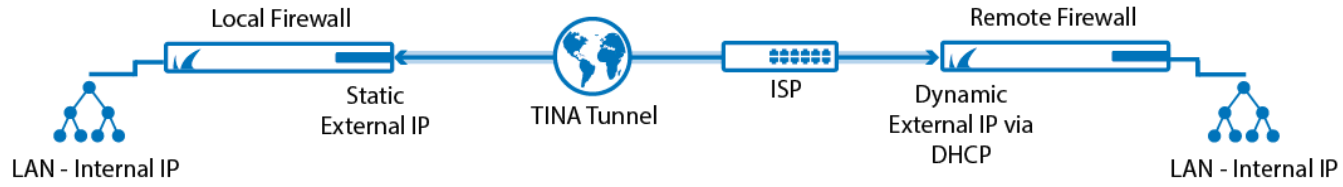
# How to Configure a TINA Site-to-Site VPN Tunnel When One Side is Using a Dynamic IP

In this example setup, two NextGen Firewalls are connected via a TINA site-to-site VPN tunnel over the Internet. The firewall on the local site is using a WAN connection with a static public IP address. The remote firewall uses a dynamic WAN connection. Since the dynamic IP address of the remote firewall is volatile and can change the remote firewall must be configured as the active VPN endpoint of the VPN tunnel.



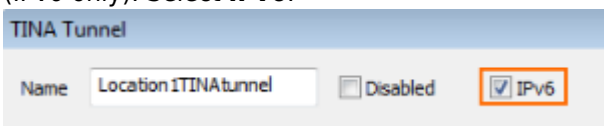

The following table refers to the image and serves as an example. You must adjust the settings to your specific network and host IP values.

| | Local Firewall | Remote Firewall |
|---|---|---|
| **External IP address** | 62.99.0.21/32 (static) | Dynamic via DHCP |
| **Local Networks** | 10.0.10.0/25 | 10.0.80.0/24 |
| **Remote Networks** | 10.0.80.0/24 | 10.0.10.0./25 |
| **State of Tunnel Server** | Passive | Active |

**Step 1. Configure the TINA Site-to-Site VPN Tunnel on the Local Firewall**

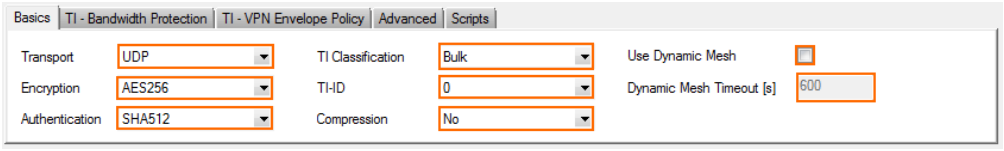
Traffic coming from the internal network 10.0.80.0/24 behind the remote firewall is forwarded through the TINA site-to-site VPN tunnel to the internal network 10.0.10.0/25 behind the local firewall. Since the public IP address of the remote firewall is dynamic, the **Call Direction** of the local firewall must be set to **Passive**.

1. Log into the local firewall.
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. (IPv6 only). Select **IPv6**.

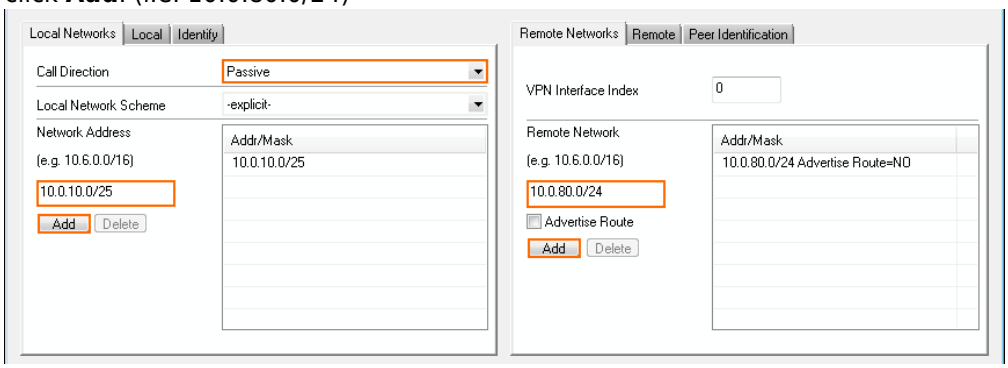



8. Configure the **Basic** TINA tunnel settings. For more information, see TINA Tunnel Settings.
   - **Transport** – Select the transport encapsulation: **UDP** (recommended), **TCP**, **TCP&UDP**, **ESP**, or **Routing**.
   - **Encryption** – Select the encryption algorithm: **AES**, **AES256**, **3DES**,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

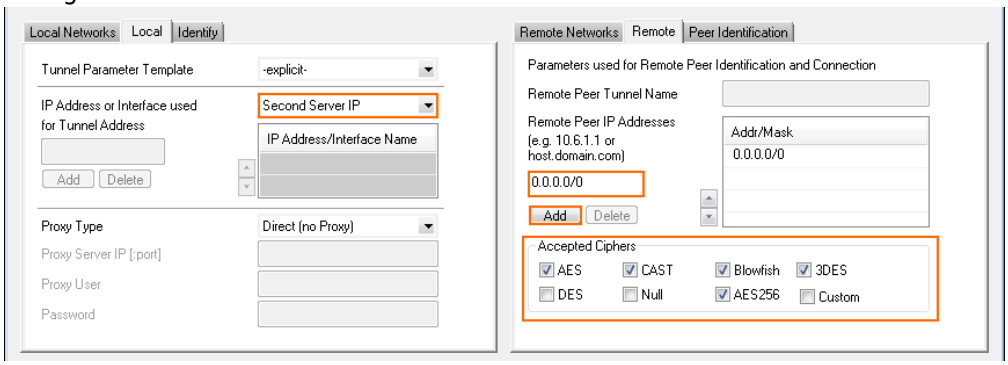
**(optional) Use Dynamic Mesh / Dynamic Mesh Timeout** – For more information, see Dynamic Mesh VPN Networks.



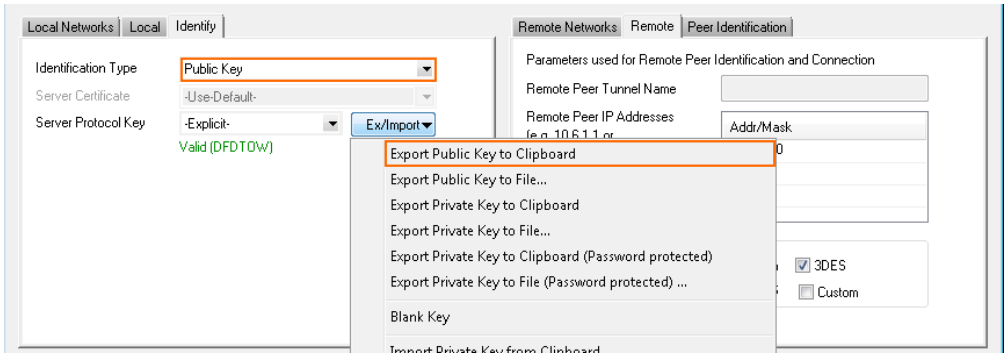

9. Configure the **Local Networks** tab:
   - **Call Direction** – Set to **Passive** so that the local firewall listens for incoming VPN tunnel requests.
   - **Networks Address** – Enter the **Network Address(es)** of your local network(s) in CIDR-notation and click **Add**. (i.e. 10.0.10.0./25)
10. Configure the **Remote Networks** tab:
    - **Remote Network** – Enter the local network address(es) of the remote peer in CIDR-notation and click **Add**. (i.e. 10.0.80.0/24)




11. 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
    - **Explicit** – For each IP address, click **+** and enter the IPv4 addresses in the **Explicit Service IPs** list.
12. Configure the **Remote** tab:
    - **Remote Peer IP Addresses** – Enter 0.0.0.0/0 for tunnel requests coming from the second firewall via the Internet and click **Add**.
    - **Accepted Ciphers** – To use a cipher, the list must match the **Encryption** settings previously configured.




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

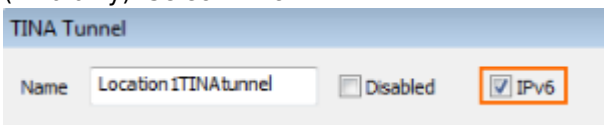



16. Click **OK**.
17. Click **Send Changes** and **Activate**.

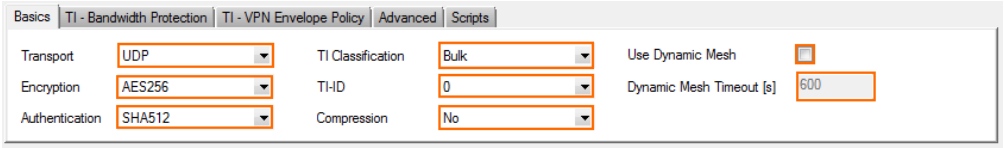
### Step 2. Configure the TINA Site-to-Site VPN Tunnel on the Remote NextGen Firewall

Since the local firewall's tunnel is working in passive mode, only the remote firewall can initiate a tunnel connection. Therefore, the **Call Direction** must be set to **Active**.

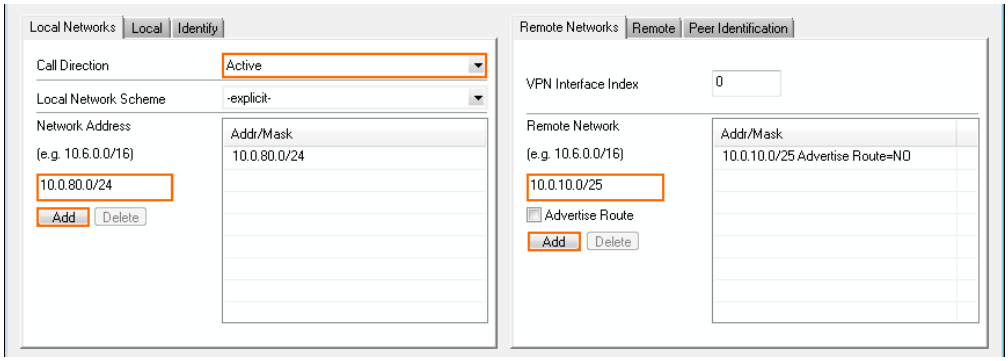
1. Log into the remote firewall.
2. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN > Site to Site**.
3. Click **Lock**.
4. Click the **TINA Tunnels** tab.
5. Right-click the table, and select **New TINA tunnel**.
6. In the **Name**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



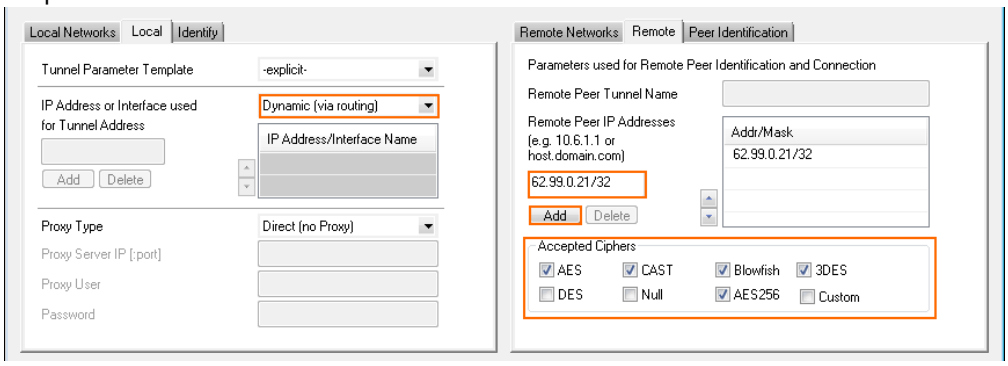

8. Configure the **Basic** TINA tunnel settings. For more information, see TINA Tunnel Settings.
   - **Transport** – Select the transport encapsulation: **UDP** (recommended), **TCP**, **TCP&UDP**, **ESP**, or **Routing**.
   - **Encryption** – Select the encryption algorithm: **AES**, **AES256**, **3DES**,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



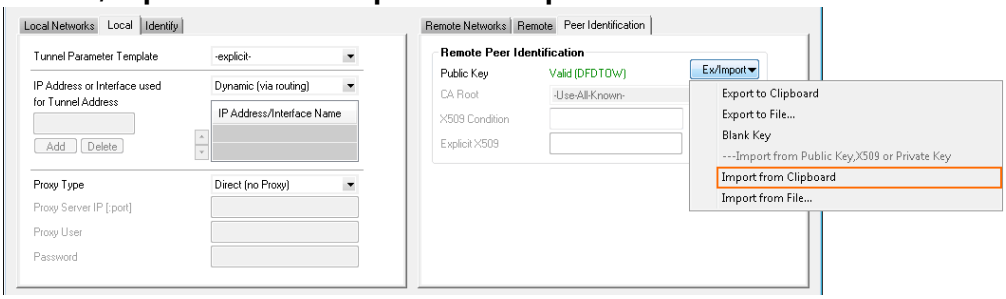

9. Configure the **Local Networks** tab:
   - **Call Direction** – Set to **Active** so that the firewall can initiate a VPN tunnel after being connected to the Internet via DHCP.
   - **Networks Address** – Enter the **Network Address(es)** of your local network(s) in CIDR-notation and click **Add**. (i.e. 10.0.80.0./24)
10. Configure the **Remote Networks** tab:
    - **Remote Network** – Enter the local network address(es) of the remote peer in CIDR-notation and click **Add**. (i.e. 10.0.10.0/25)



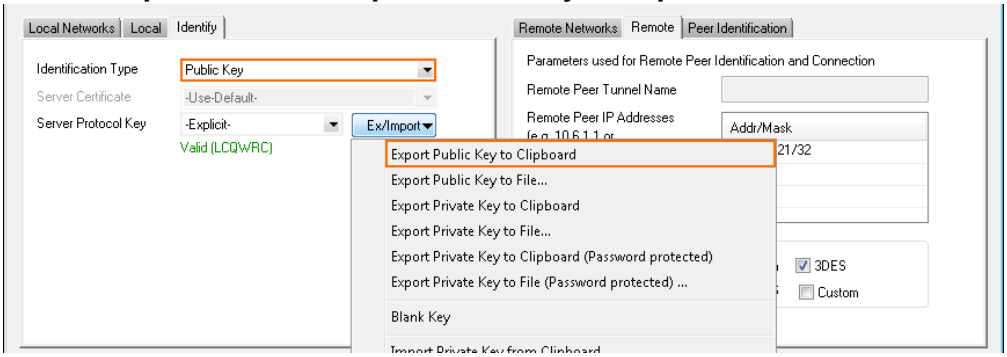

11. Click the **Local** tab, then configure :
    - **Tunnel Parameter Template** – Select **explicit**.
    - **IP address or Interface used for Tunnel Address** – The firewall must do a routing table lookup to determine the IP address.
12. Configure the **Remote** tab:
    - **Remote Peer IP Addresses** – Enter the point of entry of the first firewall, and click **Add**. (i.e., 62.99.0.21).
    - **Accepted Ciphers** – To use a cipher, the list must match the **Encryption** settings configured in Step 8.




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




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

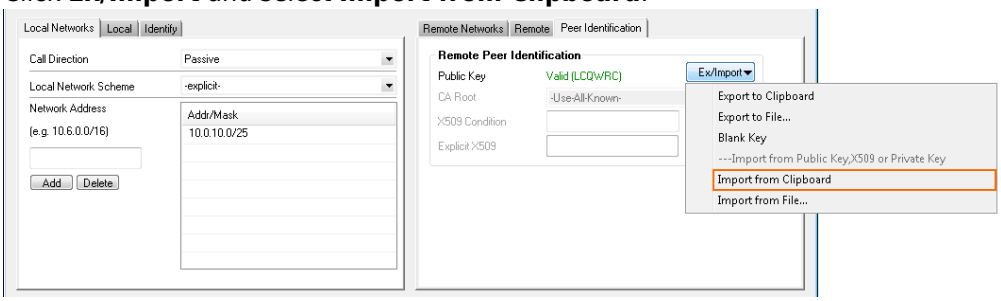



18. Click **OK**.

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

### Step 3. On the Local Firewall, Import the Public Key from the Remote Firewall

1. Log into the local firewall.
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 TINA site-to-site tunnel created on the first firewall.
5. Click the **Peer Identification** tab.
6. Click **Ex/Import** and select **Import from Clipboard**.

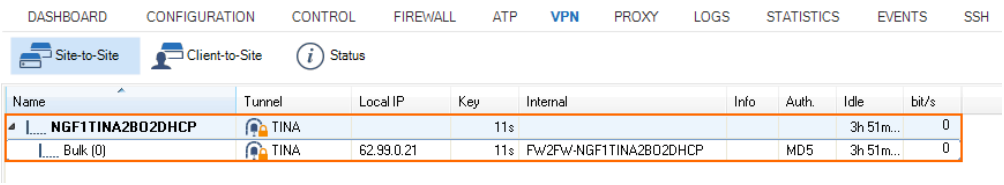


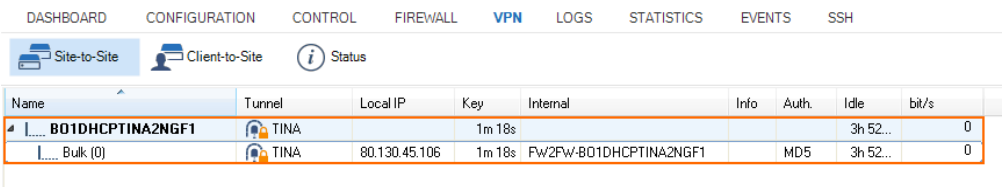

7. Click **OK**.
8. Click **Send Changes** and **Activate**.

### Access Rules

You must create Pass access rules on both systems to allow traffic between the two peers. For more information, see How to Create Access Rules for Site-to-Site VPN Access.

Verify that the TINA site-to-site tunnel is established on both firewalls:



## Figures