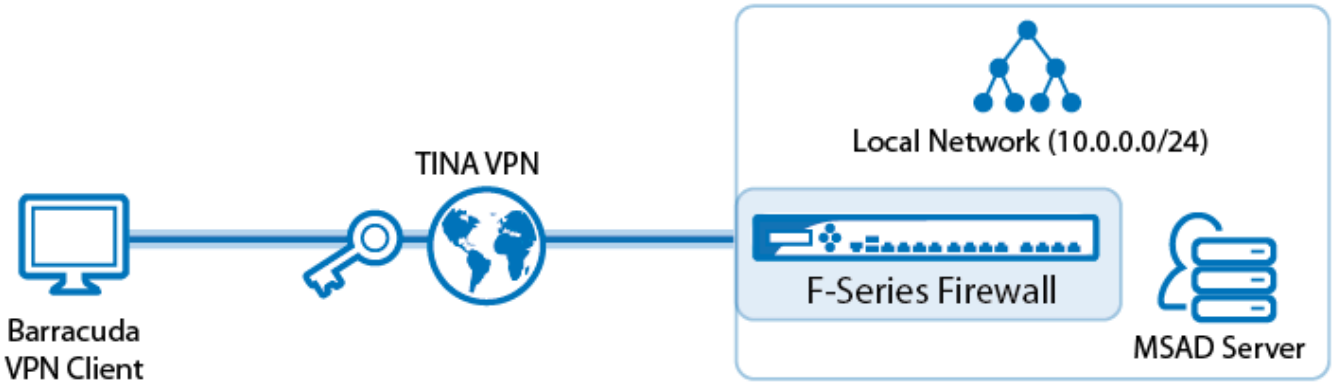
How to Configure a Client-to-Site TINA VPN with Client Certificate Authentication

https://campus.barracuda.com/doc/46208894/

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.



In this article:

Supported TINA VPN Clients

The following clients are supported with the Barracuda NextGen Firewall F-Series:

- Barracuda VPN / Network Access Clients
- CudaLaunch for Android

Before You Begin

- 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 IP address the VPN service is listening on. If you are using a dynamic WAN IP, see

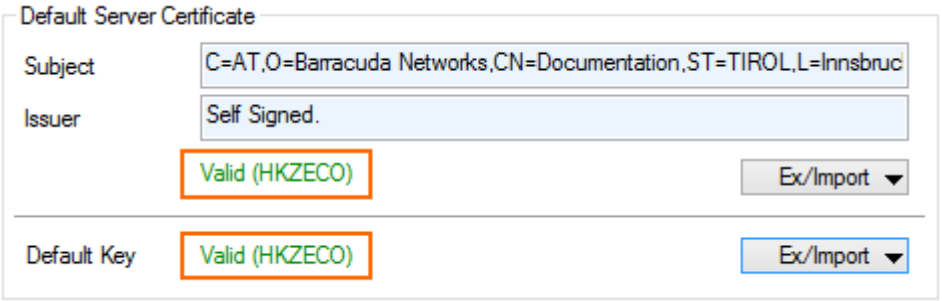
How to Configure VPN Access via a Dynamic WAN IP Address.

- Create ROOT (*.cer or *.pem), service (*.cer or *.pem), and client (*.cer) certificates. For more information, see How to Create Certificates with XCA.

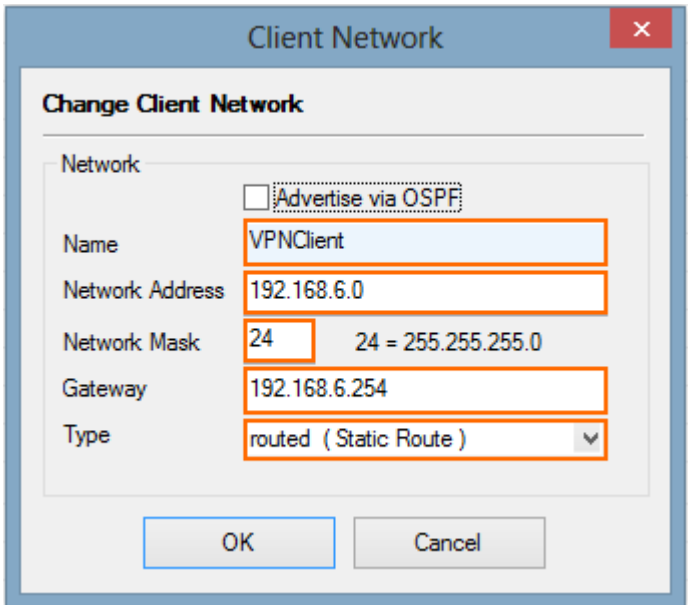
Step 1. Create the VPN Client Network

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 VPN Certificates.



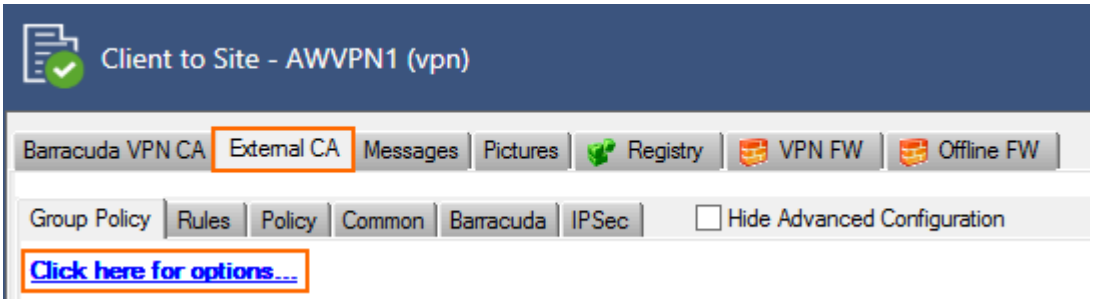
   3. Click **OK** to close the **Server Settings** window.
4. Configure the client network.
   1. Click the **Client Networks** tab.
   2. Right-click the table and select **New Client Network**. The **Client Network** window opens.
   3. In the **Client Network** window, configure the following settings:
      - **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.



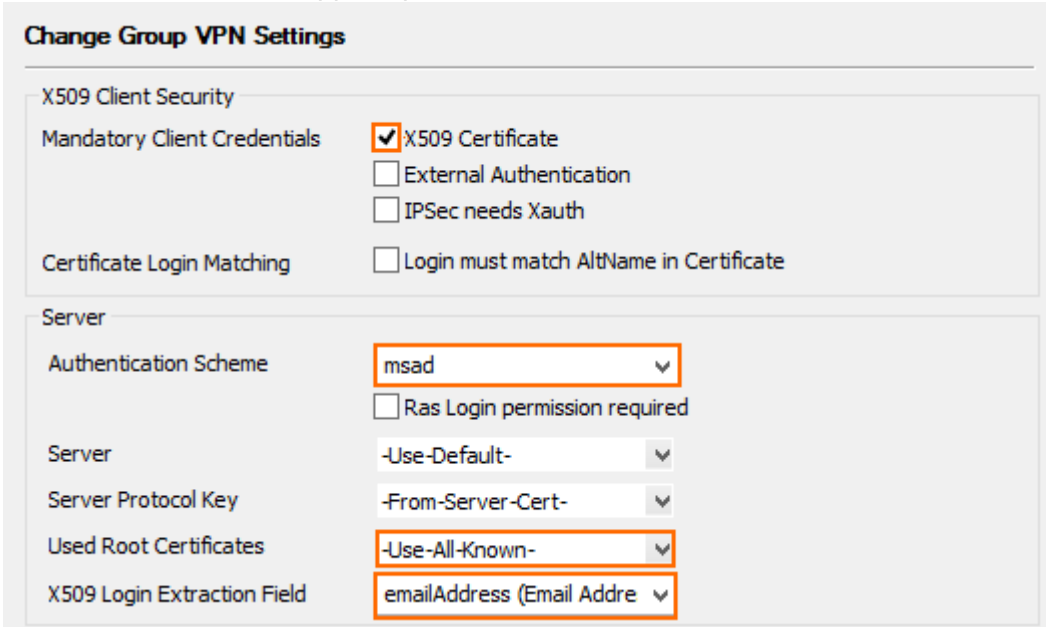
5. Click **OK**.
6. Upload the root certificate:
    1. Click the **Root Certificates** tab.
    2. Right-click the table and select **Import CER from File** or **Import PEM from File**. The **Root Certificate** window opens.
    3. Enter the **Name** for the root certificate.
    4. In the **Usage** 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 2. 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 3. Create a VPN Group Policy

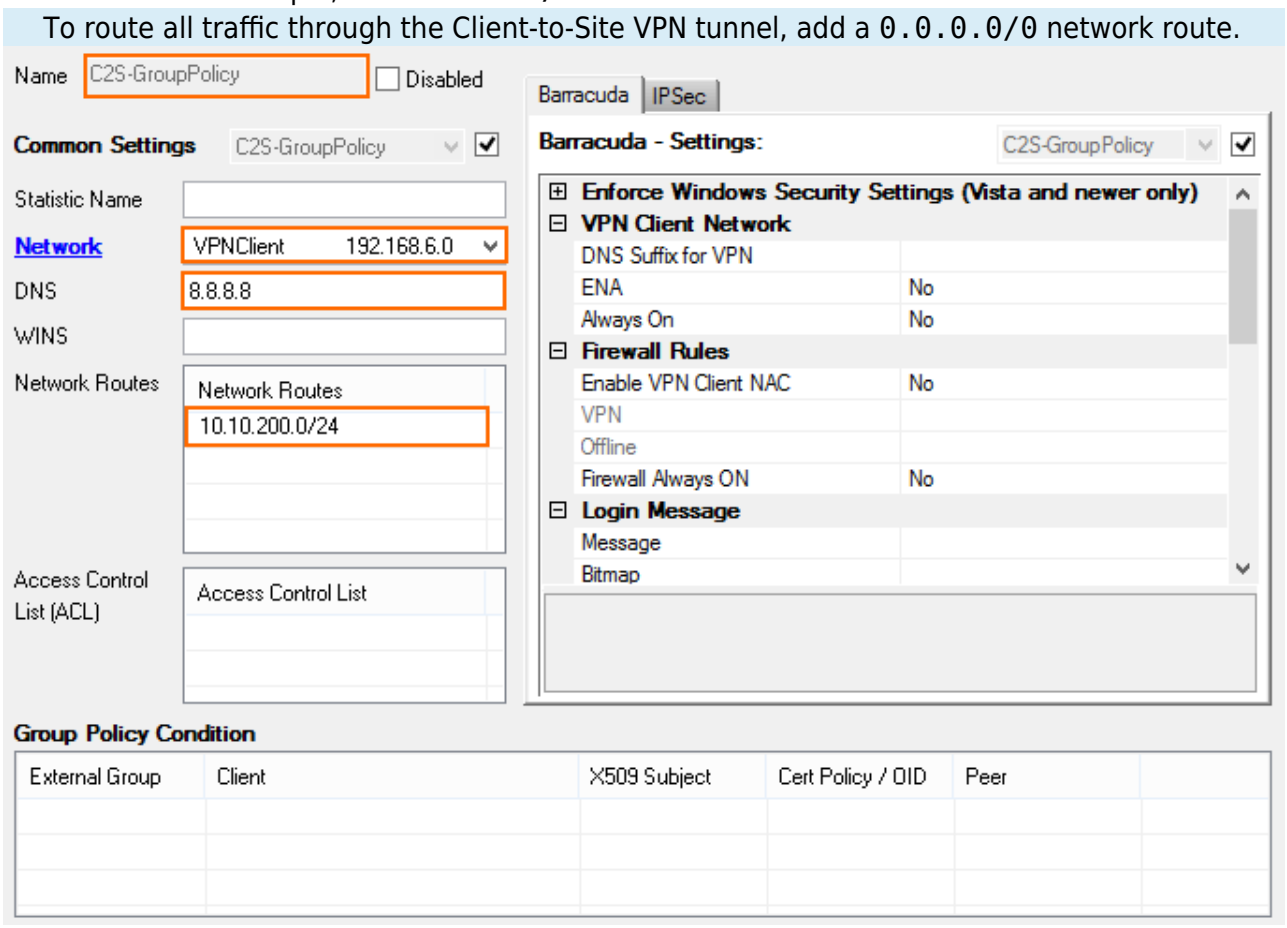
The VPN Group Policy specifies the network IPsec settings and defines the conditions to be met by the client certificate.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual***

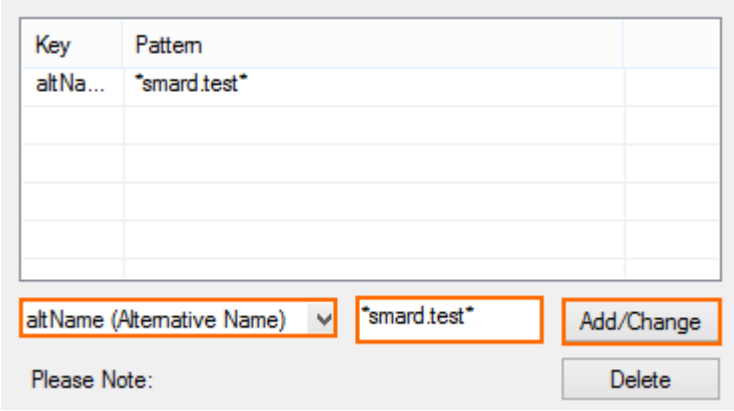
server **> Assigned Services > VPN-Service > Client to Site**.

2. Click **Lock**.
3. Click on the **External CA** tab and then click the **Group Policy** tab.
4. Right-click the table and select **New Group Policy**. The **Edit Group Policy** window opens.
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.



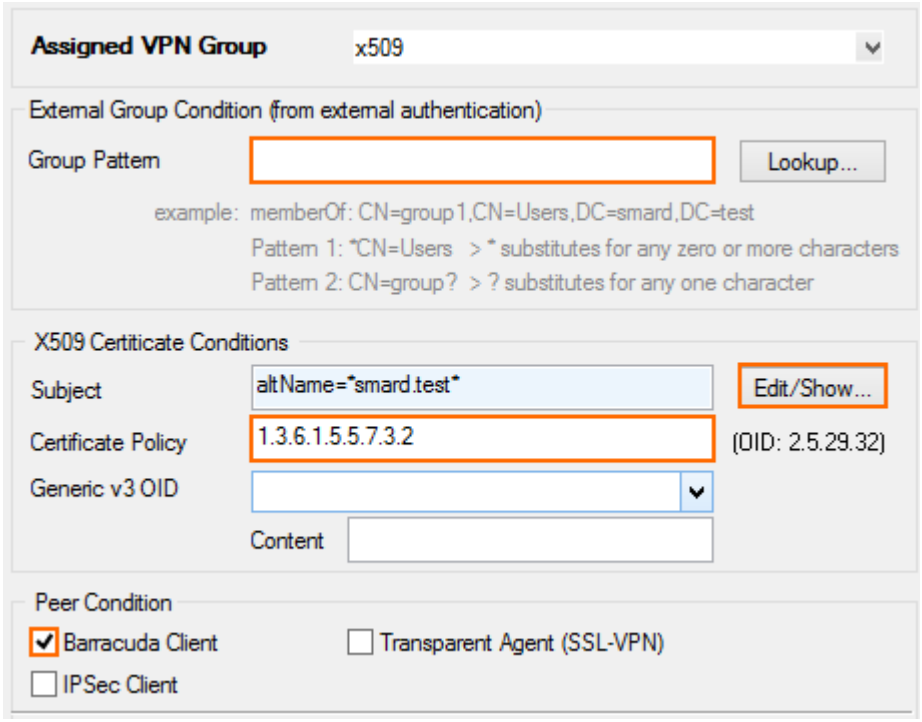
8. Configure the group policy conditions. Only clients matching these conditions are allowed to connect through this group policy.
   1. Right-click the **Group Policy Condition** table and select **New Rule**. The **Group Policy Condition** window opens.
   2. (optional) In the **Group Pattern** field, 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**.



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**.



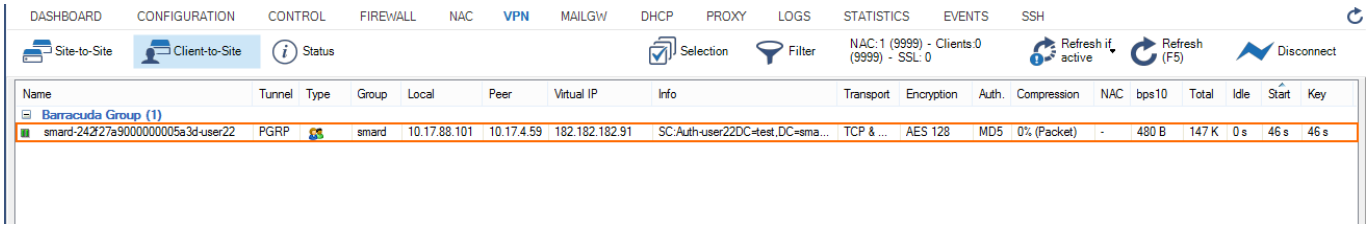
10. Click **OK**.
11. Click **Send Changes** and **Activate**.

Step 4. 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: --.



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.

Figures

1. Client2SiteTINA_CertsVPN.png
2. PSK01.png
3. PSK03.png
4. PSK04.png
5. X509_01.png
6. PSK06.png
7. X509_03.png
8. X509_02.png
9. X509_04.png