

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

https://campus.barracuda.com/doc/96026165/

In this example setup, two CloudGen 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 > 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 <u>TINA Tunnel Settings</u>.
 - 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 <u>SD-WAN</u>.
 - **(optional) Compression** Select **yes** to enable VPN compression. Do not use in combination with WAN Optimization.
 - o (optional) Use Dynamic Mesh / Dynamic Mesh Timeout For more information, see Dynamic Mesh VPN Networks.

Basics SD-WAN	I - Bandwidth Protection	SD-	WAN - VPN Envelope Polic	y Advanced Script	s		
Transport	UDP	\sim	SD-WAN Classification	Bulk	\sim	Use Dynamic Mesh	
Encryption	AES256	\sim	SD-WAN-ID	0	\sim	Dynamic Mesh Timeout [s]	600
Authentication	SHA512	\sim	Compression	Disabled	\sim	Dynamic Mesh on Dynamic Interface	

- 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 CIDRnotation 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 CIDRnotation and click Add. (i.e. 10.0.80.0/24)

Call Direction	Passive	VDN laka fa an la dau	0
Local Network Scheme	-explicit-		0
Network Address	Addr/Mask	Remote Network	Addr/Mask
(e.g. 10.6.0.0/16)	10.0.10.0/25	(e.g. 10.6.0.0/16)	10.0.80.0/24 Advertise Route=N0
10.0.10.0/25		10.0.80.0/24	
Add Delete		Advertise Route	
		Add Delete	

- 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**.

Local Networks Local Identify	Remote Networks Remote Peer Identification
Local Networks Local Identity Tunnel Parameter Template explicit- IP Address or Interface used for Tunnel Address Second Server IP Add Delete Proxy Type Direct (no Proxy) Proxy User Proxy User Password Image: Content of the second server in the second	Remote Networks Remote Peer Identification Remote Peer Tunnel Name Remote Peer IP Addresses (e.g. 10.6.1.1 or Port host domain.com) Noted domain.com) (TCP only) 0.0.0.0/0 691 Add Delete Accepted Encryption Algorithms AES CAST DES Null Accepted Authentication Algorithms Q SHA512 SHA256 SHA1 MD5

- Accepted Algorithms To use a cipher, the list must match the Encryption settings previously configured.
- 13. Click the **Identify** tab.
- 14. From the **Identification Type** list, select **Public Key**.
- 15. Click Ex/Import and select Export Public Key to Clipboard.

Identification Type	Public Key	-	Parameters used for Remote Peer Remote Peer Tunnel Name	Identification and Connection
Server Certificate Server Protocol Key	-Use-Default- -Explicit-	▼ Ex/Import ▼	Remote Peer IP Addresses (e.g. 10.6.1.1.or	Addr/Mask
		Export Public Kr Export Public Kr Export Private K Export Private K Export Private K Export Private K	ey to Clipboard ey to File ey to Clipboard ey to File 'ey to Clipboard (Password protected) 'ey to File (Password protected)	o I I 3DES I ⊂ Custom

16. Click **OK**.

17. Click Send Changes and Activate.

Step 2. Configure the TINA Site-to-Site VPN Tunnel on the Remote CloudGen 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 > 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.

🔊 TIN	A Tunnel				
Name	Location 1TINAtunnel	Disabled	Endpoint Type	◯ IPv4	● IPv6

- 8. Configure the **Basic** TINA tunnel settings. For more information, see <u>TINA Tunnel Settings</u>.
 - 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.

Transport UDP SD-WAN Classification Bulk Use Dynamic Mesh Encryption AES256 SD-WAN-ID 0 Dynamic Mesh Timeout [s] 600 Authortication SLIA512 V Compression Disabled V Descript Machine Descript Mechine	Basics SD-WAN	- Bandwidth Protection	SD-W	/AN - VPN Envelope Polic	y Advanced Scripts			
Encryption AES256 SD-WAN-ID 0 Dynamic Mesh Timeout [s] 600	Transport	UDP	\sim	SD-WAN Classification	Bulk	\sim	Use Dynamic Mesh	
Authoritication SHA512 V Compression Displied V Description Hade an Description Interface	Encryption	AES256	\sim	SD-WAN-ID	0	\sim	Dynamic Mesh Timeout [s]	600
Autrenication ShAS12 v Compression Disabled v Dynamic Mesh on Dynamic Interace	Authentication	SHA512	\sim	Compression	Disabled	\sim	Dynamic Mesh on Dynamic Interface	

- 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 CIDRnotation 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 CIDRnotation and click Add. (i.e., 10.0.10.0/25)

Local Network Scheme explicit- velocities Network Address Addr/Mask (e.g. 10.6.0.0/16) 10.0.80.0/24 10.0.80.0/24 10.0.10.0/25 Add Delete	
Network Address Addr/Mask (e.g. 10.6.0.0/16) 10.0.80.0/24 10.0.80.0/24 10.0.10.0/25 Advertise Rout 10.0.80.0/24 10.0.10.0/25 Add Delete	
[e.g. 10.6.0.0/16] 10.0.80.0/24 [e.g. 10.6.0.0/16] 10.0.10.0/25 Advertise Rout 10.0.80.0/24 10.0.10.0/25 Interview Rout Interview Rout Add Delete Interview Rout Interview Rout	
Add Delete	∋=NO
Add Delete	

- 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)

Local Networks Local Identify		Remote Networks Remote Peer Identification	
Tunnel Parameter Template	-explicit-	Remote Peer Tunnel Name	
IP Address or Interface used for Tunnel Address Add Delete	Dynamic (via routing)	Remote Peer IP Addresses Addr/Mask (e.g. 10.6.1.1 or host.domain.com) Port (TCP only) 62.99.0.21/32 691 Add Delete	
Proxy Type Proxy Server IP [:port]	Direct (no Proxy)	Accepted Encryption Algorithms	
Proxy User Password		Accepted Authentication Algorithms ☑ SHA512 ☑ SHA256 ☑ SHA1 ☑ MD5 ☑ GCM ☑ RIPEMD160 ☑ NOHASH	

- Accepted Algorithms 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**.

Tunnel Parameter Template	-explicit-	Remote Peer Id		Ex/Import
IP Address or Interface used for Tunnel Address Add Delete	Dynamic (via routing) IP Address/Interface Name	CA Root X509 Condition Explicit X509	-Use-All-Known-	Export to Clipboard Export to File Blank Key Import from Public Key,X509 or Private Key
Proxy Type Proxy Server IP [:port] Proxy User Password	Direct (no Proxy)			Import from Clipboard Import from File

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.

Identification Type	Public Key	•	Parameters used for Remote Peer	Identification and Connection
Server Certificate	-Use-Default-		Remote Peer Tunnel Name	
Server Protocol Key	-Explicit-	Ex/Import	Remote Peer IP Addresses	Addr/Mask
		Export Public K Export Private I Export Private I Export Private I	iey to File Key to Clipboard Key to File Key to Clipboard (Password protected)	
		Export Private I	Key to File (Password protected)	Custom
		Blank Key		

- 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 > 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.

Call Direction	Passive	- Remote Pee	r Identification	
Local Network Scheme	-explicit-	▼ Public Key	Valid (LCQWRC)	Ex/Import
Notwork Addross		CA Root	-Use-All-Known-	Export to Clipboard
CONVIN Addiess	Addr/Mask	×509 Conditio	1	Export to File
e.g. 10.6.0.0/16)	10.0.10.0/25	5 F 3 V500		Blank Key
		Explicit Abus		Import from Public Key,X509 or Private Key
Add Delete				Import from Clipboard
				Import from File

- 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 <u>How to Create Access Rules for Site-to-Site VPN Access</u>.

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

DASHBOARD CON	FIGURATION	CONTRO	DL FIREWAL	L ATP	VPN PROXY LO	GS S	STATISTIC	CS EVE	NTS SS
Site-to-Site	Client-to-Site	e (i) St	atus						
Name	Tu	nnel	Local IP	Key	Internal	Info	Auth.	Idle	bit/s
I NGF1TINA2B02DF	ICP 🧯	a TINA		11s				3h 51m	0
	(L TINA	62 99 0 21	11s	FW2FW-NGF1TINA2B02DHCP		MD5	3h 51m	0
		CONTR					NTC	ссц	
DASHBOARD CON	IFIGURATION	CONTRO i i St	DL FIREWAL atus Local IP	L VPN	I LOGS STATISTICS	EVE	NTS Auth.	SSH	bit/s
DASHBOARD CON	IFIGURATION	CONTR contractor states contra	DL FIREWAL atus Local IP	L VPN Key 1m 18s	LOGS STATISTICS	EVE	NTS Auth.	SSH Idle 3h 52	bit/s 0



Figures

- 1. tina_isp.png
- 2. select_ipv6.png
- 3. configure_encryption_basics.png
- 4. loc_fw_loc_rem_networks.png
- 5. loc_fw_loc_rem_peers.png
- 6. loc_fw_copy_public_key.png
- 7. select_ipv6.png
- 8. configure_encryption_basics.png
- 9. rem_fw_loc_rem_networks.png
- 10. rem_fw_loc_rem_peer.png
- 11. rem_fw_import_rem_peer_key.png
- 12. rem_fw_copy_public_key.png
- 13. loc_fw_import_rem_peer_key.png
- 14. TINA_tunnel_first_firewall.png
- 15. TINA_tunnel_second_firewall.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.