

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:

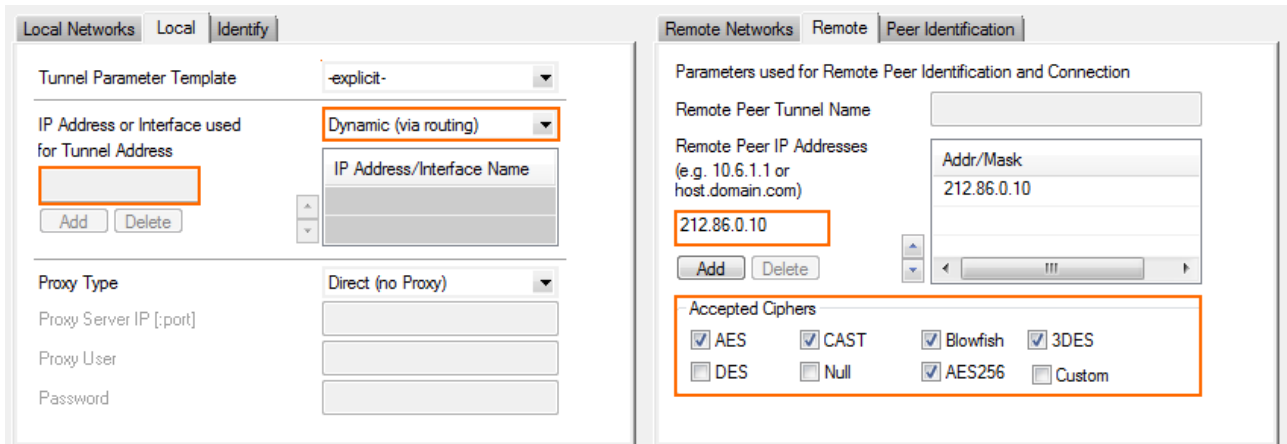
	Example Values for the Local Firewall	Example Values for the Remote Firewall
VPN Local Networks	10.0.10.0/25	10.0.81.0/24
VPN Remote Networks	10.0.81.0/24	10.0.10.0/25
External IP Address (Listener VPN Service)	62.99.0.40	212.86.0.10

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

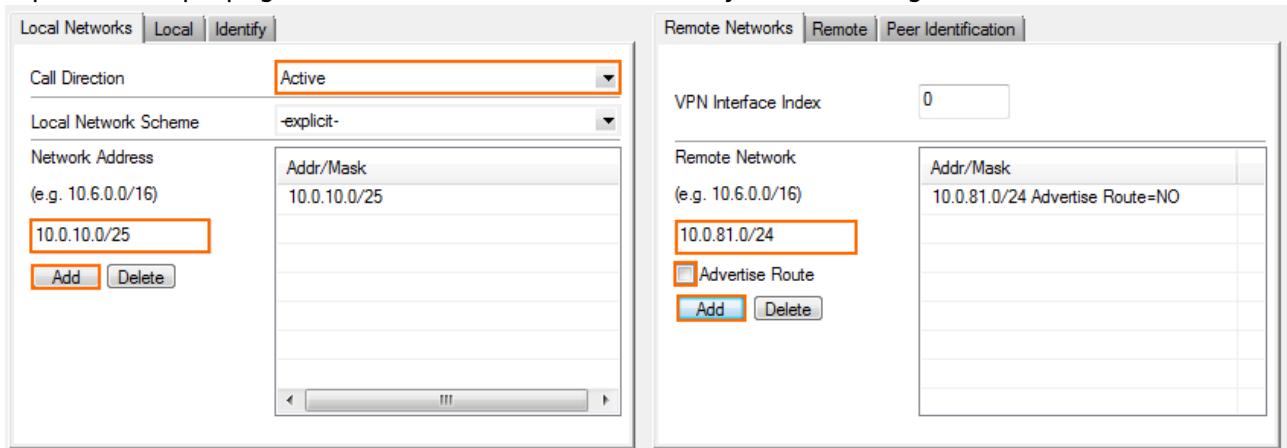
For the F-Series Firewall at Location 1, configure the network settings and export the public key. For more information on specific settings, see [TINA Tunnel Settings](#)

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**.



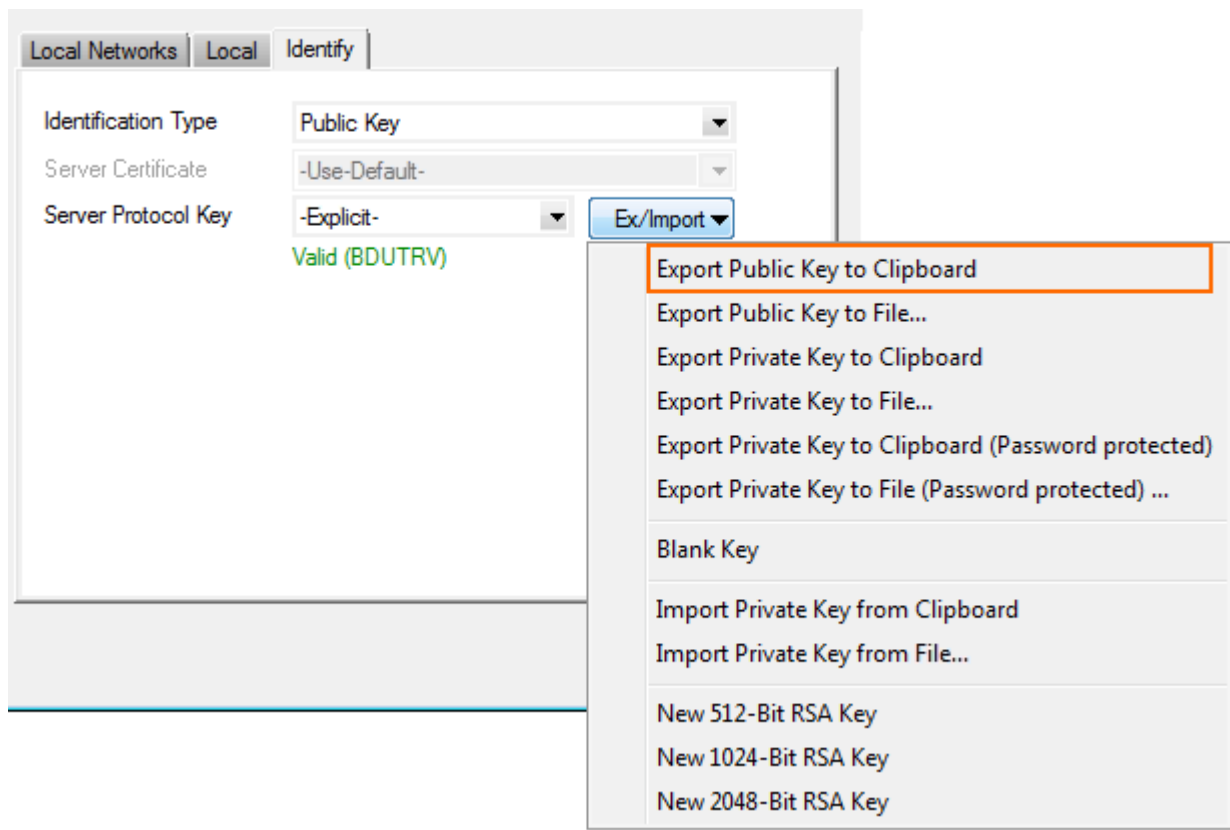
The screenshot shows two panels from the Barracuda CloudGen Firewall configuration interface. The left panel is titled 'Local Networks' and has tabs for 'Local' and 'Identify'. It contains a 'Tunnel Parameter Template' dropdown set to '-explicit-', an 'IP Address or Interface used for Tunnel Address' dropdown set to 'Dynamic (via routing)', and a table for adding local networks with columns for 'IP Address/Interface Name'. Below this are fields for 'Proxy Type' (set to 'Direct (no Proxy)'), 'Proxy Server IP [port]', 'Proxy User', and 'Password'. The right panel is titled 'Remote Networks' and has tabs for 'Remote' and 'Peer Identification'. It contains a 'Remote Peer Tunnel Name' field, a 'Remote Peer IP Addresses' table with columns for 'Addr/Mask' and 'Host', and an 'Accepted Ciphers' section with checkboxes for AES, CAST, Blowfish, 3DES, DES, Null, AES256, and Custom.

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**.



The screenshot shows the same configuration interface as above, but with specific values entered. In the 'Local Networks' panel, the 'Call Direction' dropdown is set to 'Active', and the 'Network Address' table contains one entry: '10.0.10.0/25'. In the 'Remote Networks' panel, the 'VPN Interface Index' is set to '0', and the 'Remote Network' table contains one entry: '10.0.81.0/24'. The 'Advertise Route' checkbox is checked.

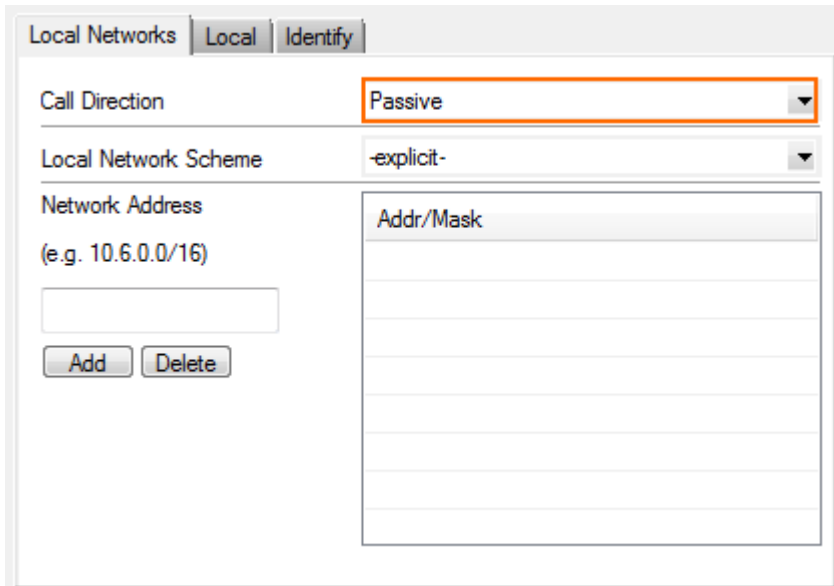
15. Click on the **Identity** tab.
16. From the **Identification Type** list, select **Public Key**.
17. Click **Ex/Import** and select **Export Public Key to Clipboard**.



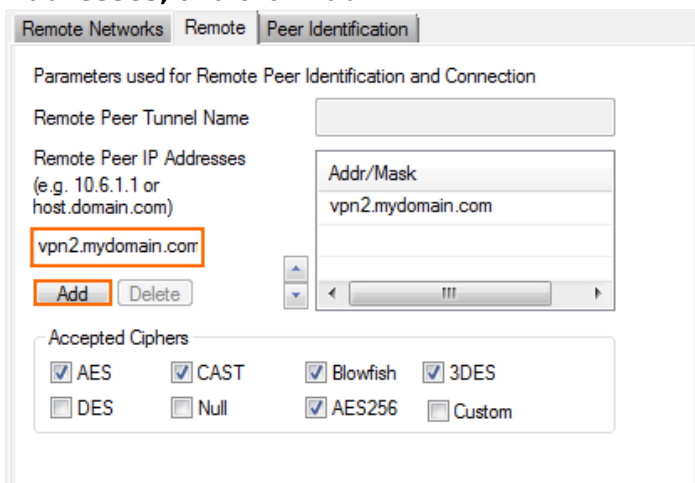
18. Click **OK**.
19. Click **Send Changes** and **Activate**.

Step 2. Create the TINA Tunnel at Location 2

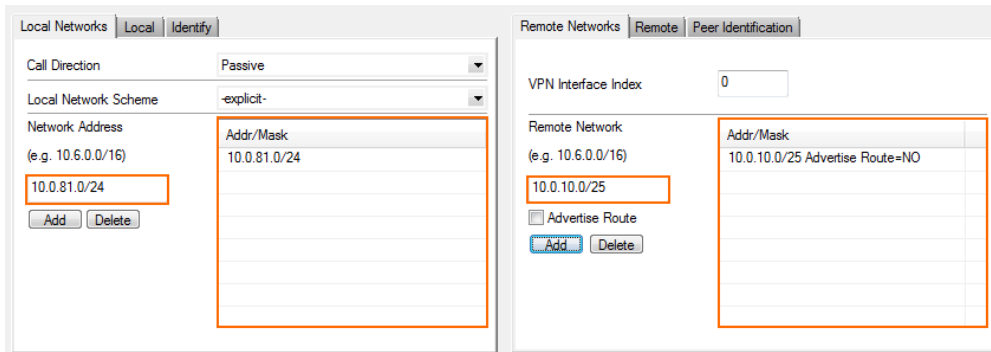
1. Log into the Firewall at Location 2.
2. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > VPN > Site to Site**.
3. Click **Lock**.
4. Click the **TINA Tunnels** tab.
5. Right-click the table, and select **New TINA tunnel**.
6. In the **Name** 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**.

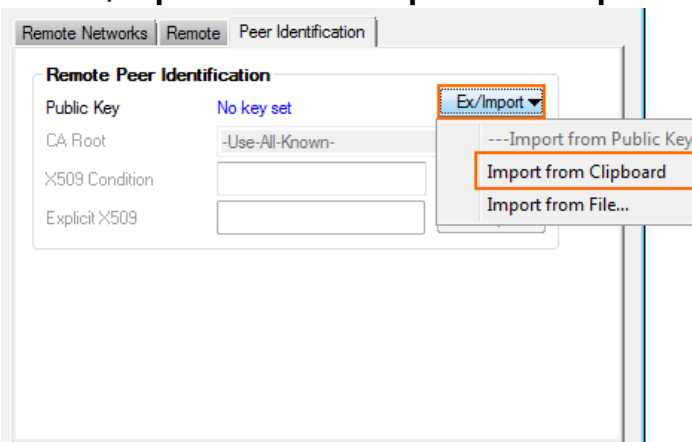


11. In the **Remote** tab, select the **Accepted Ciphers**. To use a cipher, the list must match the **Encryption** settings previously configured.
12. For each local network, enter the **Network Address** in the **Local Networks** tab and click **Add**. E.g., 10.0.81.0/24 behind Location 2 NextGen Firewall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



The screenshot shows two configuration panels side-by-side. The left panel is titled 'Local Networks' and has sub-tabs 'Local' and 'Identify'. It contains fields for 'Call Direction' (Passive), 'Local Network Scheme' (-explicit-), and a table for 'Network Address'. The table has a header 'Addr/Mask' and one row with '10.0.81.0/24'. Below the table are 'Add' and 'Delete' buttons. The right panel is titled 'Remote Networks' and has sub-tabs 'Remote' and 'Peer Identification'. It contains a 'VPN Interface Index' field (0), a 'Remote Network' table with header 'Addr/Mask' and one row with '10.0.10.0/25 Advertise Route=NO'. Below the table are 'Add' and 'Delete' buttons.

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



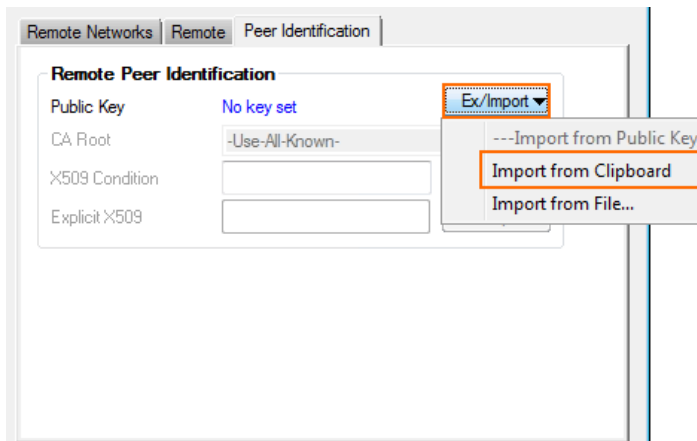
The screenshot shows the 'Remote Peer Identification' configuration window. It has a 'Public Key' field with the value 'No key set' and an 'Ex/Import' dropdown menu. A context menu is open over the dropdown, showing three options: '---Import from Public Key', 'Import from Clipboard', and 'Import from File...'. The 'Import from Clipboard' option is highlighted with an orange box.

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

© Barracuda Networks Inc., 2019 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.