import your keys and certificates.
9. Click **Send Changes** and **Activate**.
10. When updating or changing certificates, the SSL VPN service needs to be restarted:
  1. Set **Enable SSL VPN** to **no**.
  2. Click **Send Changes** and **Activate**
  3. Reenable the SSL VPN service.
  4. Click **Send Changes** and **Activate**

## Configure Authentication and Login

1. Open the **SSL-VPN** page (**Config > Full Config > Box > Virtual Servers > your virtual server > Assigned Services > VPN-Service**).
2. In the left menu, click **Authentication & Login**.
3. Click **Lock**.
4. From the **Authentication Scheme** list, select your authentication method.
5. In the **Corporate ID** section, enter a message in the **Login Message** field. For example, `Welcome to SSL VPN`.
6. Click **Send Changes** and **Activate**.

## Enable the Access Monitor

To determine the health state of a Barracuda Network Access Client, you can enable the Access

Monitor. A client is only granted access to sensitive resources if it is healthy.

1. Open the **SSL-VPN** page (**Config > Full Config > Box > Virtual Servers > your virtual server > Assigned Services > VPN-Service**).
2. In the left menu, click **NG Access Monitor**.
3. From the **Active** list, select **yes**.
4. Enter the **Access Control Service IP**.
5. In the **User Groups** field, enter the groups that should be checked.  
To configure the Access Monitor settings, edit the [Access Control Service](#) settings.
6. Click **Send Changes** and **Activate**.

## Next Step

---

Continue with [How to Configure a Local Database for SSL VPN](#).

## Figures

1. sslvpn01\_LOGJAM.png

© Barracuda Networks Inc., 2020 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.