Example - Client-to-Site TINA VPN with Client Certificate Authentication

Use a Client-to-Site VPN to let mobile workers connect securely to your Barracuda NextGen Firewall F-Series. Each client must have a valid client certificate as well as the username and password to authenticate. The client must use the Barracuda VPN Client or CudaLaunch on Android to connect to the Barracuda NextGen Firewall F-Series via the TINA VPN protocol. By default, each user can have only one concurrent client-to-site VPN connection. A Remote Access Premium subscription is required to enable concurrent Client-to-Site VPN sessions by the same user. You can connect from any IPv4 or IPv6 address, as long as an external IPv4 and IPv6 address are configured as a service IP address for the VPN service. Traffic passing through the Client-to-Site VPN is limited to IPv4.

Supported VPN clients

The following client is supported for this client-to-site configuration:

- CudaLaunch for Android via VPN Templates in SSL VPN. For more information, see How to Configure VPN Group Policies in the SSL VPN.
- VPN Client & Network Access Client

Before you begin

- Set up the VPN certificates for External CA. For more information, see How to Set Up External CA VPN Certificates.
- Configure an external or local authentication service. For more information, see Authentication.
- Identify the subnet and gateway address to use for the VPN service in your network (e.g., 192.168.6.0/24 and 192.168.6.254).
- Identify the IPv4 and IPv6 addresses the VPN service is listening on. If you are using a dynamic WAN IP, see How to Configure VPN Access via a Dynamic WAN IP Address.

Step 1. Configure the VPN service listeners

Configure the IPv4 and IPv6 listener addresses for the VPN service.

1. Go to CONFIGURATION > Configuration Tree> Box > Virtual Server > your virtual server > Assigned Services > VPN > Service Properties.
2. Click Lock.
3. From the Service Availability list, select the source for the IPv4 listeners:
   - First+Second-IP - The VPN service listens on the first and second virtual server IPv4 address.
   - First-IP - The VPN service listens on the first virtual server IPv4 address.
   - Second-IP - The VPN service listens on the second virtual server IPv4 address.
   - Explicit - For each IP address, click + and enter the IPv4 Addresses in the Explicit Service IPs list.
4. Click + to add an entry to the Explicit IPv6 Service IPs.
5. Select an IPv6 listener from the list of configured explicit IPv6 virtual server IP addresses.

6. Click **Send Changes** and **Activate**.

**Step 2. Create the VPN client network**

All VPN clients will receive an IP address from the VPN client network with a static gateway. You can choose the gateway IP address freely from the subnet.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.
3. Verify that the default server certificate and key are valid.
   1. Right-click the **Settings** table and select **Edit Server Settings**.
   2. Verify that the **Default Server Certificate** and **Default Key** are both valid (green). If the **Default Server Certificate** and **Default Key** are not valid, see **How to Set Up Barracuda VPN CA VPN Certificates**.
4. Click **OK** to close the **Server Settings** window.
5. Configure the client network.
   1. Click the **Client Networks** tab.
   2. Right-click the table and select **New Client Network**. The **Client Network** window opens.
   3. In the **Client Network** window, configure the following settings:
      - **Name** – Enter a descriptive name for the network.
      - **Network Address** – Enter the base network address for the VPN clients. E.g., 192.168.6.0
      - **Network Mask** – Enter the subnet mask for the VPN client network. E.g., 24
      - **Gateway** – Enter the gateway network address. E.g., 192.168.6.254
**Type** – Select **routed (Static Route)**. VPN clients are assigned an address via DHCP (fixed or dynamic) in a separate network reserved for the VPN. A static route on the Barracuda NextGen Firewall F-Series leads to the local network.

5. Click **OK**.
6. Upload the root certificate:
   1. Click the **Root Certificates** tab.
   2. Right-click the table and select **Import CER from File** or **Import PEM from File**. The **Root Certificate** window opens.
   3. Enter the **Name** for the root certificate.
   4. In the **Usage** section, select **Barracuda Personal**.
   5. (optional) Click on the **Certificate revocation** tab to configure a CRL host.
   6. (optional) Click on the **OCSP** tab to configure an OCSP server. For more information, see **How to Configure OCSP Validation**.
   7. Click **OK**.
7. Upload the service certificate:
   1. Click the **Service Certificates/Keys** tab.
   2. Right-click the table and select **Import from File**.
   3. Enter a **Name**.
   4. Click **OK**.
8. Click **Send Changes** and **Activate**.

**Step 3. Configure VPN group match settings**

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > VPN-Service > Client to Site**.
2. Click **Lock**.
3. Click the **External CA** tab.
4. Click the **Click here for options** link. The **Group VPN Settings** window opens.
5. In the **Group VPN Settings** window, configure the following settings:
   1. In the **X509 Client Security** section, select **X509 Certificate**. This will force all users connecting...
to this NextGen Firewall F-Series, regardless of the Group Policy, to use client certificate authentication.

Selecting mandatory client credentials forces all group policies configured on the NextGen Firewall F-Series to comply to these client security settings. If in doubt, leave these settings unchecked.

2. In the Server section, select your previously configured authentication service from the Authentication Scheme list. For more information, see Authentication.
3. (optional) To allow only one root certificate to be used for all Group Policies on this NextGen Firewall F-Series, select the certificate from the Used Root Certificates list.
4. Select which X509 certificate field is to be verified by the Authentication Scheme selected above. Typically, this is the emailAddress, or username in the Subject.

6. Click OK.
7. Click Send Changes and Activate.

Step 4. Create a VPN group policy

The VPN Group Policy specifies the network IPsec settings and defines the conditions to be met by the client certificate.

1. Go to CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > VPN-Service > Client to Site.
2. Click Lock.
3. Click on the External CA tab and then click the Group Policy tab.
5. Enter a name for the Group Policy.
6. From the Network list, select the VPN client network.
7. In the Network Routes table, enter the network that must be reachable through the VPN connection. For example, 10.10.200.0/24.

To route all traffic through the Client-to-Site VPN tunnel, add a 0.0.0.0/0 network route.
Configure the group policy conditions. Only clients matching these conditions are allowed to connect through this group policy.

1. Right-click the **Group Policy Condition** table and select **New Rule**. The **Group Policy Condition** window opens.

2. (optional) In the **Group Pattern** field, define the groups on the authentication server that will be assigned the policy. E.g.: CN=vpnusers*

3. In the **X509 Certificate Conditions** section click **Edit/Show**. The **Certificate Condition** window opens.
   1. For each certificate condition, select the certificate field from the dropdown and enter the required value and click **Add/Change**.

   ![Certificate Condition Window](image)

   2. Click **OK**.

4. (optional) Enter an OID in the **Certificate Policy** to allow only certificates with a specific **Key Usage**. E.g. Client Authentication (1.3.6.1.5.5.7.3.2)

5. In the **Peer Condition** section, verify that **Barracuda Client** checkbox is selected.

6. In the **X509 Certificate Conditions** section, enter matching conditions for the X509 client certificates.

9. Click **OK**.
10. Click **OK**.
11. Click **Send Changes** and **Activate**.

### Step 5. Add access rules

Add an access rule to allow traffic from your Client-to-Site VPN to your network. For more information, see [How to Configure an Access Rule for a Client-to-Site VPN](#).

### Monitoring VPN connections

On the **VPN > Client-to-Site** page, you can monitor VPN connections. Clients authenticated via client certificate use a **Name** in the following format: `<GroupPolicy name>-<certificate serial number>-<username>`.

The page lists all available Client-to-Site VPN tunnels. In the **Tunnel** column, the color of the square indicates the status of the VPN:

- **Blue** – The client is currently connected.
- **Green** – The VPN tunnel is available but currently not in use.
- **Grey** – The VPN tunnel is currently disabled. To enable the tunnel, right-click it and select **Enable Tunnel**.

For more information about the **VPN > Client-to-Site** page, see **VPN Tab**.

### Troubleshooting

To troubleshoot VPN connections, see the `/yourVirtualServer/VPN/VPN` and `/Box/Control/AuthService` log files. For more information, see **LOGS Tab**.
Configure the VPN client to connect to this VPN profile. For more information, see Remote Access Clients.
Figures