How to Create a TINA VPN Tunnel between F-Series Firewalls

https://campus.barracuda.com/doc/46209003/

As the TINA protocol offers significant advantages over IPsec, it is the main protocol that is used for VPN connections between Barracuda NextGen F-Series Firewalls. Many of the advanced VPN features, such as Traffic Intelligence, multiple Transports, or WAN Optimization are only supported for TINA Site-to-Site VPN tunnels.

In this article:

You must complete this configuration on both the local and the remote Barracuda NextGen Firewall F-Series by using the respective values below:

	Example Values for the Local Firewall	Example Values for the Remote Firewall
VPN Local Networks	10.0.10.0/25	10.0.81.0/24
VPN Remote Networks	10.0.81.0/24	10.0.10.0/25
External IP Address (Listener VPN Service)	62.99.0.40	212.86.0.10

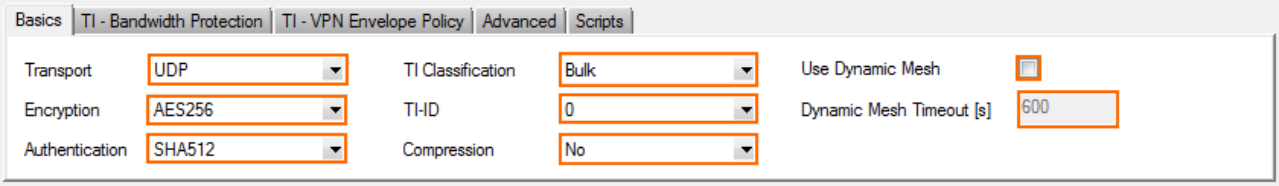
The following sections use the default transport, encryption, and authentication settings. For more detailed information, see TINA Tunnel Settings.

Step 1. Configure the TINA Tunnel at Location 1

For the F-Series Firewall at Location 1, configure the network settings and export the public key. For more information on specific settings, see TINA Tunnel Settings

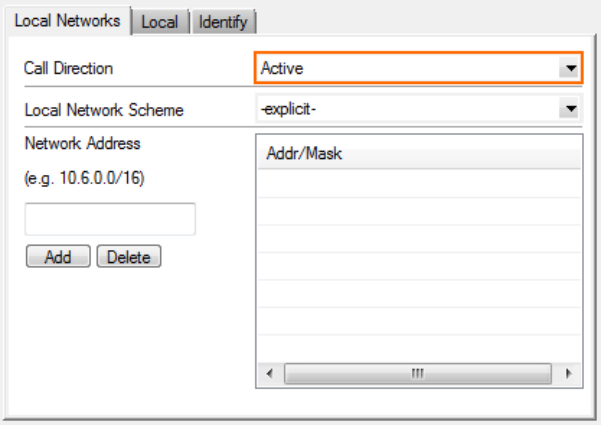
1. Log into the Firewall at Location 1.
2. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN > Site to Site**.

3. Click **Lock**.
4. Click the **TINA Tunnels** tab.
5. Right-click the table, and select **New TINA tunnel**.
6. In the **Name** field, enter the name for the new VPN tunnel.
7. Configure the **Basic** TINA tunnel settings. For more information, see TINA Tunnel Settings.
   - **Transport** – Select the transport encapsulation: **UDP** (recommended), **TCP**, **TCP&UDP**, **ESP**, or **Routing**.
   - **Encryption** – Select the encryption algorithm: **AES**, **AES256**, **3DES**, **CAST**, **Blowfish**, **DES**, or **Null**.
   - **Authentication** – Select the hashing algorithm: **MD5**, **SHA**, **SHA256**, **SHA512**, **NOHASH**, **RIPEMD160**, or **GCM**.
   - **(optional) TI Classification / TI-ID** – For more information, see Traffic Intelligence.
   - **(optional) Compression** – Select **yes** to enable VPN compression. Do not use in combination with WAN Optimization.
   - **(optional) Use Dynamic Mesh / Dynamic Mesh Timeout** – For more information,

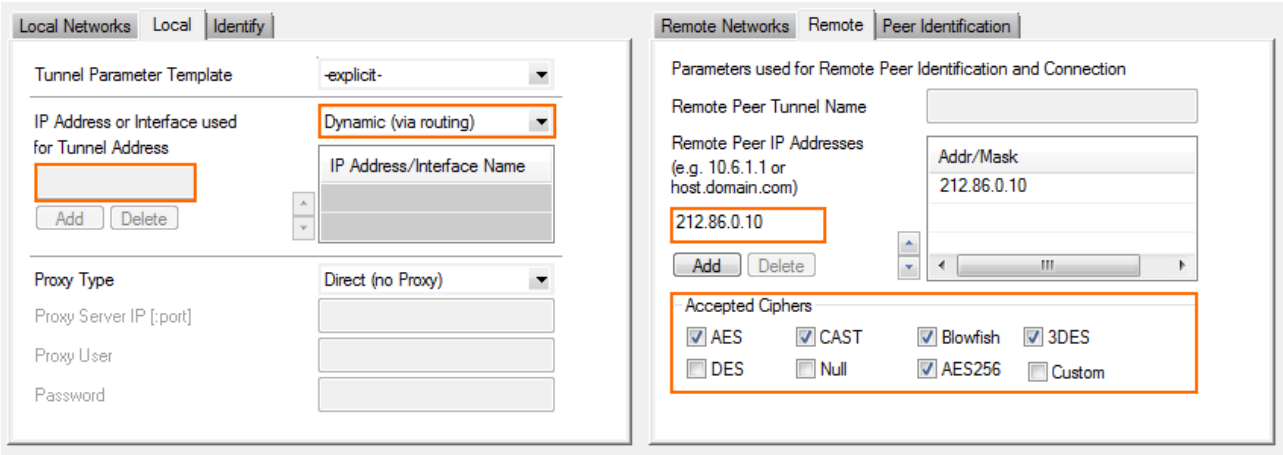


8. In the **Local Networks** tab, select the **Call Direction**. One or both firewalls must be active.

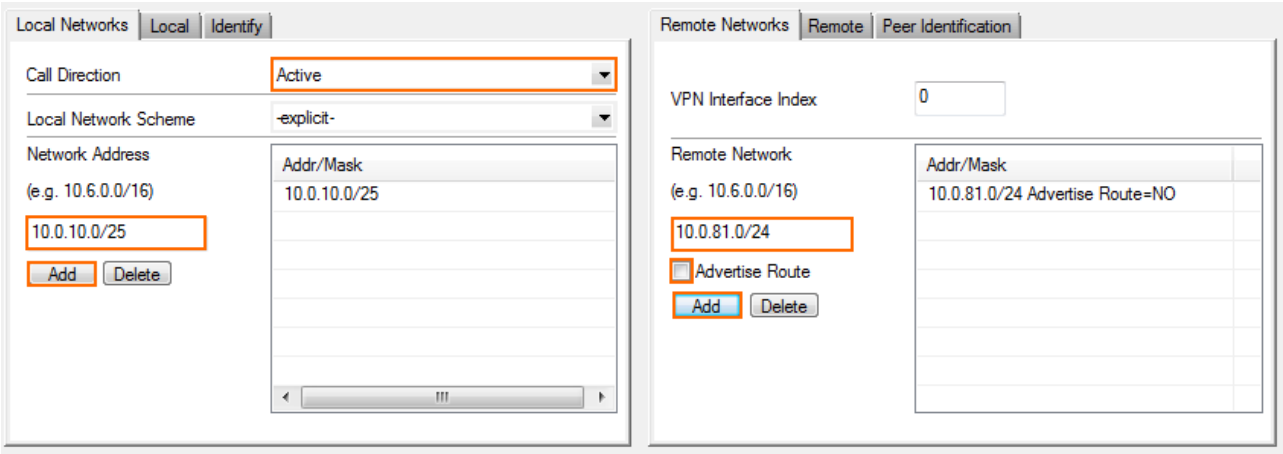
   Configure the NextGen Firewall F-Series with a dynamic IP address to be the active peer. If both firewalls use dynamic IP addresses, a DynDNS service must be used. For more information, see How to Configure VPN Access via a Dynamic WAN IP Address.



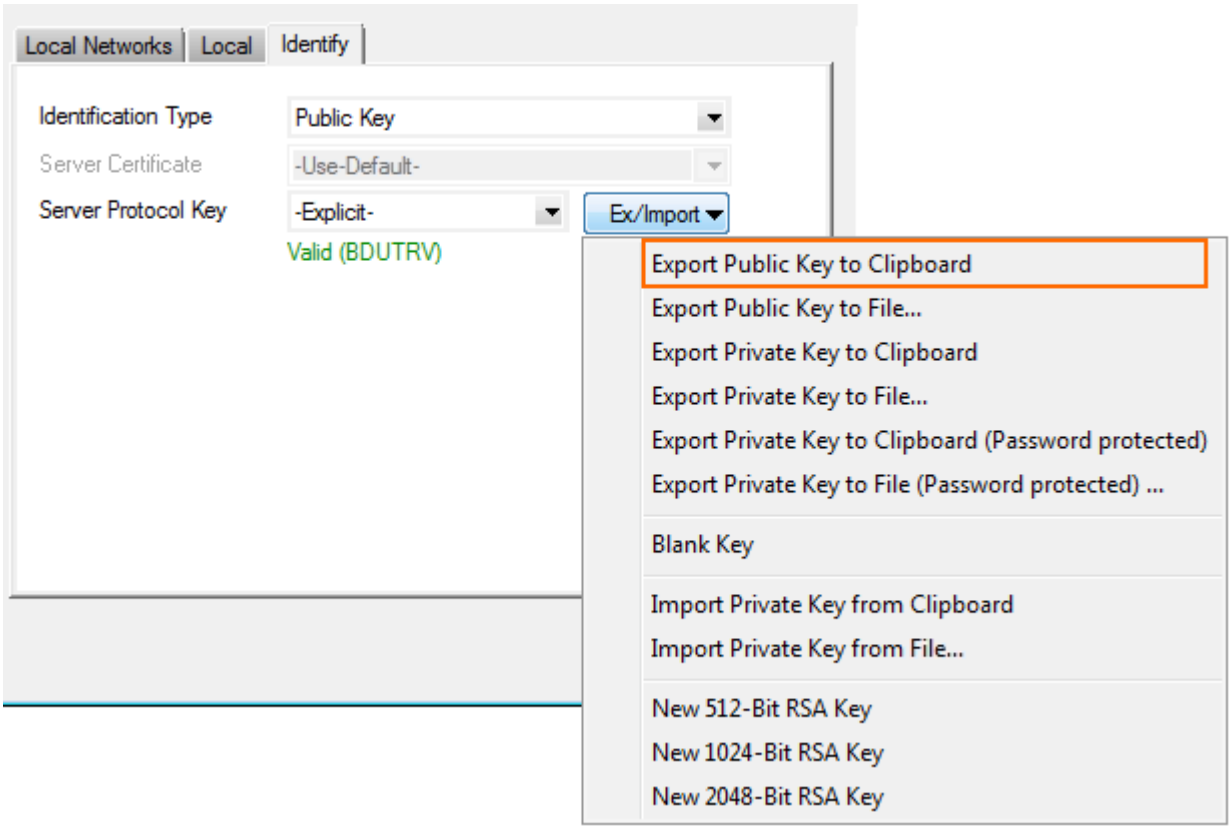
9. Click the **Local** tab, and configure the **IP address or Interface used for Tunnel Address**:
   - **First Server IP** – First IP address of the virtual server the VPN service is running on.
   - **Second Server IP** – Second IP address of the virtual server the VPN service is running on.
   - **Dynamic (via routing)** – The Barracuda NextGen Firewall F-Series uses a routing table lookup to determine which IP address to use.
   - **Explicit List (ordered)** – Enter one or more explicit IP addresses. Multiple IP addresses are tried in the listed order.
10. Click the **Remote** tab, enter one or more IP addresses or a FQDN as the **Remote Peer IP Addresses,** and click **Add**.



11. In the **Remote** tab, select the **Accepted Ciphers**. To use a cipher, the list must match the **Encryption** settings previously configured.
12. For each local network, enter the **Network Address** in the **Local Networks** tab and click **Add**. E.g., 10.0.10.0/25
13. For each remote network enter the **Network Address** in the **Remote Networks** tab and click **Add**. E.g., 10.0.81.0/24
14. (optional) To propagate the remote VPN network via dynamic routing enable **Advertise Route**.



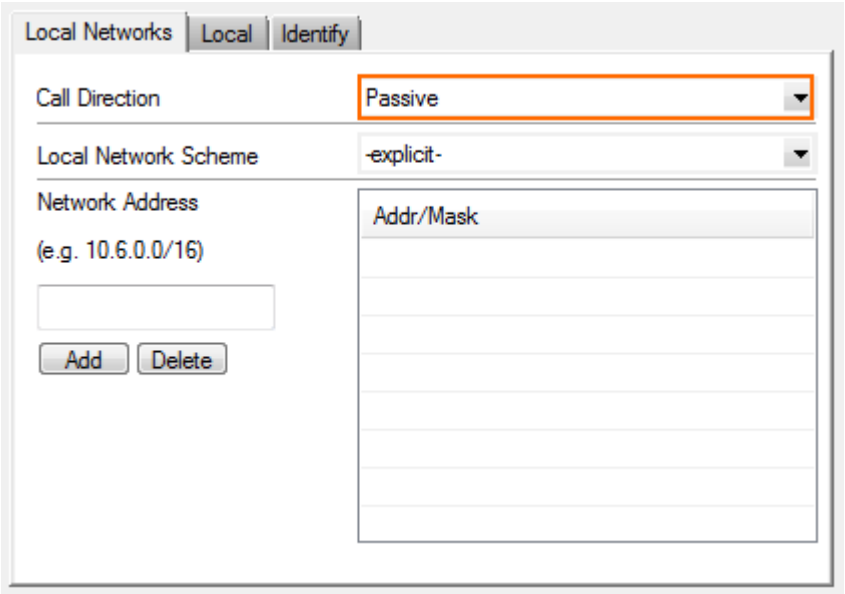
15. Click on the **Identity** tab.
16. From the **Identification Type** list, select **Public Key**.
17. Click **Ex/Import** and select **Export Public Key to Clipboard**.



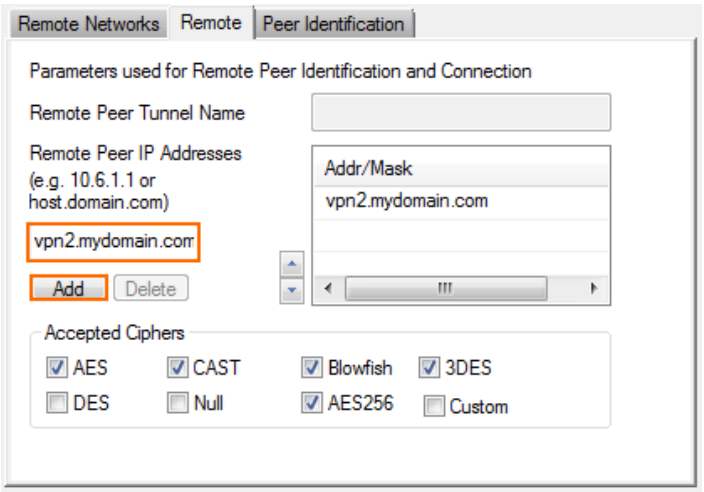
18. Click **OK**.
19. Click **Send Changes** and **Activate**.

Step 2. Create the TINA Tunnel at Location 2

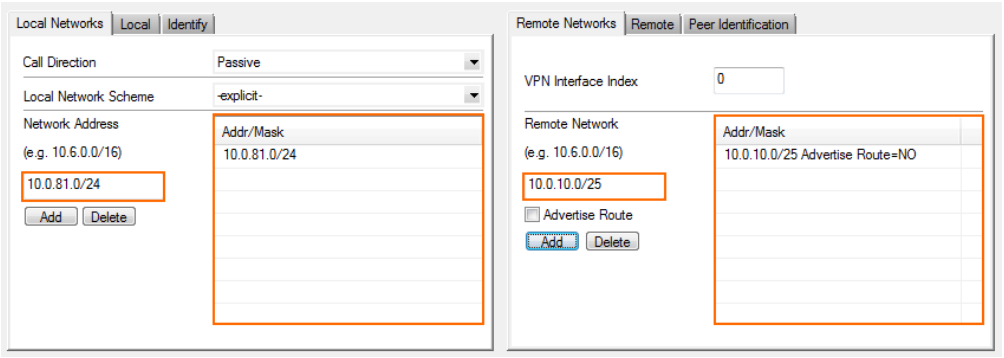
1. Log into the Firewall at Location 2.
2. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN > Site to Site** .
3. Click **Lock**.
4. Click the **TINA Tunnels** tab.
5. Right-click the table, and select **New TINA tunnel**.
6. In the **Name** field, enter the name for the new VPN tunnel.
7. Configure the **Basic** TINA tunnel settings to match the settings configured for the Location1
8. In the **Local Networks** tab, select the **Call Direction**. Make sure that one or both firewalls are set to **active**.



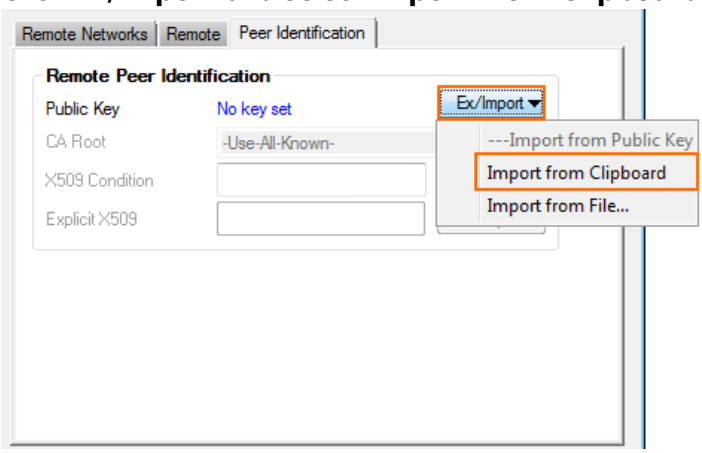
9. Click the **Local** tab, and configure the **IP address or Interface used for Tunnel Address**:
    1. **First Server IP** – First IP address of the virtual server the VPN service is running on.
    2. **Second Server IP** – Second IP address of the virtual server the VPN service is running on.
    3. **Dynamic (via routing)** – The Barracuda NextGen Firewall F-Series uses a routing table lookup to determine which IP address to use.
    4. **Explicit List (ordered)** – Enter one or more explicit IP addresses. Multiple IP addresses are tried in the listed order.
10. Click the **Remote** tab, enter one or more IP addresses or a FQDN as the **Remote Peer IP Addresses,** and click **Add**.



11. In the **Remote** tab, select the **Accepted Ciphers**. To use a cipher, the list must match the **Encryption** settings previously configured.
12. For each local network, enter the **Network Address** in the **Local Networks** tab and click **Add**. E.g., 10.0.81.0/24 behind Location 2 NextGen Firewall F-Series.
13. For each remote network, enter the **Network Address** in the **Remote Networks** tab and click **Add**. E.g., 10.0.10.0/25 behind Location1 NextGen Firewall F-Series.



14. Click on the **Peer Identification** tab.
15. Click **Ex/Import** and select **Import from Clipboard**.

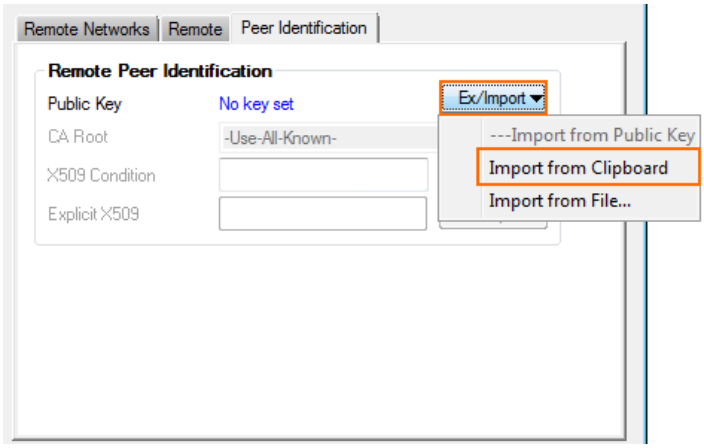


16. Click on the **Identity** tab.
17. From the **Identification Type** list, select **Public Key**.
18. Click **Ex/Import** and select **Export Public Key to Clipboard**.
19. Click **OK**.
20. Click **Send Changes** and **Activate**.

Step 3. Import the Public Key for Location 1

The TINA VPN tunnel is not activated until the public key of Location 2 is imported to Location 1.

1. Log into the Firewall at Location 1.
2. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > Site to Site** .
3. Click **Lock**.
4. Open the configuration for the Site-to-Site tunnel created in Step 1.
5. Click the **Peer Identification** tab.
6. Click **Ex/Import** and select **Import from Clipboard**.



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

After configuring the TINA VPN tunnel on both F-Series Firewalls, you must also create an access rule on both systems to allow access to the remote networks through the VPN tunnel.

Next Step

Create access rules to allow traffic in and out of your VPN tunnel: How to Create Access Rules for Site-to-Site VPN Access.

Figures

1. tina_tunnel.png
2. TINA_01.png
3. TINA_02.png
4. TINA_03.png
5. TINA_04.png
6. TINA_05.png
7. TINA_06.png
8. TINA_07.png
9. TINA_08.png
10. TINA_09.png
11. TINA_09.png