How to Set Up VPN Certificates

https://campus.barracuda.com/doc/41116173/

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 NG Firewall, complete the following steps:

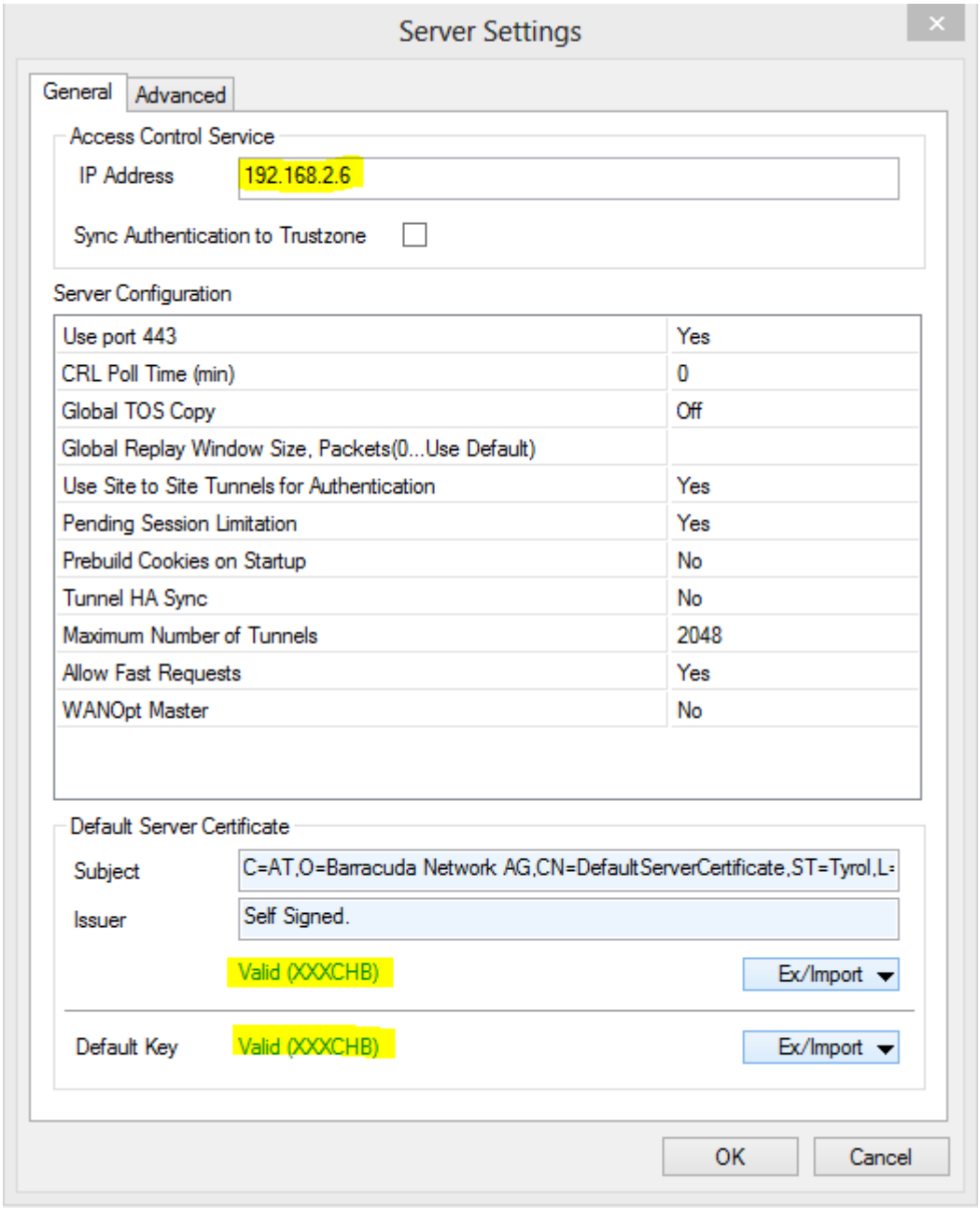
Step 1. Create the Default Certificate and Private Key

1. Open the **VPN Settings** page (**Config > Full Config > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service**).
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. This certificate will be signed by the self-signed Barracuda root certificate that is included with the Barracuda NG Firewall.
    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 and then click **OK**.
        You must set the SubAltName with the FQDN that resolves to the listening IP address of the VPN service.
7. Create the default key by clicking **Ex/Import** in the **Default Key** section and then selecting **New x-Bit RSA key** (where x is 512, 1024, or 2048).

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

Step 2. Import the Default Certificate and Private Key

1. Open the **VPN Settings** page (**Config > Full Config > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service**).
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. 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

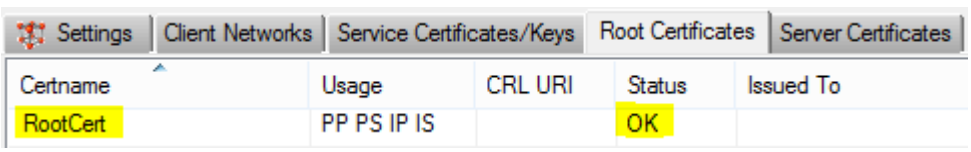
X.509 Certificate Type	Installation Location	File Type	Chain of Trust	X.509 Extensions and Value

Root Certificate (e.g., *RootCrt.crt*)	Barracuda NG Firewall	PEM	Trust Anchor	• **Key Usage:** *Certificate sign; CRL sign*
Server Certificate (e.g., *ServerCrt.pem* and *ServerCrtprivate.pem*)	Barracuda NG Firewall	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 NG Firewall must not have identical **SubjectAlternativeNames** settings and must not contain the management IP address of the Barracuda NG Firewall.
Client Certificate (if needed)	Client OS or VPN Client	PKCS12	End Instance	• **Key Usage**: *Digital Signature*

Install the Root Certificate

1. Open the **VPN Settings** page (**Config > Full Config > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service**).
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**.

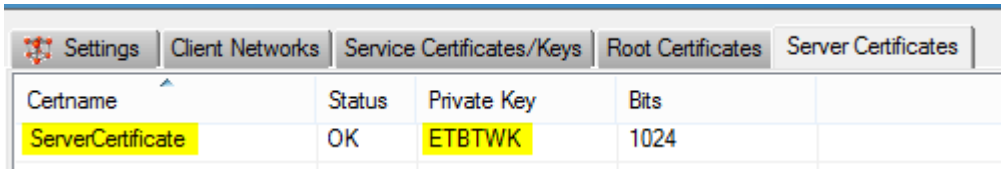
The root certificate appears under the **Root Certificates** tab.



Install the Server Certificate

1. Open the **VPN Settings** page (**Config > Full Config > Virtual Servers > *your virtual server*** **> Assigned Services > VPN-Service**).
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** (e.g., `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 (e.g. **ServerCertprivate.pem**) and then click **Open**.
6. Click **Send Changes** and **Activate**.

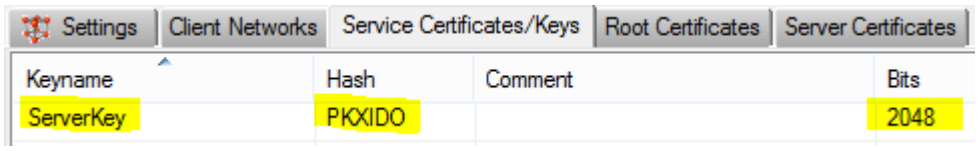
Your server certificate appears with the private key under the **Server Certificates** tab.



Create a Service Certificate/Key

1. Open the **VPN Settings** page (**Config > Full Config > Virtual Servers > *your virtual server*** **> Assigned Services > VPN-Service**).
2. Click **Lock**.
3. Click the **Service Certificates/Keys** tab.
4. Right-click the table and select **New Key**.
5. Enter a **Key Name**.
6. Select the required **Key Length**.
7. Click **Send Changes** and **Activate**.

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



Server Settings Overview

The following sections provide more details on the server settings:

General Settings

From the **General Settings** tab of the **Server Settings** window, you can configure these settings:

Section	Setting	Description
Access Control Service	**IP Addresses**	The IP address of the access control service to use.
	Sync Authentication to Trustzone	Propagates authentication information to the other systems in the same trustzone.

Server Configuration	**Use port 443** [default: **Yes**]	Defines if incoming VPN connections on port 443 should be accepted or not. VPN tunnels connecting to this port are limited to the TCP transport protocol. Port 443 can only be used by one service. If this port is redirected to another machine by the firewall service or a SSL VPN is running, disable port 443 for client-to-site VPN connections.
	CRL Poll Time	The time interval in minutes for fetching the Certificate Revocation List. Entering `0` results in a poll time of 15 minutes.
	Global TOS Copy	Enables the Type of Service (ToS) flag for site-to-site tunnels. By default, the ToS flag is globally disabled (setting: *Off*). Individual tunnel ToS policies override the global policy settings.
	Global Replay Window Size [0]	If ToS policies assigned to VPN tunnels or transports packets are not forwarded instantly according to their sequence number, you can configure the replay window size for sequence integrity assurance to avoid IP packet "replaying." The window size specifies a maximum number of IP packets that can be on hold, until it is assumed that packets have been sent repeatedly and sequence integrity has been violated. Individual window size settings are configurable per tunnel and transport, overriding global policy settings. To specify that tunnel- and transport-specific settings should be used, enter *0* (default). To view the specified replay window size, double-click the tunnel on the **VPN** page to open the **Transport Details** window (attribute: transport_replayWindow).
	Use Site to Site Tunnels for Authentication [Yes]	Typically, a tunnel registers itself at the firewall, creating an auth.db entry with the tunnel network and the tunnel credentials. You can then create a firewall rule with the tunnel name or credentials as a condition. This feature is rarely used (maybe not at all).
	Pending Session Limitation [Yes]	Enforces a limit of five sessions. Additional session requests are dropped.
	Prebuild Cookies on Startup [No]	Prebuilds the cookies when the VPN service is started. This can slow the VPN service startup but increases the speed of tunnel builds. Typically, cookies are built on demand while a VPN tunnel is initiated. Enable this setting to prevent high system load on Barracuda NG Firewalls that are concentrating a large number of VPN tunnels. High system load caused by the VPN service can occur, if a large number of VPN tunnels are established simultaneously after a reboot or Internet Service Provider outage.
	Tunnel HA Sync	Synchronization is only provided for TINA tunnels and transports using either UDP or ESP. Synchronization of hybrid, TCP, or IPsec tunnels is not available. During an HA takeover, the initialization of all VPN tunnels and transports requires a very CPU-intensive RSA handshake procedure. As long as less than approximately 200 tunnels and transports are terminated, this initialization happens very quickly and does not decrease overall system performance. Due to real-time synchronization to the HA partner unit, the system load during a takeover can be decreased, providing faster tunnel re-establishment. By default, this setting is disabled. It can be activated using **Tunnel HA Sync** through the VPN server settings. Barracuda Networks recommends that you only activate this setting when using more than 200 ESP or UDP TINA tunnels.
	Maximum Number of Tunnels	The maximum number of concurrent client-to-site and site-to-site tunnels accepted by the VPN service. Leave the default setting or select one of the values available from the drop-down list.
	Allow Fast Requests	Allows a fast request rate.
	WANOpt Master	• If the tunnel endpoint inherits the WANOpt settings from the tunnel partner, select *Yes*. • If the tunnel partner inherits the WANOpt settings from the tunnel endpoint, select *No*. Do not set both tunnel endpoints to the same value.

Default Server Certificate Section	**Subject/Issuer**	These two fields display the certificate subject and issuer. Note, that L2TP and IPsec require server certificates with SubAltName: DNS:your.vpnserver.com
	Default Key	If the VPN server demands a key but the key is not stated explicitly, you can generate it by clicking **Ex/Import** and selecting a suitable option.
	For a successful client-to-site connection, you must define a default server certificate.	

Advanced Settings

From the **Advanced Settings** tab of the **Server Settings** window, you can configure these settings:

Section	Description
VPN Interface Configuration | VPN Next Hop Interface Configuration	In these sections, configure the VPN interfaces and next hop interfaces. To add and configure virtual interfaces equipped with unique index numbers, click **Add**. Indexed virtual interfaces may, for example, be required for direct OSPFv2 or RIP multicast propagation of VPN networks. After assigning the interface with a local IP address, it may be directly used within the OSPF router configuration. The interfaces become active and visible on the **Control > Network** page of the corresponding Barracuda NG Firewall as soon as a tunnel endpoint using the indexed interface has been created. Indexed VPN interfaces are labeled as follows: *vpn[INDEX]* For example: *vpn1* In the **VPN Interface Properties** window, edit the following settings for each interface: • **VPN Interface Index** – The unique index number of the VPN interface. • **MTU** – The Maximum Transmission Unit size. You can select either *1398* or *1500*. • **IP Addresses** – The IP addresses that should be started on the *vpnX* interface. You can enter a space-delimited list of IP addresses. • **Multicast Addresses** – The multicast addresses that should be propagated into this field. You can enter a space-delimited list of IP addresses. For example, to transport OSPF multicast via the VPN tunnel, enter `224.0.0.5` `224.0.0.6`

IKE Parameters	In this section, configure the global IKE settings for all configured IPsec tunnels. You can edit the following settings: • **Exchange Timeout (s)** – The maximum period to wait until the request for IPsec tunnel connection establishment has to be approved by the remote peer (default: *30* seconds). • **Tunnel Check Interval (s)** – The interval between queries for a valid exchange that is assignable to an IPsec tunnel (default: *5* seconds). If a tunnel that is configured with direction assignment *Active* has been terminated, it will be re-established automatically when the check interval expires. If a tunnel that is configured with direction assignment *Passive* has been terminated, a corresponding status message is triggered and the interface is updated on the **VPN** page. • **Dead Peer Detection Interval (s)** – The interval between keep-alive checks on the remote peer (default: 5 seconds). • **Use IPSec dynamic IP** – If the service is connected to the Internet via a dynamic link (dynamic IP address), select *Yes*. The server IP address is not yet known at configuration time and IKE then listens to all local IP addresses. • **IPSec Log Level** – The debug log level of IKE. The debug log may be very "noisy." Do not select a log level greater than *0* if the log is not required for solving an issue.
Custom Ciphers	In this section, add or remove custom ciphers.

Certificate Import Settings Overview

The following sections provide more details on the settings for importing certificates:

Certificate Detail Settings

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

Section	Setting	Description
Certificate Details	**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.	

CRL Error Handling	**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.

- If a CRL is already included within the certificate, import the CRL URI by clicking **Load paths from certificate**.
- To add a CRL URI manually, configure the settings in the **URI**, **Login**, and **Proxy** sections and then click **Add**.

Section	Setting	Description
URI	**Protocol**	The required connection protocol. The following protocols are available: **Protocol** / **Default Port** / **Comment** LDAP / 389 / DNS-resolvable LDAPS / 636 / DNS-resolvable HTTP / 80 / - HTTPS / 443 / -
	Host	The DNS-resolvable host name or IP address of the server that makes the CRL available.

	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 NG Firewall 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.

Login	**User / Password**	The username and corresponding password. This information is necessary if the LDAP or HTTP server requires authentication.
Proxy	**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.

OCSP Settings

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

Setting	Description
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. ngadmin_server_settings_client_to_site.PNG
2. ngadmin_root_certificate_vpn.PNG
3. ngadmin_server_key_client_to_site.PNG
4. ngadmin_service_certificates_and_keys_client_to_site.PNG