How to Set Up External CA VPN Certificates

https://campus.barracuda.com/doc/53248801/

To configure a client-to-site or site-to-site VPN using certificates created by External CA, you must create the following VPN certificates for the VPN service to be able to authenticate.

Before You Begin

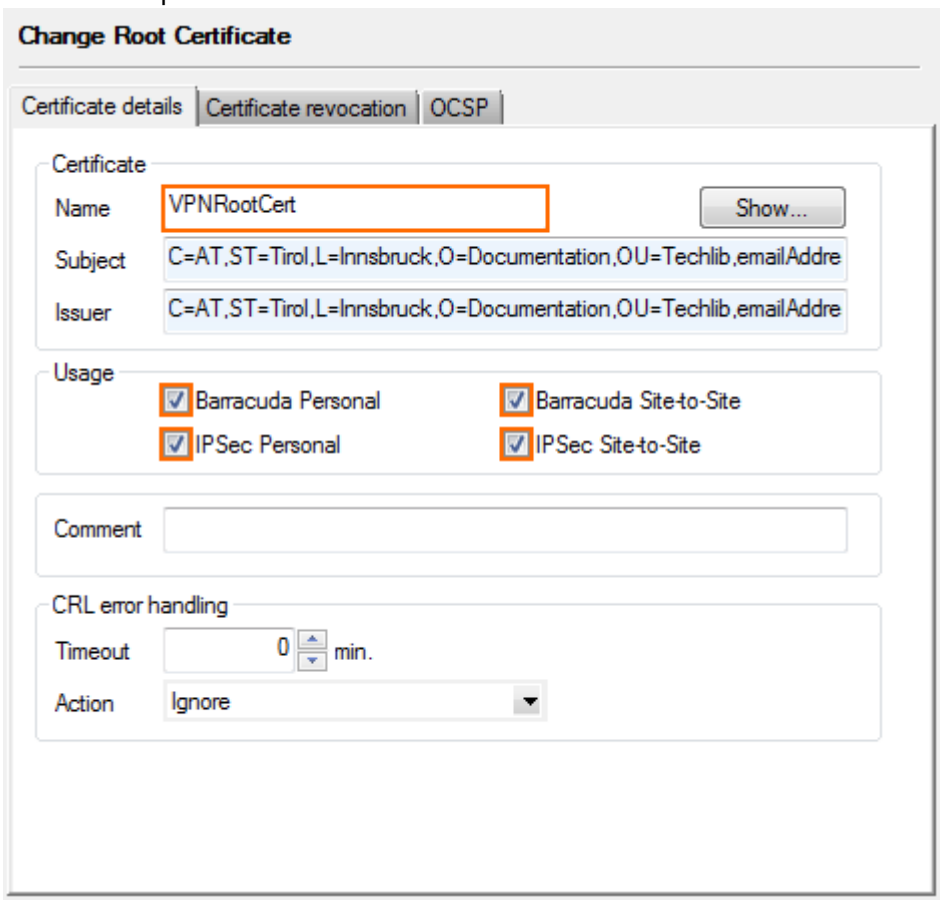
Use an external CA to create the following certificates. For an example using XCA, see How to Create Certificates with XCA.

X.509 certificate type	Installation location	File type	Chain of trust	X.509 extensions
Root certificate	**VPN Settings** on the firewall	PEM	Trust anchor	• **Key Usage:** *Certificate sign; CRL sign*
Server certificate	**VPN Settings** on the firewall	PKCS12	End instance	• **Key Usage:** *Digital Signature* • **Subject Alternative Name**: *DNS: tag with the FQDN that resolves to the IP the VPN Service listens on, or create a wildcard certificate* 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 operating system or VPN client	PKCS12	End instance	• **Key Usage**: *Digital Signature*

Step 1. Install the Root Certificate

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

5. Select the file containing the root certificate and click **Open**. The **Root Certificate** window opens.
6. Enter a **Name**. This is the name that is displayed for this certificate throughout the VPN configuration.
7. Select the **Usage**.
   - **Barracuda Personal** – Select to use this certificate for client-to-site VPN using the TINA protocol.
   - **IPsec Personal** – Select to use this certificate for client-to-site VPN using the IPsec protocol.
   - **Barracuda Site-to-Site** – Select to use this certificate for site-to-site VPN tunnels using the TINA protocol.
   - **IPsec Site-to-Site** – Select to use this certificate for site-to-site VPN tunnels using the IPsec protocol.



8. (optional) Click on the **Certificate revocation** tab and configure the CRL host.
   1. Click **Load paths from certificate** to use the CRL information included in the certificate.
   2. You can also manually enter the **URI**, **Login**, and optional **Proxy** settings.

Certificate revocation settings

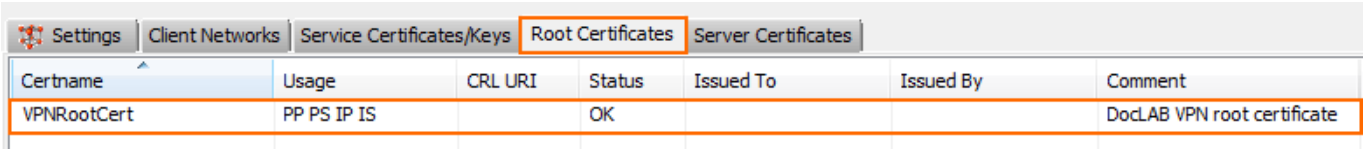
Section	Setting	Description

<table>
<tr><td rowspan="3">URI</td><td>Protocol</td><td>The required connection protocol. The following protocols are available:<table><tr><th>Protocol</th><th>Default Port</th><th>Comment</th></tr><tr><td>LDAP</td><td>389</td><td>DNS-resolvable</td></tr><tr><td>LDAPS</td><td>636</td><td>DNS-resolvable</td></tr><tr><td>HTTP</td><td>80</td><td>-</td></tr><tr><td>HTTPS</td><td>443</td><td>-</td></tr></table></td></tr>
<tr><td>Host</td><td>The DNS-resolvable hostname or IP address of the CRL server.</td></tr>
<tr><td>URL-Path</td><td>The path to the CRL. For example: <code>cn=vpnroot,ou=country,ou=company,dc=com?,cn=*</code>
When the CRL is made available through SSL-encrypted LDAP (LDAPS), use the fully qualified domain name (the resolvable hostname) in the CN subject to refer to the CRL. For example, if a server's hostname is server.domain.com, enter the following in the URL path: <code>cn=vpnroot,ou=country,ou=company,dc=com,cn=server.domain.com</code>
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.</td></tr>
<tr><td>Login</td><td>User / Password</td><td>The username and password for LDAP or HTTP servers requiring authentication.</td></tr>
<tr><td rowspan="3">Proxy</td><td>Proxy</td><td>The DNS-resolvable hostname or IP address of the proxy server.</td></tr>
<tr><td>Port</td><td>The proxy server port used for connection requests.</td></tr>
<tr><td>User / Password</td><td>The username and password required by the proxy server.</td></tr>
</table>

9. (optional) Click on the **OCSP** tab and configure the OCSP server.
   - **Host** – Enter the DNS resolvable hostname or IP address of the OCSP server.
   - **Port** – Enter the listening port.
   - **Use SSL** – Click to enable SSL.
   - **Phibs Scheme** – Select **ocsp**. This allows you to use OCSP as a directory service.
   - **OCSP Server Identification**
     - **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.

10. Click **OK**.

The root certificate is now listed in the **Root Certificates** tab.

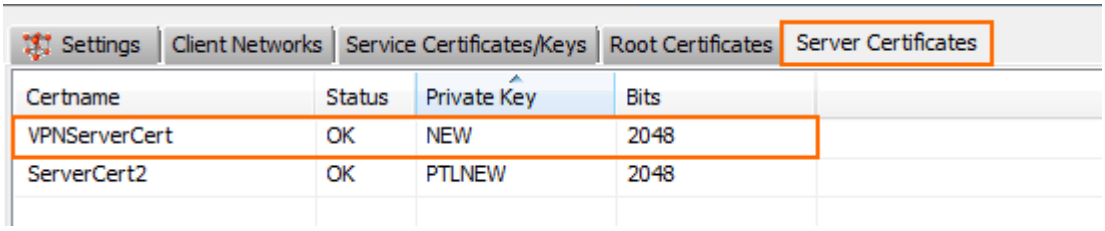


Step 2. Install the Server Certificate

Install the server certificate signed by the root certificate uploaded in step 1.

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**, and then click **OK**. The certificate is now listed in 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 and then click **Open**.
6. Click **Send Changes** and **Activate**.

Your server certificate appears with the private key under the **Server Certificates** tab.

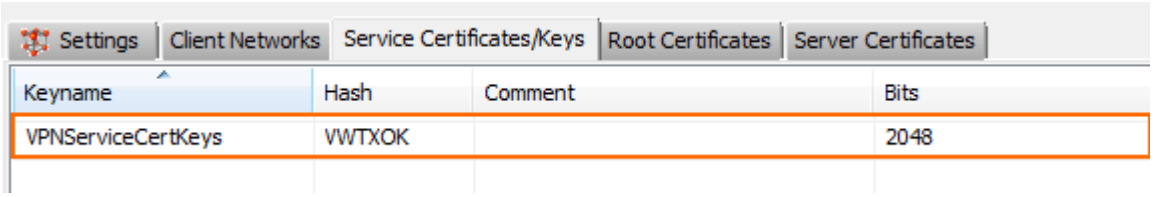


Step 3. Create a Service Certificate/key

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 **Key Length** and click **OK**.
7. Click **Send Changes** and **Activate**.

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



You now have root, server, and service certificates for your VPN service. Depending on the **Usage** selected in step 1, you can now configure your client-to-site or site-to-site VPN.

Figures

1. vpn_certs_01.png
2. vpn_certs_02.png
3. vpn_certs_03.png
4. vpn_certs_04.png