How to Set Up VPN Certificates

https://campus.barracuda.com/doc/46209306/

For the VPN service, you can use either self-signed certificates or certificates that are generated by an external CA.

In this article:

Before You Begin

Before you set up VPN certificates, verify that the VPN service has been properly created and configured. For more information on how to create a service, see How to Configure Services.

Set Up Certificates with the Barracuda CA for a Barracuda VPN

If you want to use a Barracuda VPN with the Barracuda CA installed on the Barracuda NextGen Firewall F-Series, complete the following steps:

Step 1. Create the Default Certificate and Private Key

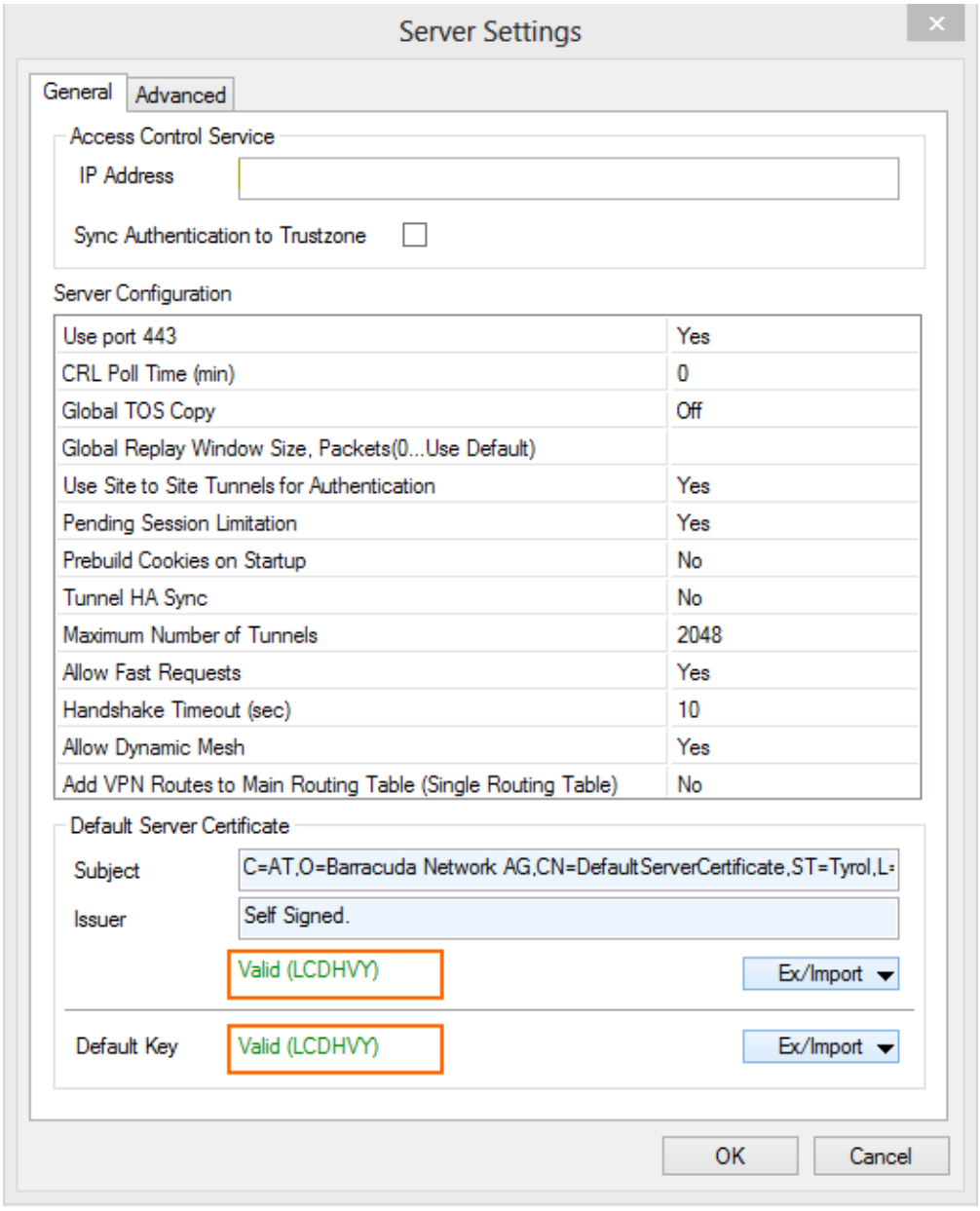
The default server certificate will be signed by the self-signed Barracuda root certificate that is included with the Barracuda NextGen Firewall F-Series.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.
3. Click the **Settings** tab.
4. Click the **Click here for Server Settings** link.
5. If you are using the Access Control service, enter its **IP Address** in the **Access Control Service** section of the **Server Settings** window.
6. Create the certificate:
    1. In the **Default Server Certificate** section, click **Ex/Import** and select **New/Edit Certificate**.
    2. In the **Certificate View** window, fill out the **Subject** section completely. You must set the **SubAltName** and **Name** to the FQDN resolving to the listening IP address of the VPN service.
    3. Click **OK**.

7. Create the default key:
    1. Click **Ex/Import** in the **Default Key** section.
    2. Select **New x-Bit RSA key** (where x is 512, 1024, or 2048).
    3. Click **OK**.
8. Click **Send Changes** and **Activate**.

Step 2. Import the Default Certificate and Private Key

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.
3. Click the **Settings** tab.
4. Click the **Click here for Server Settings** link.
5. If you are using the Access Control Service (NAC), enter its **IP Address** in the **Access Control Service** section of the **Server Settings** window.
6. In the **Default Server Certificate** section, click **Ex/Import** and select either **Import PEM from file** or **Import from PKCS12**, depending on the external certificate format.
7. In the **Default Key** section, click **Ex/Import** and select **Import Private Key from File**.
   If the certificates match, the **Default Server Certificate** and the **Default Server Key** display 'Valid' in green.



8. Click **OK**.
9. Click **Send Changes** and **Activate**.

Set Up Certificates with an External CA for a Barracuda, IPsec, or L2TP/IPsec VPN

Requirements

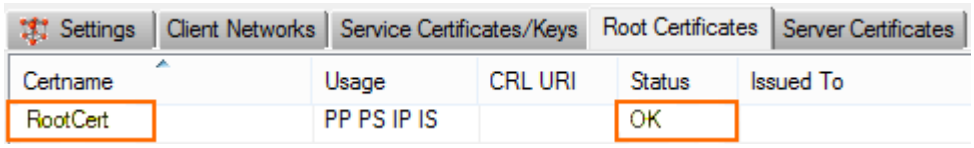
X.509 Certificate Type	Install Location	File Type	Chain of Trust	X.509 Extensions and Value

Root Certificate, for example, *RootCrt.crt*	Barracuda NextGen Firewall F-Series	PEM	Trust Anchor	• **Key Usage:** *Certificate sign; CRL sign*
Server Certificate, for example, *ServerCrt.pem* and *ServerCrtprivate.pem*	Barracuda NextGen Firewall F-Series	PKCS12	End Instance	• **Key Usage:** *Digital Signature* • **Subject Alternative Name**: *DNS: tag with the FQDN which resolves to the IP the VPN Service listens on.* For example: *DNS: vpn.yourdomain.com* X.509 certificates on the Barracuda NextGen Firewall F-Series must not have identical **SubjectAlternativeNames** settings and must not contain the management IP address of the Barracuda NextGen Firewall F-Series.
Client Certificate, if needed	Client OS or VPN Client	PKCS12	End Instance	• **Key Usage**: *Digital Signature*

Install the Root Certificate

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.
3. Click the **Root Certificates** tab.
4. Right-click the table and select **Import PEM from File** or **Import CER from File**, depending on the root certificate format.
5. In the **Open** window, select the root certificate file and click **Open**.
6. In the **Root Certificate** window, configure the following settings under the **Certificate details** tab:
   - **Name** – A descriptive name for the root certificate. For example, *RootCert*.
   - **Usage** – The types of VPNs that will use this root certificate. For example, *Barracuda Personal* and *IPsec Personal*.
7. Click **OK**.

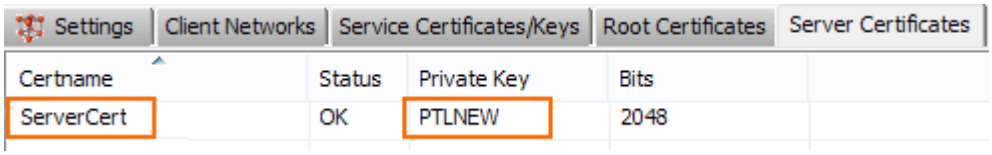
The root certificate appears under the **Root Certificates** tab.



Install the Server Certificate

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.
3. Click the **Server Certificates** tab.
4. Import the server certificate.
    1. Right-click the table and select **Import Certificate from File**.
    2. In the **Open** window, select the server certificate file and click **Open**.
    3. Enter the **Certificate Name**, for example, `ServerCertificate`, and then click **OK**. The certificate appears under the **Server Certificates** tab.
5. Import the private server key.
    1. Right-click the server certificate and select **Import Private Key From File**.
    2. In the **Open** window, select the private server key file, for example, **ServerCertprivate.pem**, and then click **Open**.
6. Click **Send Changes** and **Activate**.

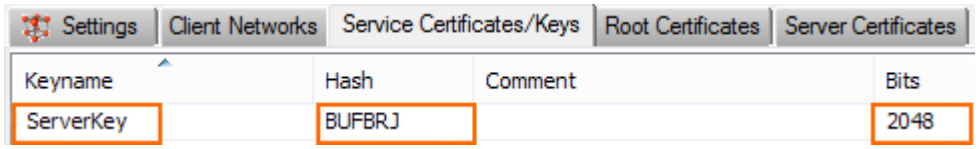
Your server certificate appears with the private key in the **Server Certificates** list.



Create a Service Certificate/Key

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.
3. Click the **Service Certificates/Keys** tab.
4. Right-click the table and select **New Key**.
5. Enter a **Key Name**, and click **OK**.
6. Select the required **Key Length**, and click **OK**.
7. Click **Send Changes** and **Activate**.

Your service certificate appears under the **Service Certificates/Keys** tab.



Create a CSR on the Barracuda NextGen Firewall F-Series

You can create a certificate signing request (CSR) directly on the command line of the Barracuda NextGen Firewall F-Series.

1. Go to **SSH** and login.
2. On the command line enter:
   `openssl req -new -newkey rsa:2048 -nodes -keyout domain.key -out domain.csr`
3. Download the certificate to your desktop:
   `[down] domain.csr`
4. Save the csr file to your disk.

You can now submit the certificate signing request to your CA to receive a signed certificate.

Certificate Detail Settings

From the **Certificate details** tab, you can configure the following settings:

- **Certificate** – The certificate's subject and issuer.
- **Name** – The certificate name for easier recognition.
- **Usage** – The tunnel types that the certificate is valid for. The following tunnel types are available:
  - **Personal**
  - **Site-to Site**
  - **IPSec Personal**
  - **IPSec Site-to-Site**
- **Comment** – An optional description of the certificate.
- **Timeout (min.)** – The length of time after which the fetching process is started again if all URIs of the root certificate fail.
- **Action** – The action that is taken if the CRL is not available after the fetching process that is started after the **Timeout**. You can select one of the following actions:
  - **Terminate all sessions** – Every VPN session relating to this root certificate is terminated.
  - **Do not allow new sessions** – New VPN sessions relating to this root certificate are not allowed.
  - **Ignore** – A log entry is created but does not have any effect on VPN connections relating to this root certificate.

Certificate Revocation Settings

From the **Certificate details** tab, you can either import or manually add a CRL URI.

1. If a CRL is already included within the certificate, import the CRL URI by clicking **Load paths from certificate**.
2. To add a CRL URI manually, configure the settings in the **URI**, **Login**, and **Proxy** sections and then click **Add**.
3. **Protocol** – The required connection protocol. The following protocols are available:
   - **LDAP** – DNS-resolvable, default port: 389
   - **LDAPS** – DNS-resolvable, default port: 636
   - **HTTP** – Default port: 80
   - **HTTPS** – Default port: 443
4. **Host** – The DNS-resolvable host name or IP address of the server that makes the CRL available.
5. **URL-Path** – The path to the CRL. For example: `cn=vpnroot,ou=country,ou=company,dc=com?,cn=*`

   When the CRL is made available through SSL-encrypted LDAP (LDAPS), use the fully qualified domain name (that is the resolvable host name) in the CN subject to refer to the CRL. For example, if a server's host name is *server.domain.com*, enter the following in the URL path: `cn=vpnroot,ou=country,ou=company,dc=com, cn=server.domain.com`
   The A-Trust LDAP server requires the CRL distribution point referring to it to terminate with a CN subject. Therefore, as from Barracuda NextGen Firewall F-Series 3.6.3 when loading the CRL from a certificate, the search string "*?cn*=*" will automatically be appended if the CRL is referring to an LDAP server and if a search string (CN subject) is not available in the search path by default. Note that existing configurations will remain unchanged and that the wildcard CN subject does not conflict with other LDAP servers.

- **User / Password** – The username and corresponding password. This information is necessary if the LDAP or HTTP server requires authentication.
- **Proxy** – The DNS-resolvable host name or IP address of the proxy server.
- **Port** – The proxy server port used for connection requests.
- **User / Password** – The username and corresponding password. This information is necessary if the proxy server requires authentication.

From the **OCSP** tab, you can configure the following settings:

- **Host** – The DNS-resolvable hostname or host IP address.
- **Port** – The OCSP server listening port. **Use SSL** – Enforces an SSL connection to the OCSP server.
- **Phibs Scheme** – Allows selection of an OCSP scheme (default: *ocsp*). **CA Root** – Specifies how the OCSP server is verified. You can select the following options:
  - **This root certificate** – The OCSP server certificate signing the OCSP answer was issued by this root certificate.
  - **Other root certificate** – The OCSP server certificate signing the OCSP answer was

issued by another root certificate. This other root certificate must be imported via the **Other root** setting.
  - **Explicit Server certificate** – The OCSP server certificate signing the OCSP answer might be self-signed or another certificate. This X.509 certificate must be imported via the **Explicit X.509** setting.

Take into consideration that the extended certificate usage is set to OCSP signing in the OCSP-server certificate when you select **This root certificate** or **Other root certificate**.

- **Other root** – If **CA Root** is set to **Other root certificate**, click **Ex/Import** to import the certificate in either PEM or PKCS12 format.
- **Explicit X509** – If **CA Root** is set to **Explicit Server**, click **Ex/Import** to import the certificate in either PEM or PKCS12 format.

Figures

1. vpn_certificate_setup_01.PNG
2. vpn_certificate_setup_02.PNG
3. vpn_certificate_setup_03.PNG
4. vpn_certificate_setup_04.PNG