How to Configure the SSL VPN Service

https://campus.barracuda.com/doc/46209316/

The SSL VPN service is part of the VPN service on the Barracuda NextGen Firewall F-Series. Configure the SSL VPN to listen on a public IP address and to authenticate the users via an external authentication server. It is recommended to use signed SSL certificates to avoid SSL error messages for the users when connecting to the NextGen F-Series SSL VPN. NextGen F-Series SSL VPN is supported for Barracuda NextGen Firewall F-Series F80 and larger, as well as all Barracuda NextGen Firewall F-Series Vx models.

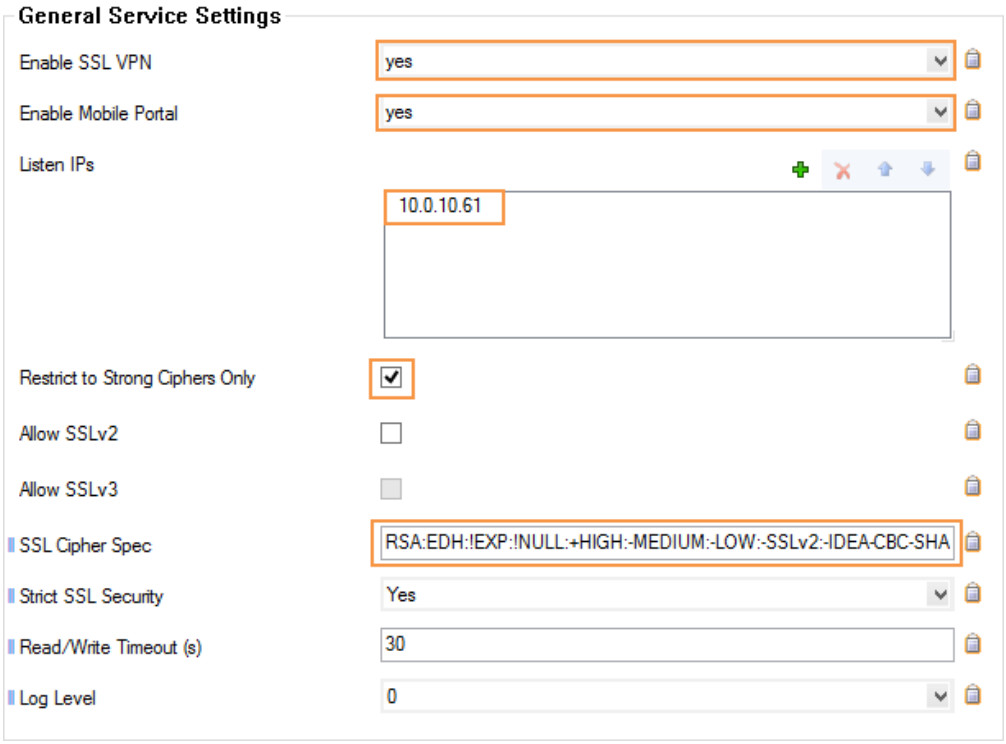
In this article:

Before you Begin

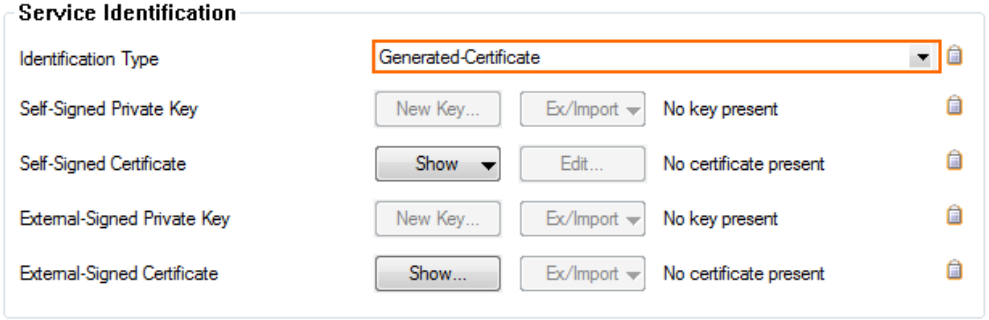
- A Remote Access premium subscription is required to use the NextGen F-Series SSL VPN.
- Because the VPN service can also listen on port 443, verify that **Use Port 443** is set to **No** in the **Server Settings** on the **VPN Settings** page.
- Verify that the IP address you want the SSL VPN to listen on is configured as as Virtual Server and VPN service IP address. For more information, see Virtual Servers and Services.
- Configure an external authentication server or NGF local authentication. For more information, see Authentication

Step 1. Enable the SSL VPN

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > SSL-VPN**.
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**.



6. Select the **Identification Type**
   - **Generated-Certificate** – The certificate and the private key is automatically created by the Barracuda NextGen Firewall F-Series.
   - **Self-Signed-Certificate** – Click **New** to create a **Self-Signed Private Key** and then **Edit** to create the **Self-Signed Certificate**.
   - **External-Certificate** – Click **Ex/Import** to import the CA-signed **External Certificate** and the **External-Signed Private Key**.



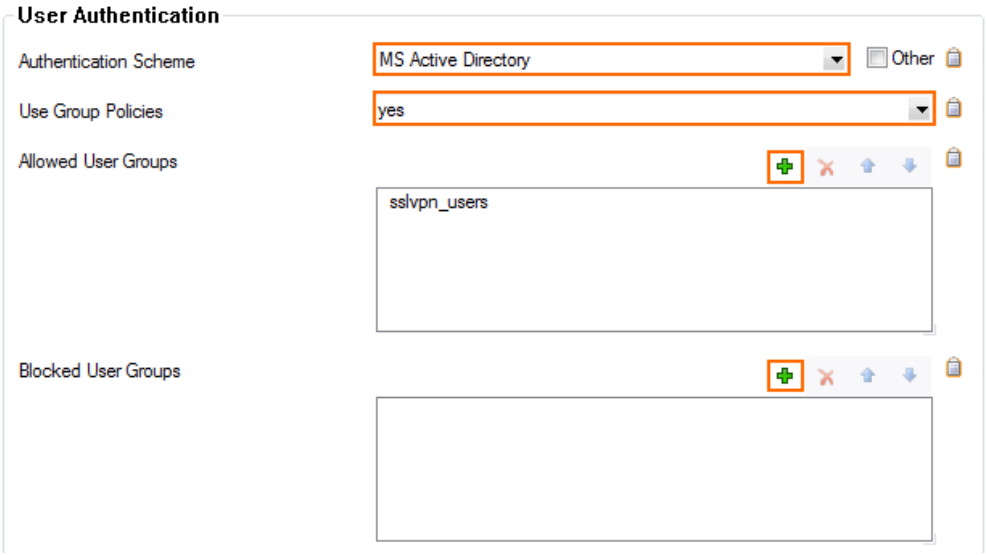
7. Click **Send Changes** and **Activate**.

Step 2. Configure Authentication and Login

Configure the authentication server and the allowed and blocked user groups. Users that are not members of one of these groups will be denied access to the NextGen F-Series SSL VPN.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > SSL-VPN**.

2. In the left menu, click **Authentication & Login**.
3. Click **Lock**.
4. From the **Authentication Scheme** list, select your authentication method.
5. If you are using an authentication service with group information, or an authentication helper scheme to provide group information, set **Use Group Policies** to **yes**.
6. (optional) Click **+** to add **Allowed User Groups**.
7. (optional) Click **+** to add **Blocked User Groups**.

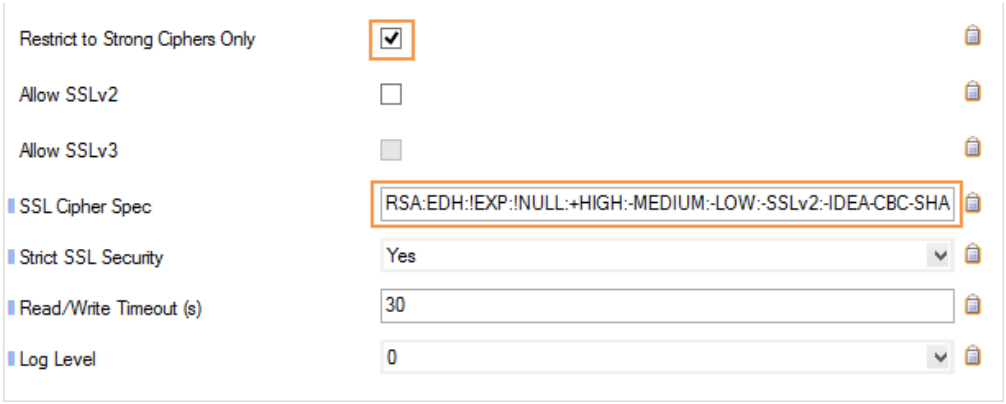


8. (optional) Configure the following settings as needed:
   - **Use Max Concurrent Users** – Enable to limit the number of simultaneous users using the NextGen F-Series SSL VPN.
   - **Max Concurrent Users** – Enter the maximum number of users that simultaneously can be connected to the NextGen F-Series SSL VPN.
   - **Cookie Timeout (Min)** – Enter the session timeout in minutes.
   - **Authentication Request Timeout (sec)** to a value up to 20 seconds if you are using multi-factor authentication.
   - **Browser Cleanup** – Enable to clear the browser cache after logging out. Only for Internet Explorer and Firefox.
   - **Deny Autocomplete** – Set to **yes** to disable auto completion for the HTML forms in the SSL VPN.
   - **Deny Remember Me** – Set to **yes** to remove the **Remember me** checkbox on the login page.
9. Customize the login messages and logos:
   - (optional) Import a **Logo**.
     It is recommended to use a 200 x 66px PNG or JPG image.
   - (optional) Enter a plain text **Login Message**. E.g, `Welcome to the Barracuda NextGen F-Series SSL VPN`.
   - (optional) Enter a HTML **Help Text**.
10. Click **Send Changes** and **Activate**.

Step 3. (optional) Enforce Strong Ciphers

Replace the default ciphers by a more secure spec.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > SSL-VPN**.
2. Click **Lock**.
3. In the left menu expand **Configuration Mode** and click on **Switch to Advanced View**.
4. Disable **Allow SSLv2** and **Allow SSLv3**
   Enable **Restrict to Strong Ciphers Only**.
   For Barracuda NextGen F-Series Firewalls versions 6.1 and below, Barracuda Networks strongly recommends to set the following custom **SSL Cipher Spec** settings to mitigate CVE-2015-4000 aka. Logjam.
5. Enter the **SSL Cipher Spec**: `RSA:EDH:!EXP:!NULL:+HIGH:-MEDIUM:-LOW:-SSLv2:-IDEA-CBC-SHA`



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

Troubleshooting

- If the **sslvpn** log contains the following line: `http_listener: failed to listen on <IP address>@443` verify that no other service on the Barracuda NextGen Firewall F-Series is running on that port and no DNAT access rules are redirecting the traffic to a different IP address.
- 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. Set **Enable SSL VPN** to **yes**.
  4. Click **Send Changes** and **Activate**.

Figures

1. sslvpn01_LOGJAM.png
2. sslvpn02.png
3. sslvpn03.png
4. sslvpn04_LOGJAM.png