

How to Create a TINA VPN Tunnel between CloudGen Firewalls

https://campus.barracuda.com/doc/72516534/

The TINA protocol offers significant advantages over IPsec and is, therefore, the preferred protocol for VPN connections between CloudGen Firewalls. Many of the advanced VPN features, such as Traffic Intelligence or WAN Optimization, are supported only for TINA site-to-site tunnels.



You must complete this configuration on both the local and the remote firewall 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.

Before You Begin

Connecting two sites via the Internet using a VPN TINA tunnel requires a configured public network interface. For more information about WAN connections, see How to Configure an ISP with Dynamic IP Addresses (DHCP).

Step 1. Enable a VPN Listener on a Public Network IP

The following steps must be done on both the local and the remote firewall.

- 1. Log into the local/remote firewall.
- 2. Go to **NETWORK > IP Configuration**.



- 3. In the **Static Interface Configuration** section, click **Edit** to modify the entry that contains the configuration of your public network interface.
- 4. The Edit Static Network Interface window opens.
- For Services to Allow, select the VPN server check box to enable a listener for your VPN service.
- 6. Click Save.

Services to Allow:

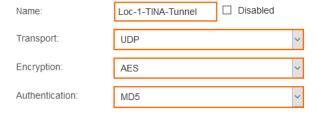
Ping VPN Server SSL VPN

Enable/Disable 'reply to ping' or NTP requests. To be able to enable SSLVPN, you need to select a certificate under VPN > SSLVPN > Server Settings.

Step 2. Configure the TINA Tunnel on the Local Firewall

For the local firewall, configure the network settings and export the public key.

- 1. Log into the local firewall.
- 2. Go to VPN > Site to Site VPN.
- 3. In the Site-to-Site TINA Tunnel section, click Add TINA Tunnel. The Add Site-to-Site TINA Tunnel window opens.
- 4. Configure the TINA Tunnel settings:
 - Name Enter the name for the new VPN tunnel.
 - 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.

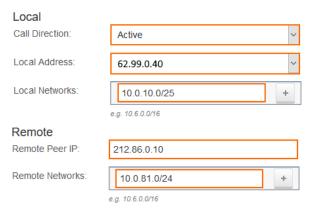


• Call Direction - At least one of the firewalls must be active.

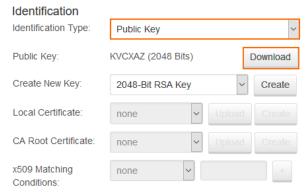
In case you use a dynamic IP address, configure the firewall to be the active peer. If both firewalls use dynamic IP addresses, a DynDNS service must be used. For more information, see How to Configure VPN Access via a Dynamic WAN IP Address.

- Local Address IP address used for the tunnel address.
- Local Networks For each local network, enter the Network Address in the Local Networks list and click +. E.g., 10.0.10.0/25
- Remote Peer IP Enter an IPv4 address as the Remote Peer IP, and click +.
- Remote Networks For each remote network, enter the Network Address in the Remote Networks list and click +. E.g., 10.0.81.0/24





- 5. Configure the security settings for the VPN tunnel on the local firewall:
 - From the Identification Type list, select Public Key.
 - Click **Download** to save the public key to a file on your system.



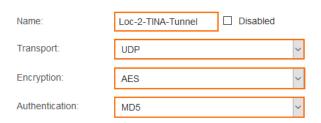
6. Click Save.

Step 3. Configure the TINA Tunnel for the Remote Firewall

For the remote firewall, configure the network settings and export the public key.

- 1. Log into the remote firewall.
- 2. Go to VPN > Site to Site VPN.
- 3. In the **Site-to-Site TINA Tunnel** section, click **Add TINA Tunnel**. The **Add Site-to-Site TINA Tunnel** window opens.
- 4. Configure the TINA Tunnel settings:
 - Name Enter the name for the new VPN tunnel.
 - 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.





• **Call Direction** – At least one of the firewalls must be active.

In case you use a dynamic IP address, configure the firewall to be the active peer. If both firewalls use dynamic IP addresses, a DynDNS service must be used. For more information, see <u>How to Configure VPN Access via a Dynamic WAN IP Address</u>.

- Local Address IP address used for the tunnel address.
- Local Networks For each local network, enter the Network Address in the Local Networks list and click +. E.g., 10.0.81.0/24
- Remote Peer IP Enter an IPv4 address as the Remote Peer IP, and click +.
- Remote Networks For each remote network, enter the Network Address in the Remote Networks list and click +. E.g., 10.0.10.0/25

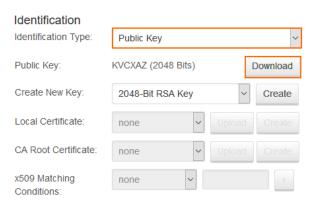


- 5. Import the public key from the local firewall:
 - Click **Browse** to select the file path for the public key from the local firewall.
 - Click **Upload** to save the public key.



- 6. Configure the security settings for the VPN tunnel on the remote firewall:
 - From the **Identification Type** list, select **Public Key**.
 - Click **Download** to save the public key to a file on your system.





7. Click Save.

Step 4. Import the Public Key on the Local Firewall Originating from the Remote Firewall

Upload the public key from the remote firewall on the local firewall:

- 1. Log into the local firewall.
- 2. Go to VPN > Site to Site VPN.
- 3. In the Site-to-Site TINA Tunnel section, click edit () in the table of the VPN tunnel.
- 4. Import the public key from the remote firewall:
 - Click Browse to select the file path for the public key from the remote firewall.
 - Click **Upload** to save the public key.



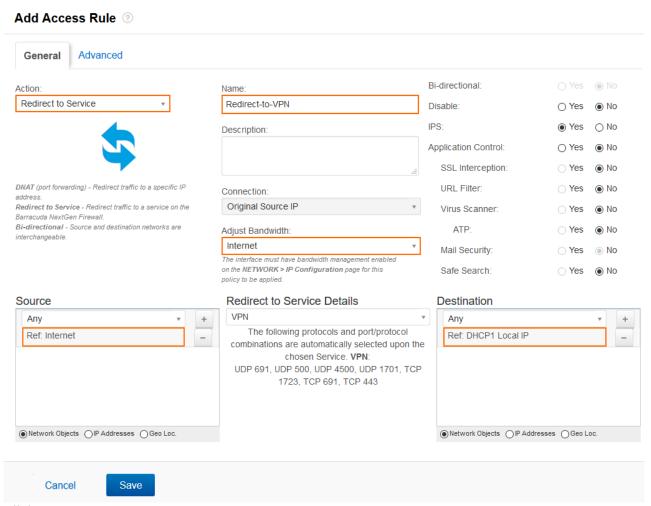
Step 5. Create an Access Rule to Redirect VPN Traffic to the VPN Server

The following steps must be done on both the local and the remote firewall.

Create a new access rule that redirects the VPN traffic to the VPN server to establish the tunnel:

- 1. Go to FIREWALL > Access Rules.
- 2. Click Add Access Rule. The Add Access Rule window opens.
- 3. In the Add Access Rule window, configure a Redirect to Service firewall rule that redirects incoming VPN connections on the dynamic interface to the VPN server listening on the local IP address. For the Destination, select the network object corresponding to your Internet connection type (DHCP, WWAN, or DSL).





- 4. Click Save.
- 5. Reorder the access rule by dragging it to the correct position in the Forwarding Firewall ruleset. Make sure no access rule placed above it will match the traffic for the site-to-site access rule.
- 6. Click Save.

The firewall can now route traffic from the private net 10.0.10.0/25 through the TINA VPN tunnel into the remote private net 10.0.81.0/24 and vice versa.

Barracuda CloudGen Firewall



Figures

- 1. tina tunnel.png
- 2. enable vpn service.png
- 3. conf_tina_tunnel_basic_loc_1.png
- 4. conf local loc1.png
- 5. conf_remote_loc1.png
- 6. download_public_key_from_loc1.png
- 7. conf tina tunnel basic loc 2.png
- 8. conf local loc2.png
- 9. conf_remote_loc2.png
- 10. upload remote public key.png
- 11. download_public_key_from_loc1.png
- 12. edit.png
- 13. upload_remote_public_key.png
- 14. dynamic-IP_VPN-access.png

[©] Barracuda Networks Inc., 2024 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.