

How to Configure a Client-to-Site VPN with Certificate Authentication

<https://campus.barracuda.com/doc/11142156/>

The Barracuda NextGen Firewall X-Series supports client-to-site VPN with certificate authentication. You can use either the Barracuda VPN client, mobile clients running iOS or Android, as well as third-party IPsec clients supporting client authentication:

Mobile devices

The X-Series Firewall supports IPsec VPN connections for Apple iOS and Android devices. You must enable the **IPsec client** option in the access policy to be able to connect with a mobile client.

Barracuda VPN client

The Barracuda VPN client authenticates with the certificate and username/password. You must enable the **Barracuda VPN Client** option in the access policy to be able to connect with the Barracuda VPN client.

Third-party IPsec clients

The X-Series Firewall adheres to the IPsec standard. Any third-party IPsec client implementing this standard can connect to the IPsec VPN. You must enable IPsec client in the access policy to use the IPsec VPN client.

Step 1. Enable the VPN service on a network interface

Enable the VPN service on a static IP address. If you do not have a static WAN IP address, you must enable the VPN service for a static internal interface and then redirect incoming connections to the VPN service with a firewall rule.



Static (fixed) WAN IP address

To enable the VPN service for the static network interface:

1. Go to the **NETWORK > IP Configuration** page.
2. In the **Static Interface Configuration** section click **Edit** to configure your static WAN interface.

STATIC INTERFACE CONFIGURATION

Add Static Network Interface

Name	IP Address/Mask	Interface	Classification	Action
HQDMZ	172.16.0.1/255.255.255.0	p4	DMZ	Edit 
HQISP1	62.99.0.50/255.255.255.0	p3	WAN	Edit 

3. In the **Edit Static Network Interface** window, select the **VPN Server** check box.

Network Interface: p3 ▾

Name: HQISP1
Maximum 8 characters, no spaces allowed.

IP Address: 62 . 99 . 0 . 50

Netmask: 255 . 255 . 255 . 0

Services to Allow: ☒ Ping ☐ DNS Server ☒ **VPN Server** ☐ SSL VPN
Enable/Disable 'reply to ping' or NTP requests.

If SSL VPN service is also enabled for this interface, go to the **VPN > Site-To-Site VPN** page and disable the **Use TCP Port 443** setting for the VPN service.

4. Click **Save**.

Dynamic (DHCP/3G/PPPoE) WAN IP Address

You must have an active DynDNS account, so that the client can connect to the dynamic IP address. For more information on creating a DynDNS account, see <http://www.dyndns.org>.

To use the VPN service with a dynamic WAN IP address, run the VPN service on an internal IP address. Do not use the management IP address; instead, add a secondary IP address. Then, create an access rule to redirect all incoming VPN traffic from the dynamic interface to the VPN service.

- Go to the **NETWORK > IP Configuration** page.
- Enable dynamic DNS.
 - In the **Dynamic Interface Configuration** section, click **Edit** to configure the dynamic WAN interface.
 - In the **Edit Dynamic Network Interface** window, enable **Use Dynamic DNS**.
 - Enter the **DynDNS Hostname** and authentication information.
 - Click **Save**.
- In the **Management IP Configuration** section, enter a secondary IP address:
 - IP ADDRESS** – Enter an IP address that is free in the local network. For

example, 10.0.10.6 if the MIP address is in the 10.0.10.0/24 network.

- **VPN SERVER** – Select this check box.

Secondary IP Addresses:

IP Address	Ping	DNS Server	VPN Server	SSL VPN	
- . - . -	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Add
10 . 0 . 10 . 6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

4. Click **Add**.

5. Create an access rule to redirect incoming VPN connections on the dynamic interface to the VPN server listening on the local IP address.

1. Go to the **FIREWALL > Firewall Rules** page.
2. Click **Add Access Rule**.
3. In the **Add Access Rule** window, configure a **Redirect to Service** firewall rule.
 - For the **Destination**, select the network object corresponding to your Internet connection type (DHCP, 3G, or DSL).
 - For the **Redirected To** setting, select the **VPN** network object.

Add Access Rule ?

General Advanced

Action:

Redirect to Service

Name:

DynamicIP-2-VPN

Bi-directional:

☐ Yes ☒ No

Disable:

☐ Yes ☒ No

Description:

IPS:

☒ Yes ☐ No

Application Control:

☐ Yes ☒ No

URL Filter:

☐ Yes ☒ No

Virus Protection:

☐ Yes ☒ No

SSL Inspection:

☐ Yes ☒ No

Connection:

Default (SNAT)

Adjust Bandwidth:

Internet

The interface must have bandwidth management enabled on the NETWORK > IP Configuration page for this policy to be applied.

URL Filter, Virus Protection and SSL Inspection depend on Application Control enabled. URL Filter and Virus Protection require a valid Web Security subscription.

Source

Internet

Ref: Any

Redirect to Service Details

VPN

The following protocols and port/protocol combinations are automatically selected upon the chosen Service VPN:

UDP 691, UDP 500, UDP 4500, UDP 1701, TCP 1723, TCP 691, TCP 443

Destination

Trusted LAN

Ref: DHCP1 Local IP

Ref: DSL1 Local IP

Ref: 3G Local IP

☒ Network Objects ☐ IP Address ☐ Geo Loc.

☒ Network Objects ☐ IP Address ☐ Geo Loc.

4. Click **Save**.

6. Move the access rule above the **BLOCKALL** rule so it is the first access rule to match incoming VPN traffic. For more information, see [Firewall Rules Order](#).

7. Click **Save**.

Step 2. Upload or create certificates

Use a third-party PKI to create the VPN and client certificates. For more information on how to create certificates, see [How to Create Certificates with XCA](#) and [How to Create Certificates for a Client-to-Site VPN](#).

The **SubAlt name** of the VPN server certificate must be DNS: examplevpn.domain.com or DNS: *. If you are using an FQDN, it must resolve to the IP address of the X-Series Firewall VPN service.

1. Go to the **ADVANCED > Certificates** page.
2. Click **Upload**.
 - **Certificate Name** - Enter VPN Certificate.
 - **Certificate Type** - Select the type of certificate you want to upload.
 - **Add to VPN Certificates** - Enable the checkbox.
 - **Certificate File** - Select the certificate file you want to upload.
3. Click **Save**.

Step 3. Configure client-to-site VPN settings

Configure user authentication and IPsec settings.

Step 3.1 Configure user authentication and select the certificate

1. Go to the **VPN > Client-To-Site VPN** page.
2. In the **Settings** section, select a **User Authentication** method. You can use local or [external user authentication](#).
3. From the **Local Certificate** list, select the certificate that you created in Step 2 (e.g., **VPNCertificate**).
4. Click **Save**.

Step 3.2 Configure IPsec settings for certificate authentication

Configure the authentication type and, if needed, the encryption algorithms for IPsec phase 1 and 2.

1. Go to the **VPN > Client-To-Site VPN** page.
2. In the **IPsec Settings** section select **Client Certificate** as the **Authentication** type.
3. (optional) Configure the **IPsec Phase 1 Settings** and **IPsec Phase 2 Settings**.

Do not change the default IPsec Phase 1 and Phase 2 settings if you want to use iOS or Android devices as VPN clients,

4. Click **Save**.

IPSEC SETTINGS

Authentication

☐ Shared Key ☐ Shared Key or Client Certificate ☒ Client Certificate

Shared Key: Requires an additional password (shared key) to be entered below.

IPsec Phase 1 Settings

Encryption	Hash	DH Group	Lifetime
AES	SHA	Group 2	3600

Lifetime in seconds, from 60 to 86400. Recommended: 3600

IPsec Phase 2 Settings

Name	Encryption	Hash	DH Group	Lifetime	
	AES	SHA	Group 2	3600	Add
Client2SiteVPNclients	AES	SHA	Group 2	3600	

To connect with iOS or Android mobile devices, select Encryption: AES, HASH: SHA, Group: Group 2 and Lifetime: 3600

Step 3.3 Create a VPN access policy

Define the VPN clients and network information to be passed to client.

Access policies are matched based on the **Allowed Group** of the access policy from top to bottom. Make sure access policies are entered so the more specific **allowed groups** are on the top of the list and the generic * conditions are on the bottom of the list.

- Go to the **VPN > Client-To-Site VPN** page.
- In the **VPN Access Policies** section, click **Add Access Policy**.
- In the **Add VPN Access Policy** window, configure the following settings:
 - Name** – A name for the access policy.

The name of the access policy is referred to as **group name** on iOS and Android devices.
 - Client Network** – The network that the client will be assigned to (e.g., 192.168.100.0/24).
 - (Optional) Domain** – The domain assigned to the client.
 - Primary DNS Server** – The IP address of the DNS server.
 - Published Networks** – The local networks available for the VPN client.

Add 0.0.0.0/0 to the Published Networks to allow the client to access the Internet through the VPN tunnel.
 - IPsec Phase 2** – The IPsec Phase 2 settings that you configured in Step 3.2 (e.g., **Client2SiteVPNclients** from the example in Step 3.2).
 - No Split Tunnel Mode** – Enable to lock down the client to only connect to the **Published Networks** of the VPN tunnel. Windows hosts using the Barracuda VPN client only.

Enabling this option blocks VPN access for all non-Windows clients!

- **Allowed Peers** – Enable **IPsec Clients** for mobile devices and third-party IPsec clients and **Barracuda VPN client** to be able to connect with the Barracuda VPN client.
- **Allowed Groups** – The groups that are allowed to connect. To allow all groups, enter an asterisk (*).
- **Use for CudaLaunch** – Enable self-provisioning on Windows, macOS, or iOS devices for remote clients using the CudaLaunch portal. For more information, see [CudaLaunch](#).
Configure the following settings:
 - **CudaLaunch Server** – Enter the IP address of the server providing CudaLaunch.
 - **Allowed Groups** – Enter the user groups that the policy applies to. Click + after each entry. You can use question marks (?) and asterisks (*) as wildcard characters.

4. Click **Save**.

Step 4. Configure clients

Configure VPN clients to connect to the IPsec VPN with certificate authentication.

Barracuda VPN clients

Configure the Barracuda VPN client to connect to the IPsec VPN with certificate authentication you just created.

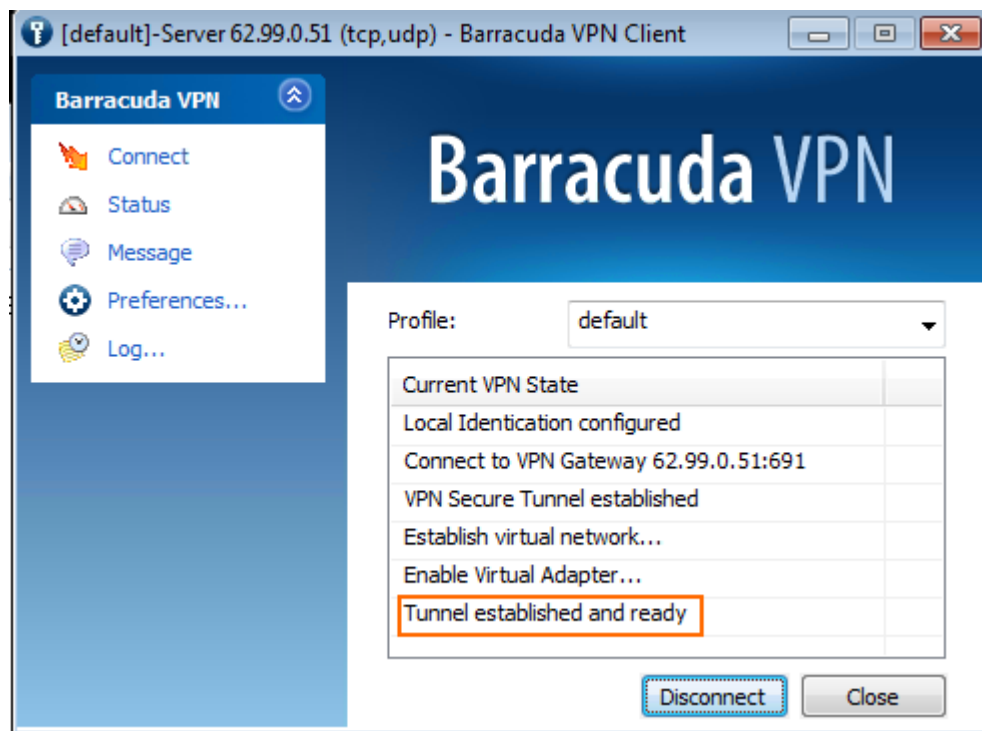
1. Go to the **VPN > Client-To-Site** page.
2. Download and install the Barracuda VPN Client.
 1. In the **Settings** section, select your operating system from the **Download Barracuda VPN Client** list and click **Download**.
 2. Install the **Barracuda VPN Client**. You must have administrative rights.
 3. Reboot the computer after the installation.
3. Configure a profile for connecting to the IPsec VPN.
 1. Start the Barracuda VPN Client.
 2. In the left pane, click **Preferences**.
 3. In the **Barracuda VPN Control** window, right-click the **default** profile and select **Modify Profile**.
 4. In the **Properties** window, specify these settings:
 - **Certificate** – Select **X509 authentication**.
 - **Remote Server** – Enter the WAN IP address or DynDNS name (e.g., 62.99.0.51 or bfw-vpn.dyndns.org) in the **Host names or IP addresses of remote server** field.
 5. Click **OK**.
4. Close the **Barracuda VPN Control** window.

After configuring the Barracuda VPN client, you can connect to the IPsec VPN:

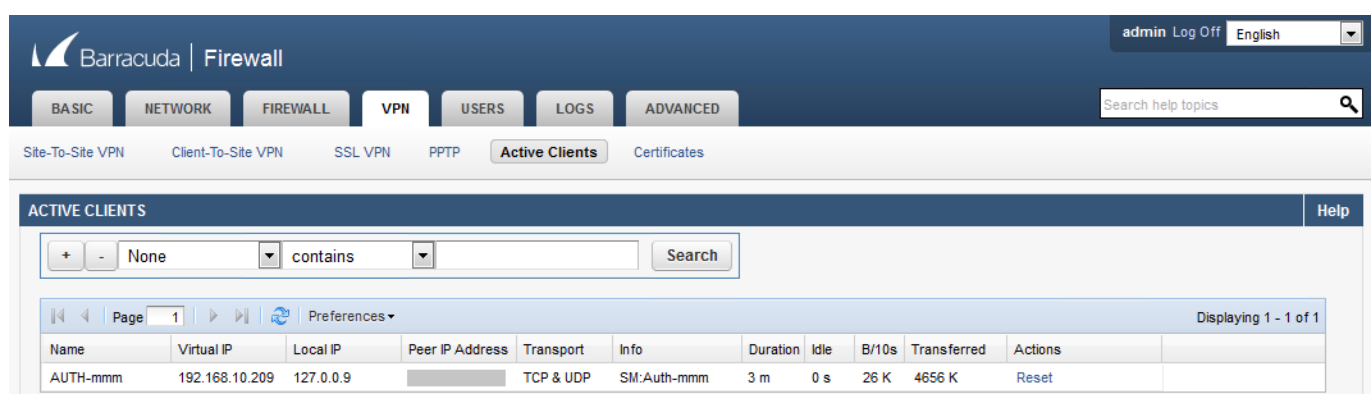
1. Start the **Barracuda VPN Connector**.

2. Enter your **Username** and **Password**.
3. Click **Connect**.

You are now connected to the client-to-site IPsec VPN with the Barracuda VPN Client.



The connection status is displayed on the **VPN > Active Connections** page.



Mobile clients

For instructions on configuring mobile clients, see these articles:

Mobile OS	Supported Version	Article
-----------	-------------------	---------

Apple iOS	5.2 and above	How to Configure the Apple iOS VPN Client for IPsec Shared Key VPN
Android	4.0 and above	How to Configure the Android VPN Client for IPsec Shared Key VPN

Third-party IPsec VPN clients

The X-Series Firewall adheres to the IPsec standard. Any third-party IPsec client implementing this standard can connect to the IPsec VPN.

Figures

1. c2sIPsec_67_01.png
2. c2sIPsec02_67.png
3. c2sIPsec03_67.png
4. c2sIPsec04_67.png
5. c2sIPsec07_67.png
6. c2sIPsec06.png
7. c2s_connect.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.