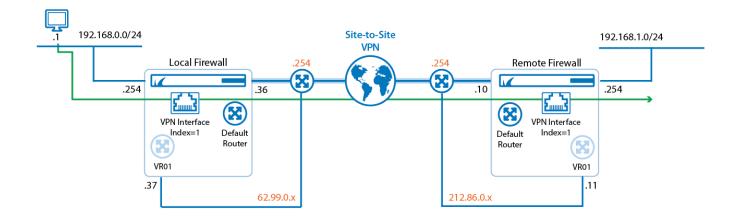


How to Create a VPN TINA Tunnel for Forwarding Traffic from a Local Default Router Instance to a Remote Default Router Instance

https://campus.barracuda.com/doc/96026166/

If you are running multiple virtual routers on your CloudGen Firewall, each virtual router instance can be configured independently of any other one. Because the VPN service is available only to the default router, the traffic managed by an additional virtual router instance must be handed over to the VPN service running in the default router so that it can be encapsulated into the VPN TINA tunnel. This is achieved by a VPN interface index that binds the tunnel configuration and the traffic from the additional virtual router instance to the VPN interface running on the default router.



In the following example, a VPN TINA tunnel is used for forwarding traffic between two private networks that are located behind a local and a remote firewall. The local firewall actively initiates a TINA tunnel while the remote firewall passively listens for tunnel connection requests. The first private network (192.168.0.0/24) is attached to an interface on the local firewall. This interface is managed by an additional virtual router instance (VR01). The second private network (192.168.1.0/24) is attached to an interface on the remote firewall. This interface is also managed by an additional virtual router instance (VR01). The second private network (192.168.1.0/24) is attached to an interface on the remote firewall. This interface is also managed by an additional virtual router instance (VR01). Both public IPs of the VPN TINA tunnel are managed by the default router. A client PC sends ping messages to the router address of the private network on the remote firewall (192.168.1.254).

Although not required, it is recommended for a better overview to use the same number for the VPN interface index as the number of your additional virtual router. For example, VR01 should correspond to a VPN interface index equal to 1.

Before You Begin

• Configure an additional virtual router instance on both the local and remote firewall. For more information, see <u>Virtual Routing and Forwarding (VRF)</u> and <u>How to Configure and Activate a</u>



Virtual Router Instance with Hardware, Virtual, VLAN or Bundled Interfaces.

 Configure the VPN service for general operation. For more information, see <u>How to Assign</u> <u>Services</u>.

Create a VPN Interface on the Local and Remote Firewall

Execute the following steps for both the local and remote firewall. Start with the local firewall.

- 1. Go to CONFIGURATION > Configuration Tree > Box > your local firewall > Assigned Services > VPN > VPN Settings.
- 2. Click **Lock**.
- 3. In the left menu, select **Routed VPN**.
- 4. Next to the **Interface Configuration** table, click **Add**. The **VPN Interface Properties** window opens.
- 5. For **VPN Interface Index**, enter a number. For a better overview, always use the same number as the number of your additional virtual router. For example, in case your router instance name is VR01, enter 1.

VPN Interface Properties		\times
VPN Interface Properties		
VPN Interface Index	1	
MTU	1398 ~	
IP Addresses		
Multicast Addresses		
VR Instance	VR01 🗠	
OK	Cancel	

- 6. From the **VR Instance** list, select your virtual router instance, e.g., VR01.
- 7. Click **OK**.
- 8. Click Send Changes and Activate.

If not yet done, repeat the previous steps on the remote firewall.

Create a VPN TINA Tunnel on the Local Firewall

- 1. Go to CONFIGURATION > Configuration Tree > Box > your local firewall > Assigned Services > VPN > Site to Site.
- 2. Click **Lock**.
- 3. Select **TINA Tunnels**.



- 4. Right-click and select New TINA tunnel... from the list.
- 5. In the **TINA Tunnel** window, enter a name for the TINA tunnel.
- 6. In the **Name** field, enter the name for the new VPN tunnel.
- 7. (IPv6 only) Select the **IPv6** check box.
- 8. Configure the **Basics** TINA tunnel settings to match the settings configured for the local firewall.
- 9. In the Local Networks tab, select the Call Direction to Active.
- 10. For the **Network Address**, enter the network address of the private network behind the local firewall, e.g., 192.168.0.0/24.
- 11. Click **Add**.

Local Networks Local Ide	ntify	
Call Direction	Active	\sim
Local Network Scheme	-explicit-	\sim
Network Address	Addr/Mask	
(e.g. 10.6.0.0/16)		
192.168.0.0/24		
Add Delete		

- 12. Click the Local tab and select Explicit List (ordered) from the list.
- 13. Enter the IP address or Interface used for Tunnel Address.
- 14. Click **Add**.

\sim
ed) 🗸
ace Name
\sim

- 15. In the **Remote Networks** tab, enter 1 for the **VPN Interface Index**.
- 16. For the **Remote Network**, enter the network address for the private network behind the remote firewall, e.g., 192.168.1.0/24.
- 17. Click Add.

Barracuda CloudGen Firewall



Remote Networks Remote P	eer Identification
VPN Interface Index	1
Remote Network (e.g. 10.6.0.0/16)	Addr/Mask
192.168.1.0/24	
Advertise Route	

18. Click the **Remote** tab and enter the **Remote Peer IP Address**, e.g., 212.86.0.10.

19. Click **Add**.

Remote Networks	Remote Peer	r Identification		
Parameters used fo	or Remote Peer	Identification	and Connection	
Remote Peer Tunn	el Name			
Remote Peer IP Ad (e.g. 10.6.1.1 or host.domain.com)	ldresses Port (TCP only)	Addr/Mask	¢	
212.86.0.10/32	691 🗠	1		
Add Delete				▲
Accepted Cipher	s			
AES 🗸	CAST	Blowfish	☑ 3DES	
DES	Null	AES256	Custom	

- 20. Click **OK** to leave the **TINA Tunnel** window.
- 21. When you are informed that the identification information between the two sites has not been set, click **OK** to proceed. This information will be configured in a following step.

Create a VPN TINA Tunnel on the Remote Firewall

- 1. Go to CONFIGURATION > Configuration Tree > Box > your remote firewall > Assigned Services > VPN > Site to Site.
- 2. Click Lock.
- 3. Select TINA Tunnels.
- 4. Right-click and select New TINA tunnel... from the list.
- 5. In the **TINA Tunnel** window, enter a name for the TINA tunnel.
- 6. In the Name field, enter the name for the new VPN tunnel.
- 7. (IPv6 only) Select the **IPv6** check box.
- 8. Configure the **Basics** TINA tunnel settings to match the settings configured for the remote firewall.
- 9. In the Local Networks tab, select the Call Direction to Passive.
- 10. For the **Network Address**, enter the network address of the private network behind the local firewall, e.g., 192.168.1.0/24.
- 11. Click **Add**.

Barracuda CloudGen Firewall



Call Direction	Passive	~
Local Network Scheme	-explicit-	~
Network Address	Addr/Mask	
(e.g. 10.6.0.0/16)		
192.168.1.0/24		
Add Delete		

- 12. Click the Local tab and select Explicit List (ordered) from the list.
- 13. Enter the **IP address or Interface used for Tunnel Address**, e.g. 212.86.0.10.
- 14. Click **Add**.

unnel Parameter Template	-explicit-	\sim
P Address or Interface used	Explicit List (ordered)	~
or Tunnel Address 212.86.0.10 Add Delete	IP Address/Interface	e Name
гоху Туре	Direct (no Proxy)	~
Proxy Server IP [:port]		
Proxy User		

- 15. In the **Remote Networks** tab, enter 1 for the **VPN Interface Index**.
- 16. For the **Remote Network**, enter the network address for the private network behind the remote firewall, e.g., 192.168.0.0/24.
- 17. Click **Add**.

Remote Networks Remote F	Peer Identification
VPN Interface Index	1
Remote Network (e.g. 10.6.0.0/16)	Addr/Mask
192.168.0.0/24	
Advertise Route	

- 18. Click the **Remote** tab and enter the **Remote Peer IP Address**, e.g., 62.99.0.36.
- 19. Click **Add**.



r didineters us	ed for Remote Pe	eridentilication	and connection	
Remote Peer	Funnel Name			
Remote Peerl (e.g. 10.6.1.1) host.domain.co	pr Port	Addr/Mask	:	
62.99.0.36/3	2 691	\sim		_
Add De	elete			-
Accepted Ci	phers			
AES	CAST	🗸 Blowfish	✓ 3DES	
DES	Null	AES256	Custom	

20. Directly proceed with the next step without leaving the displayed window.

Exchange the Public Keys Between the Local and Remote Firewall

Start with exporting the public key in the displayed window on the remote firewall.

- 1. Click the **Identify** tab.
- 2. Click **Ex/Import**.

Identification Type	Public Key		\sim		
Server Certificate	-Use-Default-		\sim		
Server Protocol Key	-Explicit-	\sim	Ex/Import 🔻		
	Valid (ZWPFMN)				
In the menu,	click Export	Public	: Kev 1	to Clip	boa
			,	in enbi	
Export Public Key t	to Clipboard		,,		
Export Public Key t Export Public Key t			,, , .		
	to File		,	io enp	
Export Public Key t	to File to Clipboard		,		
Export Public Key t Export Private Key Export Private Key	to File to Clipboard				
Export Public Key t Export Private Key Export Private Key Export Private Key	to File to Clipboard to File	l protected)			
Export Public Key t Export Private Key Export Private Key Export Private Key	to File to Clipboard to File to Clipboard (Password	l protected)			
Export Public Key t Export Private Key Export Private Key Export Private Key Export Private Key	to File to Clipboard to File to Clipboard (Password to File (Password prote	l protected)			
Export Public Key t Export Private Key Export Private Key Export Private Key Export Private Key Blank Key	to File to Clipboard to File to Clipboard (Password to File (Password prote	l protected)			
Export Public Key t Export Private Key Export Private Key Export Private Key Export Private Key Blank Key Import Private Key	to File to Clipboard to File to Clipboard (Password to File (Password prote from Clipboard from File	l protected)			
Export Public Key t Export Private Key Export Private Key Export Private Key Export Private Key Blank Key Import Private Key	to File to Clipboard to File to Clipboard (Password to File (Password prote from Clipboard from File	l protected)			

5. Go to CONFIGURATION > Configuration Tree > Box > your local firewall > Assigned



- Services > VPN > Site to Site.
- 6. Click Lock.
- 7. Select TINA Tunnels.
- 8. Double-click the entry for the VPN tunnel.
- 9. The **TINA Tunnel** window is displayed.
- 10. Click the **Peer Identification** tab.
- 11. Click Ex/Import.
- 12. In the menu, click Import Private Key from Clipboard.

Export to Clipboard
Export to File
Blank Key
Import from Public Key,X509 or Private Key
Import from Clipboard
Import from File

- 13. Click the **Identify** tab.
- 14. Click **Ex/Import**.
- 15. In the menu, click Export Public Key to Clipboard.
- 16. Click **OK** to close the **TINA Tunnel** window.
- 17. Go to CONFIGURATION > Configuration Tree > Box > your remote firewall > Assigned Services > VPN > Site to Site.
- 18. Click Lock.
- 19. Select TINA Tunnels.
- 20. Double-click the entry for the VPN tunnel.
- 21. The TINA Tunnel window is displayed.
- 22. Click the Peer Identification tab.
- 23. Click Ex/Import.
- 24. In the menu, click Import Private Key from Clipboard.
- 25. Click **OK** to close the **TINA Tunnel** window.

Verify that the VPN TINA Tunnel is up

- 1. Log into your local firewall.
- 2. Go to VPN > Site-to-Site.

DASHBOARD	CONFIGURATION	CONTROL	FIREWALL V	PN LOGS	STATIST	TICS EVE	NTS SSH			Ċ
Site-to-Site	Client-to-Site	(i) Status	<		NAC:0 (501) - (500) - SSL:0	Clients:0 (500) 0 Refresh if active	C (F5)	🗡 Disc	onnect
Name	^	Tunnel	Local IP	Peer IP	bit/s	Key	Internal	Auth.	Transport	Idle
I HA12toBO	1721	TINA			0	4m 21s				4m 41s
Bulk (0)		TINA	62.99.0.36:691	212.86.0.10:6	. 0	4m 21s	FW2FW-HA12toBO1721	MD5	UDP	4m 41s
Log into	your remote N > Site-to									
Log into	•			/PN LOGS	STATIST	ICS EVE	NTS SSH			d
Log into Go to VP	N > Site-to	-Site.				Clients:0 (500		C Refresh (F5)	N Disc	
Log into Go to VP	N > Site-to	-Site.			NAC:0 (501) -	Clients:0 (500) 0 🔥 Refresh if_		Disc Transport	
Log into y Go to VP DASHBOARD	N > Site-to CONFIGURATION	CONTROL	FIREWALL V	Filter	NAC:0 (501) - (500) - SSL:0	Clients:0 (500) 0 Refresh if active	C (F5)		



Create an Access Rule for the Local and Remote Firewall to let VPN Traffic Pass

Traffic originating from the private network behind the local firewall must be able to reach the private network behind the remote firewall. The access rule must be configured to be **Bi-Directional**. In order to forward traffic from the interfaces that are assigned to the additional virtual router instance, the access rule must be applied to this virtual router instance, e.g., VR01. The access rule must be created on both the local firewall and the remote firewall.

- 1. On the local firewall, go to CONFIGURATION > Configuration Tree > Box > your local firewall > Assigned Services > Firewall > Forwarding Rules.
- 2. The Forwarding Rules window is displayed.
- 3. Click **Lock**.
- 4. Click + to add a new access rule.
- 5. For the access rule type, select **Pass**.
- 6. Enter the name for the access rule, e.g., VPN-S-2-S.
- 7. Click Bi-Directional.
- 8. Select the virtual router instance for **Source VR Instance** and **Destination VR Instance**, e.g., VR01.
- 9. For **Source**, click **<explicit-src>** from the list, and enter the network address for the private network behind the local firewall, e.g., 192.168.0.0/24.
- 10. For **Service**, select **Any** from the list.
- 11. For **Destination**, click **<explicit-src>** from the list, and enter the network address for the private network behind the remote firewall, e.g., 192.168.1.0/24.
- 12. For the Connection Method, select Original Source IP.

Pass	VPN-S	-2-S					
🛹 🗹 Bi-Directional		💍 🗌 Dynamic Rule	🕘 🗌 Deactivate Rule				
Source VR Instance	VR01	 Destinati 	ion VR Inst	ance	VR01 ~		
Source		Service		Destination	DN		
<explicit-src></explicit-src>	~	Any	~	<explicit-< td=""><td>dest> ~</td></explicit-<>	dest> ~		
192.168.0.0/24		Ref: Any-TCP		192,168	1.0/24		
		Ref: Any-UDP					
		Ref: ICMP					
		ALLIP					
Authenticated User		Policies		Connecti	on Method		
Authenticated User	~	Policies IPS Policy					
	~		~	Original S	ource IP V		
	~	IPS Policy		Original S			
	~	IPS Policy Default Policy		Original S	ource IP V		
	~	IPS Policy Default Policy Application Policy		Original S	ource IP V		
	~	IPS Policy Default Policy Application Policy AppControl		Original S	ource IP V		
	×	IPS Policy Default Policy Application Policy AppControl SSL Inspection Policy	~	Original S	ource IP V		
	~	IPS Policy Default Policy Application Policy AppControl SSL Inspection Policy N.A.	~	Original S	ource IP V		
		IPS Policy Default Policy Application Policy AppControl SSL Inspection Policy N.A. Schedule	>	Original S	ource IP V		
		IPS Policy Default Policy Application Policy AppControl SSL Inspection Policy N.A. Schedule Always	>	Original S	ource IP V		
	~	IPS Policy Default Policy Application Policy AppControl SSL Inspection Policy N.A. Schedule Always QoS Band (Fwd)	~	Original S	ource IP V		

13. Click **OK**.



Repeat the previous steps for the remote firewall.

Verify that the Virtual Tunnel is Forwarding Traffic

- 1. Attach a client host to the private network behind the local firewall, and configure the standard route pointing to the interface that is managed by the additional virtual router instance, e.g., 192.168.0.254.
- 2. Start sending ping messages to the gateway address interface on the remote firewall that is managed by the additional virtual router instance, e.g., 192.168.1.254.
- 3. On the local firewall, go to **FIREWALL > Live**.
- 4. Set the filter for **Src. VR Instance** to the name of your additional virtual router instance, e.g., VR01.

DAS	IBOARD	CONFIGURA	ATION	CONTROL	FI	REWALL VPN	LOG	STATISTICS	EVENTS SSF	4					Ċ
P	Monitor	(A) Live	О н	story 🔞	Threat Scan	Audit Log	Sha	ping 👤 Users	S Dynamic	Host Rules		🎟 📸	2 Sessions	C 🕕	~
Traffic	Selection	Forward, Loc	al In, Loc	cal Out, IPv4, IP	v6	Status Selection	Closing	, Established, Failing, Pe	ending 🔍 Src. V	R Instance 🖂 VF	R01	>	•		
ID	State	IP Protocol	Port	Source	Interfac	e Destination	SNAT	Output-IF	Src. VR Instan	ce Dst VR Instance	Application	Application Context	Rule	bit/s	Total
∥ 776	3 🚓 🐥	ICMP		192.168.0.1	eth2	192.168.1.254		vpn1@FW2FW-HA12to	BO1 VR01				VPN-S-2-S	960	6.8 K

- 5. In the column Output-IF, the firewall displays the name of the VPN tunnel connection, e.g., vpn1@FW2FW-..... Note that the number 1 is part of vpn1@..., indicating the VPN Interface Index that was set to 1 at the beginning. The client PC is sending ping messages from its IP address 192.168.0.1.
- 6. On the remote firewall, go to **FIREWALL > Live**.
- 7. Set the filter for **Dst. VR Instance** to the name of your additional virtual router instance, e.g., VR01.

DASH	BOARD	CONFIGURAT	ION (CONTROL	FIREWALL VPN	LOGS	STATIS	TICS E	VENTS	SSH				Ċ
P	onitor	(A) Live	History	Three Scar	at Audit	Shap	oing 👤	Users (S Dynamic	Host Rules	Fa	🔜 😽	2 Sessions) 🕕 🗡
Traffic S	election	Forward, Local	In, Local O	ut, IPv4, IPv6	Status Selection	Closing	, Established, F	ailing, Pending	Dst	t. VR Instance 🔽	VR01		× +	
ID	State	IP Protocol	Port	Source	Interface	C	estination	SNAT	Output-IF	Src. VR Instance	Dst VR Instance	Application	Application Context	Rule
153	🔶 🐥	ICMP		192.168.0.1	vpn1@FW2FW-BO172	toHA12 1	92.168.1.254		vpn1		VR01			OP-SRV-VPN

8. In the column Interface, the firewall displays the name of the VPN tunnel connection, e.g., vpn1@FW2FW-..... Note that the number 1 is part of vpn1@..., indicating the VPN Interface Index that was set to 1 at the beginning. The column Output-IF displays the name of the VPN tunnel, e.g., vpn1.

(Optional) Verify that a Client Host on the Remote Private Network can be Reached

- 1. Attach a client host to the private network behind the remote firewall and configure its IP address, e.g., 192.168.1.1.
- 2. Ensure that there is no local firewall running on the client host. If so, disable the firewall completely on the client host so that all packages can reach the client host.
- 3. Start sending ping messages from the local client host to the remote client host: On your client host, enter ping 192.168.1.1
- 4. On the remote firewall, go to **FIREWALL > Live**.
- 5. Set the filter for **Dst. VR Instance** to the name of your additional virtual router instance, e.g., VR01.





6. In the column **Interface**, the firewall displays the name of the VPN tunnel connection, e.g., vpn1@FW2FW-. Note that in this case the access rule is now VPN-S-2-S, which indicates that the ping packages are now forwarded from the VPN service on the remote firewall to the remote client host while traversing the interface eth3 on the virtual router VR01.



Figures

- 1. vpn_tina_tunnel_forwarded_by_dflt_router.png
- 2. vrf_VPN_interface_properties.png
- 3. add_local_network_address_on_local_fw.png
- 4. add_local_tunnel_parameters_on_local_fw.png
- 5. add_remote_network_address_on_local_fw.png
- 6. add_remote_peer_address_on_local_fw.png
- 7. add_local_network_address_on_remote_fw.png
- 8. add_local_tunnel_parameters_on_remote_fw.png
- 9. add_remote_network_address_on_remote_fw.png
- 10. add_remote_peer_address_on_remote_fw.png
- 11. export_public_key_on_the_remote_firewall.png
- 12. export_public_key.png
- 13. import_public_key.png
- 14. vpn_tina_tunnel_up_local_firewall.png
- 15. vpn_tina_tunnel_up_remote_firewall.png
- 16. vrf_VPN_s2s_access_rule_for_default_router.png
- 17. firewall live output local firewall.png
- 18. firewall_live_output_remote_firewall.png
- 19. ping reaches client host behind remote 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.