

How to Create a TINA VPN Tunnel between CloudGen Firewalls

<https://campus.barracuda.com/doc/79462893/>

As the TINA protocol offers significant advantages over IPsec, it is the main protocol that is used for VPN connections between CloudGen Firewalls. Many of the advanced VPN features, such as SD-WAN or WAN Optimization, are only supported for TINA site-to-site tunnels.



You must complete this configuration on both the local and the remote Barracuda CloudGen Firewall by using the respective values below:

Setting	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](#).

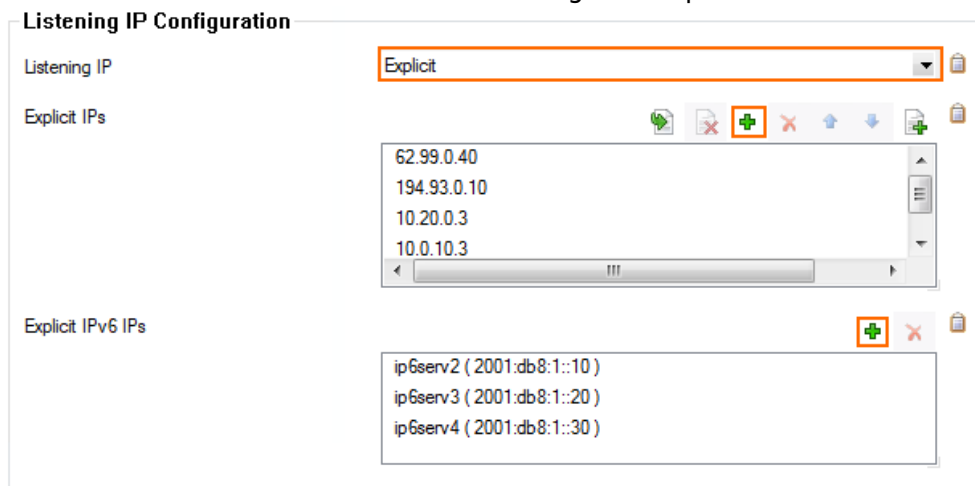
Before You Begin

If not already present, configure the **Default Server Certificate** in **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN > VPN Settings**. For more information, see [VPN Settings](#)

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 > Assigned Services > VPN > Service Properties**.
2. Click **Lock**.
3. From the **Listening IP** 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 IPs** list.
4. Click + to add an entry to the **Explicit IPv6 IPs**.
5. Select an IPv6 listener from the list of configured explicit IPv6 virtual server IP addresses.

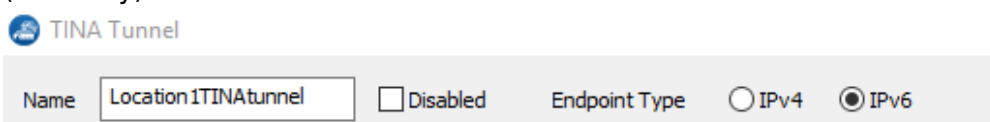


6. Click **Send Changes** and **Activate**.

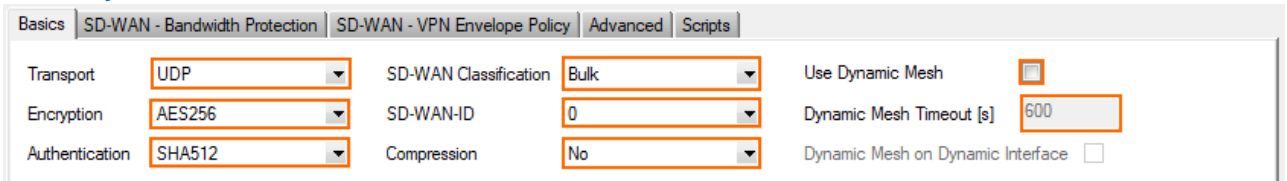
Step 2. Configure the TINA Tunnel at Location 1

For the 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 > 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. (IPv6 only). Select **IPv6**.

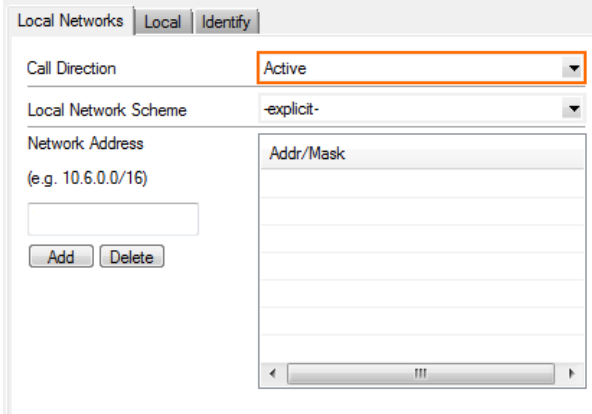


8. Configure the **Basic** TINA tunnel settings. For more information, see [TINA Tunnel Settings](#).
 - **Transport** – Select the transport encapsulation: **UDP** (recommended), **TCP**, **TCP&UDP**, **ESP**, or **Routing**.
 - **Encryption** – Select the encryption algorithm: **AES**, **AES256**, **3DES**, **CAST**, **Blowfish**, **DES**, or **Null**.
 - **Authentication** – Select the hashing algorithm: **MD5**, **SHA**, **SHA256**, **SHA512**, **NOHASH**, **RIPEMD160**, or **GCM**.
 - **(optional) SD-WAN Classification / SD-WAN-ID** – For more information, see [SD-WAN](#).
 - **(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, see [Dynamic Mesh VPN Networks](#).

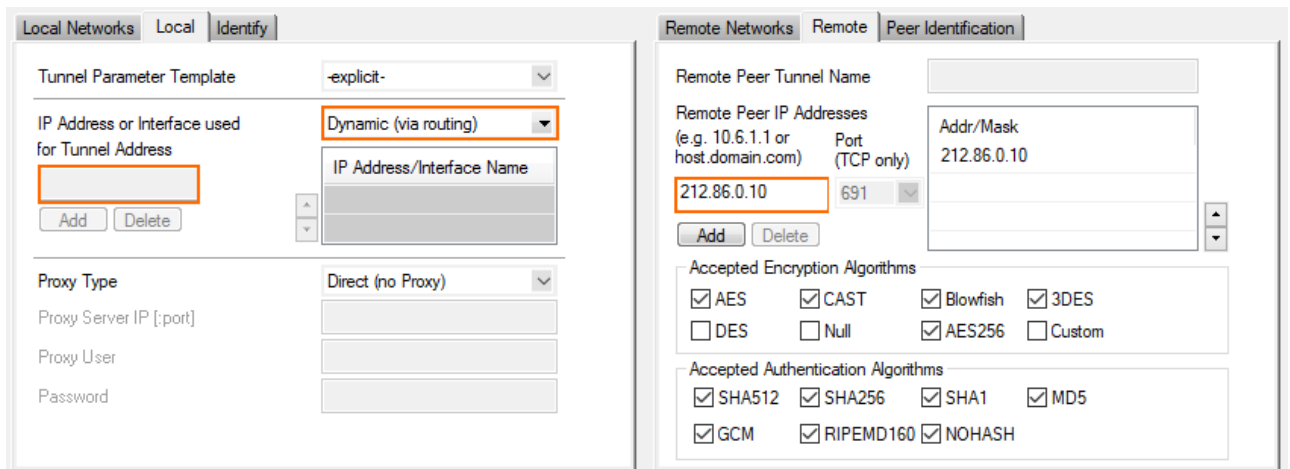


9. In the **Local Networks** tab, select the **Call Direction**. At least one of the firewalls must be active.

Configure the CloudGen Firewall 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](#).



10. Click the **Local** tab, and configure the **IP address or Interface used for Tunnel Address**:
 - **(IPv4 only) First Server IP** – First IP address of the virtual server the VPN service is running on.
 - **(IPv4 only) Second Server IP** – Second IP address of the virtual server the VPN service is running on.
 - **Dynamic (via routing)** – The firewall uses a routing table lookup to determine the IP address.
 - **Explicit List (ordered)** – Enter one or more explicit IP addresses. Multiple IP addresses are tried in the listed order.
 - In the **Remote** tab, enter one or more IPv4 or IPv6 addresses or an FQDN as the **Remote Peer IP Addresses**, and click **Add**.



Local Networks Local Identify

Tunnel Parameter Template: -explicit-

IP Address or Interface used for Tunnel Address: **Dynamic (via routing)**

IP Address/Interface Name

Proxy Type: Direct (no Proxy)

Proxy Server IP [:port]

Proxy User

Password

Remote Networks Remote Peer Identification

Remote Peer Tunnel Name

Remote Peer IP Addresses (e.g. 10.6.1.1 or host.domain.com): **212.86.0.10** Port (TCP only): 691

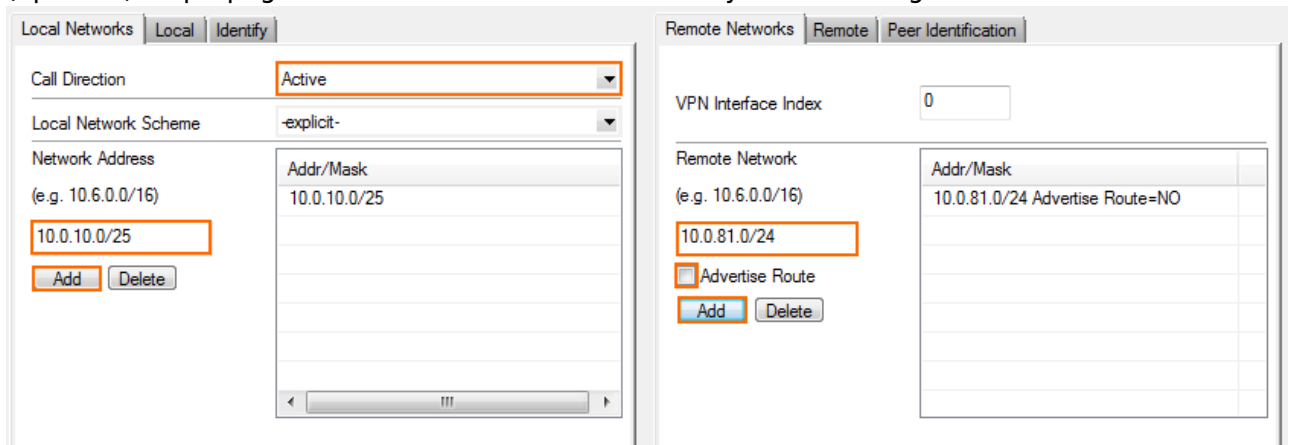
Accepted Encryption Algorithms:

- AES
- CAST
- Blowfish
- 3DES
- DES
- Null
- AES256
- Custom

Accepted Authentication Algorithms:

- SHA512
- SHA256
- SHA1
- MD5
- GCM
- RIPEMD160
- NOHASH

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



Local Networks Local Identify

Call Direction: **Active**

Local Network Scheme: -explicit-

Network Address (e.g. 10.6.0.0/16): **10.0.10.0/25**

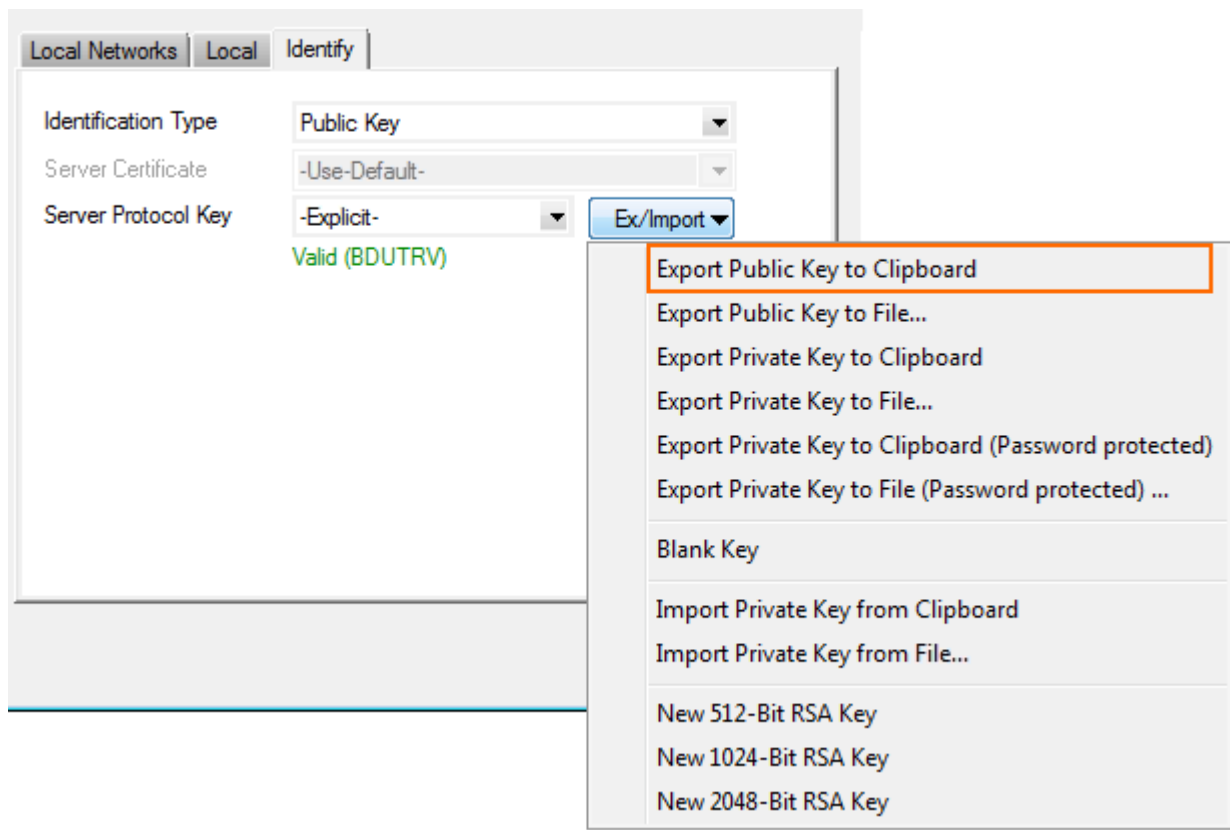
Remote Networks Remote Peer Identification

VPN Interface Index: 0

Remote Network (e.g. 10.6.0.0/16): **10.0.81.0/24**

Advertise Route

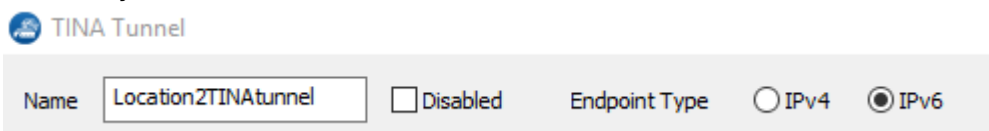
- Click on the **Identity** tab.
- From the **Identification Type** list, select **Public Key**.
- Click **Ex/Import** and select **Export Public Key to Clipboard**.



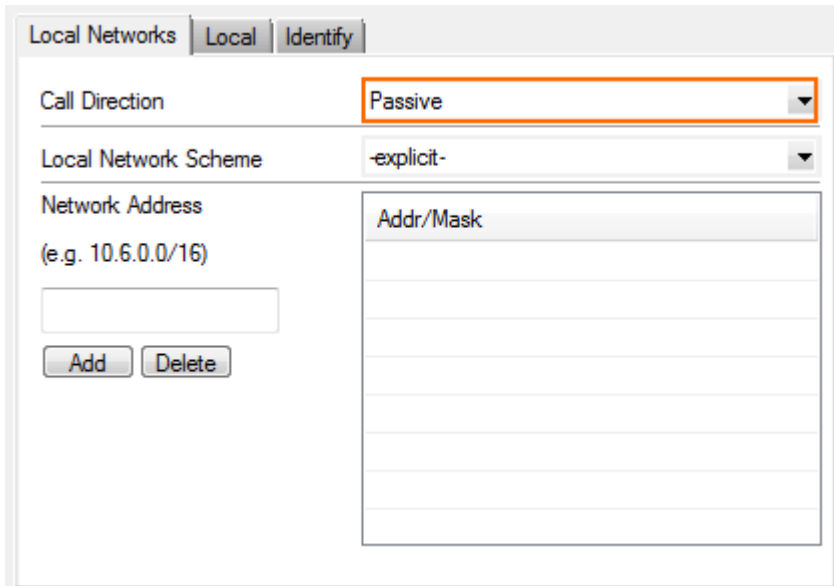
18. Click **OK**.
19. Click **Send Changes** and **Activate**.

Step 3. Create the TINA Tunnel at Location 2

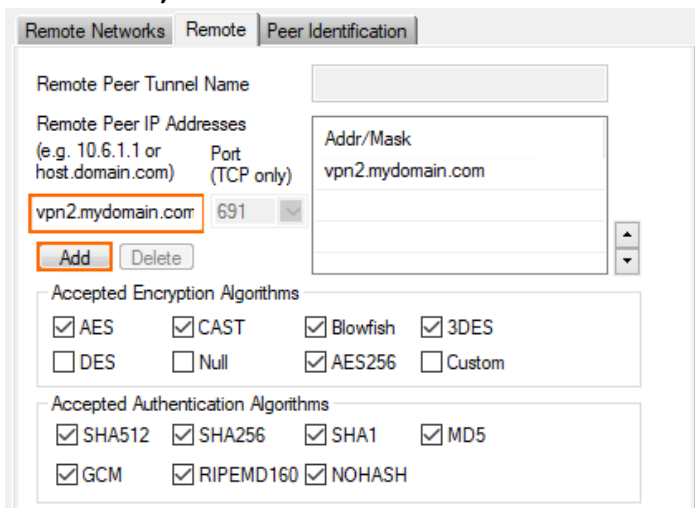
1. Log into the firewall at Location 2.
2. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN > Site to Site**.
3. Click **Lock**.
4. Click the **TINA Tunnels** tab.
5. Right-click the table, and select **New TINA tunnel**.
6. In the **Name** field, enter the name for the new VPN tunnel.
7. (IPv6 only) Click the **IPv6** check box.



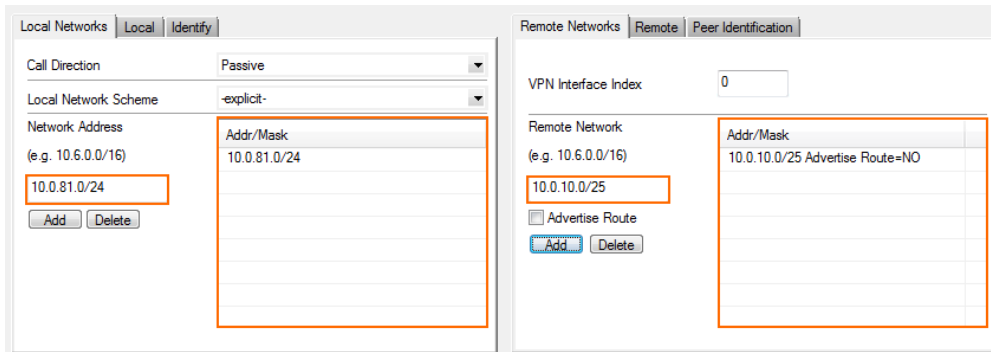
8. Configure the **Basic** TINA tunnel settings to match the settings configured for the Location 1
9. In the **Local Networks** tab, select the **Call Direction**. Make sure that one or both firewalls are set to **active**.



10. Click the **Local** tab, and configure the **IP address or Interface used for Tunnel Address**:
 - **(IPv4 only) First Server IP** – First IP address of the virtual server the VPN service is running on.
 - **(IPv4 only) Second Server IP** – Second IP address of the virtual server the VPN service is running on.
 - **Dynamic (via routing)** – The firewall uses a routing table lookup to determine the IP address.
 - **Explicit List (ordered)** – Enter one or more explicit IP addresses. Multiple IP addresses are tried in the listed order.
11. Click the **Remote** tab, enter one or more IP addresses or a FQDN as the **Remote Peer IP Addresses**, and click **Add**.

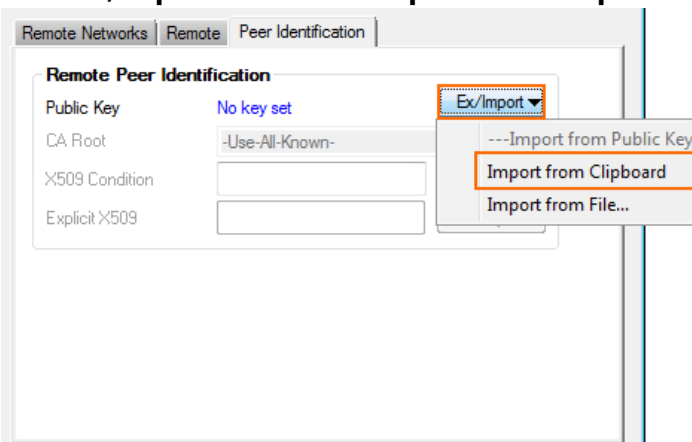


12. In the **Remote** tab, select the **Accepted Algorithms**. To use a cipher, the list must match the **Encryption** settings previously configured.
13. For each local network, enter the **Network Address** in the **Local Networks** tab and click **Add**. E.g., 10.0.81.0/24 behind Location 2 CloudGen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



The screenshot shows two configuration panels side-by-side. The left panel is titled 'Local Networks' and has sub-tabs 'Local' and 'Identify'. It features a 'Call Direction' dropdown set to 'Passive' and a 'Local Network Scheme' dropdown set to '-explicit-'. Below is a table for 'Network Address' with a header 'Addr/Mask' and one row containing '10.0.81.0/24'. The right panel is titled 'Remote Networks' and has sub-tabs 'Remote' and 'Peer Identification'. It features a 'VPN Interface Index' input field set to '0' and a table for 'Remote Network' with a header 'Addr/Mask' and one row containing '10.0.10.0/25 Advertise Route=NO'. Both tables have 'Add' and 'Delete' buttons below them.

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



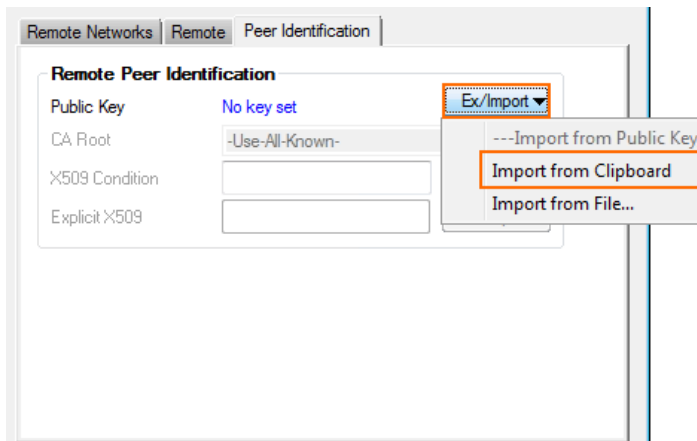
The screenshot shows the 'Remote Peer Identification' configuration window. It has a 'Public Key' field set to 'No key set' and a 'CA Root' dropdown set to '-Use-All-Known-'. There are also fields for 'X509 Condition' and 'Explicit X509'. An 'Ex/Import' dropdown menu is open, showing three options: '---Import from Public Key', 'Import from Clipboard', and 'Import from File...'. The 'Import from Clipboard' option is highlighted with an orange box.

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

Step 4. Import the Public Key for Location 1

The 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 > 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 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. vpn_service_listeners.png
3. TINA_00.png
4. TINA_01.png
5. TINA_02.png
6. TINA_03.png
7. TINA_04.png
8. TINA_05.png
9. TINA_05a.png
10. TINA_06.png
11. TINA_07.png
12. TINA_08.png
13. TINA_09.png
14. 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.