How to Set Up External CA VPN Certificates

https://campus.barracuda.com/doc/96026182/

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

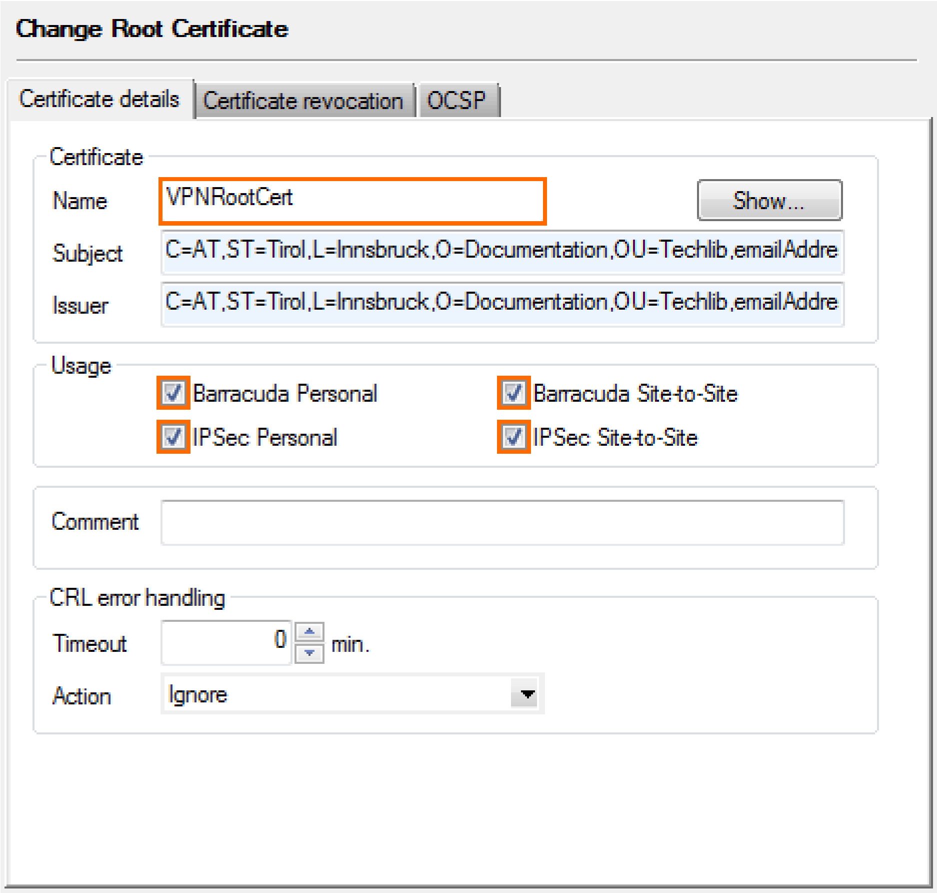
Use an external CA to create the following certificates. For an example using XCA, see How to Create Certificates with XCA.

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 CloudGen Firewall must not have identical **SubjectAlternativeNames** settings and must not contain the management IP address of the Barracuda CloudGen Firewall.
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 > Assigned Services > VPN > VPN Settings**.
2. In the left menu, select **Root Certificates**.
3. Click **Lock**.

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. Verify that the window displays the tab **Certificate details**.
7. Enter a **Name**. This is the name that is displayed for this certificate throughout the VPN configuration.
8. 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.



Change Root Certificate

Certificate

Name: VPNRootCert

Subject: C=AT,ST=Tirol,L=Innsbruck,O=Documentation,OU=Techlib,emailAddre

Issuer: C=AT,ST=Tirol,L=Innsbruck,O=Documentation,OU=Techlib,emailAddre

Usage

☑ Barracuda Personal ☑ Barracuda Site-to-Site

☑ IPSec Personal ☑ IPSec Site-to-Site

Comment

CRL error handling

Timeout: 0 min.

Action: Ignore

9. In the **CRL error handling** section, you can configure the actions to be taken in case a certificate referred within the Certificate Revocation List (CRL) is unavailable:
    - **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.

10. (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

<table>
<tr><th>Section</th><th>Setting</th><th>Description</th></tr>
<tr><td rowspan="5"><b>URI</b></td><td><b>Protocol</b></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><b>Host</b></td><td>The DNS-resolvable hostname or IP address of the CRL server.</td></tr>
<tr><td><b>URL-Path</b></td><td>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 (the resolvable hostname) in the CN subject to refer to the CRL. For example, if a server's hostname is <i>server.domain.com</i>, 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 3.6.3, when loading the CRL from a certificate, the search string "<i>?cn=*</i>" 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><b>CRL Issuer Certificate</b></td><td>The certificate by which the CRL was signed. This is used to verify the CRL.</td></tr>
<tr><td><b>Explicit X509</b></td><td>The explicit certificate by which the CRL was signed. This is used when selecting <b>Explicit Issuer</b> from the drop-down menu.</td></tr>
<tr><td><b>Login</b></td><td><b>User / Password</b></td><td>The username and password for LDAP or HTTP servers requiring authentication.</td></tr>
</table>

Proxy	**Use Proxy**	The proxy server used for certificate revocation.
	Proxy	The DNS-resolvable hostname or IP address of the proxy server.
	Port	The proxy server port used for connection requests.
	User / Password	The username and password required by the proxy server.

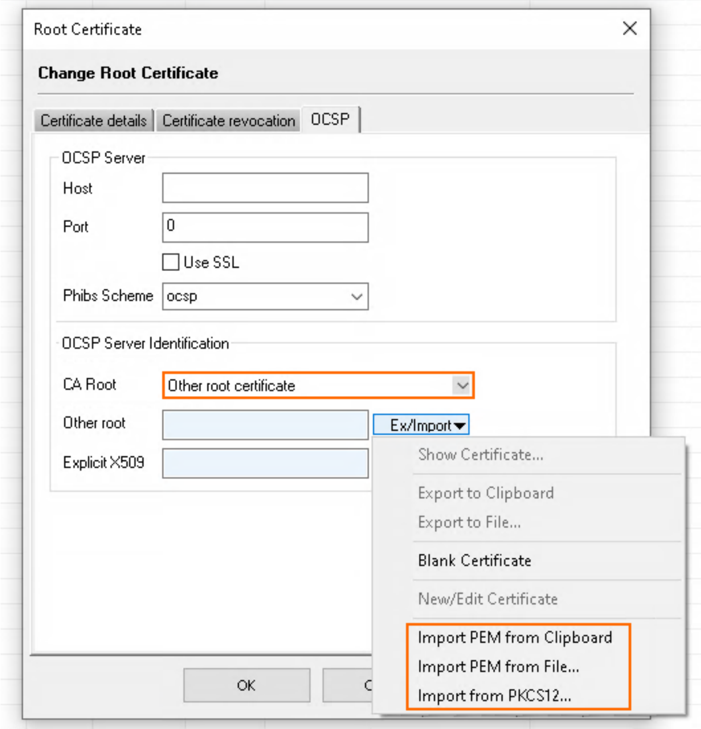
11. (optional) Click on the **OCSP** tab and configure the OCSP server.
    - **Host** – Enter the DNS resolvable hostname or IP address of the OCSP server.
    - **Port** – Enter the listening port.
    - **Use SSL** – Click to enable SSL.
    - **Phibs Scheme** – Select **ocsp**. This allows you to use OCSP as a directory service.
    - **OCSP Server Identification**
        - **This root certificate** – This certificate is used as trusted root certificate authority when verifying the signature of OCSP responses.

          > In case intermediate certificates are used in a certificate chain:
          > If the certificate chain contains one or more intermediate certificates, they must be served with the OCSP response.

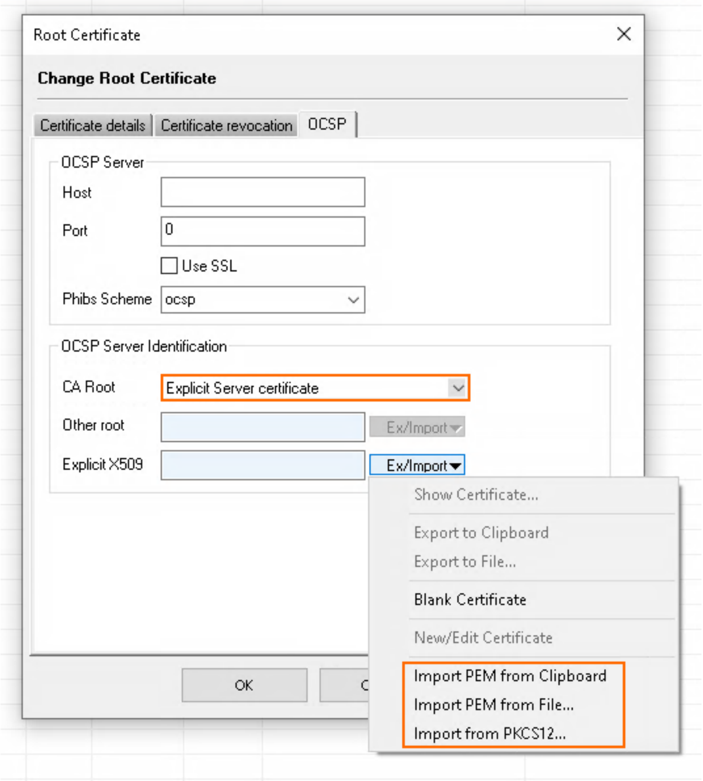
        - **Other root certificate** – The certificate that is imported via the **Other root** setting is used as trusted root certificate authority when verifying the signature of OCSP responses.

          > If the certificate chain contains one or more intermediate certificates, they must be served with the OCSP response.

            - **Option 1:**
                - Import the *root certificate* (at the top of the chain) as **Other root certificate**.
                    - For **Other root**, click **Ex/Import**.
                    - From the list, select the source where to import the root certificate from.



- **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.
  - **Option 2:**
    - Import the certificate as **Explicit Server Certificate**.
      - For **Explicit X509**, click **Ex/Import**.
      - From the list, select the source where to import the intermediate certificate from.



12. Click **OK**.

The root certificate is now displayed on the **Root Certificates** list.

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 > Assigned Services > VPN-Service > VPN Settings**.
2. In the left menu, select **Service Certificates**.
3. Click **Lock**.
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 **Service 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 on the **Service Certificates** list.

Step 3. Create a Service Key

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > VPN Settings**.
2. In the left menu, select **Service Keys**.
3. Click **Lock**.
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**.

You now have root- 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