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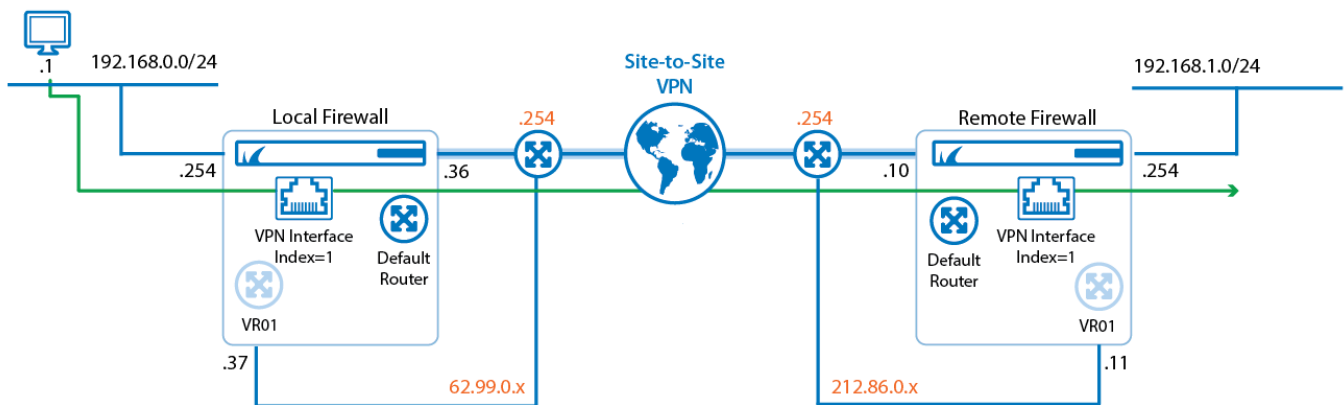 How to Create a VPN TINA Tunnel for Forwarding Traffic from a Local Default Router Instance to a Remote Default Router Instance

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). 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 Virtual Routing and Forwarding (VRF) and How to Configure and Activate a

How to Create a VPN TINA Tunnel for Forwarding Traffic from a Local Default Router Instance to a Remote Default Router Instance
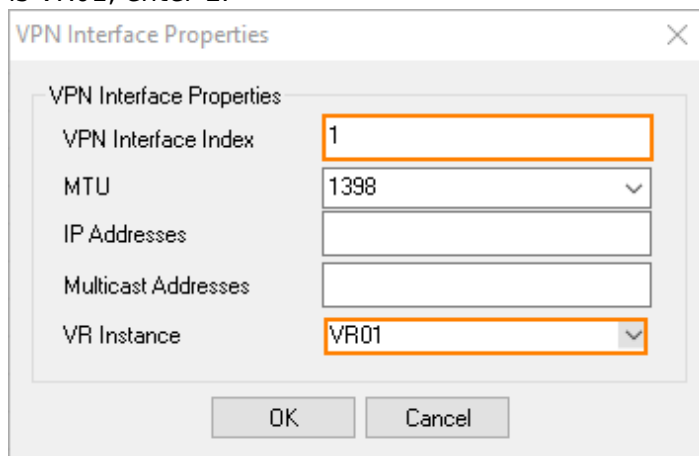
1 / 11

[Virtual Router Instance with Hardware, Virtual, VLAN or Bundled Interfaces](#).
- Configure the VPN service for general operation. For more information, see [How to Assign Services](#).

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.
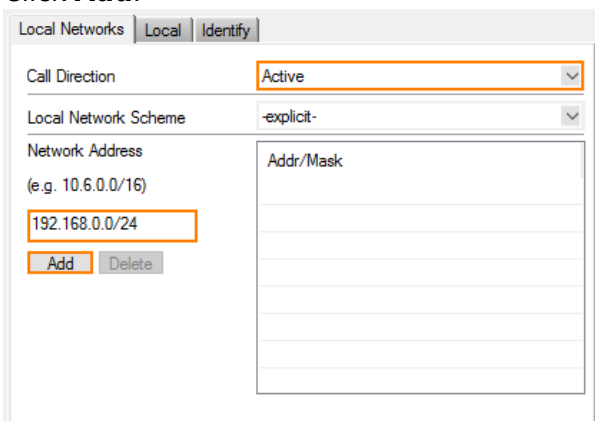

6. From the **VR Instance** list, select your virtual router instance, e.g., VR01.
7. Click **OK**.
8. Click **Send Changes** and **Activate**.

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**.

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

2 / 11

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**.
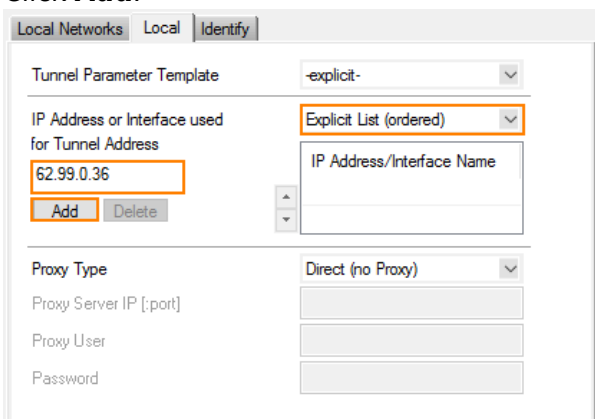
12. Click the **Local** tab and select **Explicit List (ordered)** from the list.
13. Enter the **IP address or Interface used for Tunnel Address**.
14. Click **Add**.
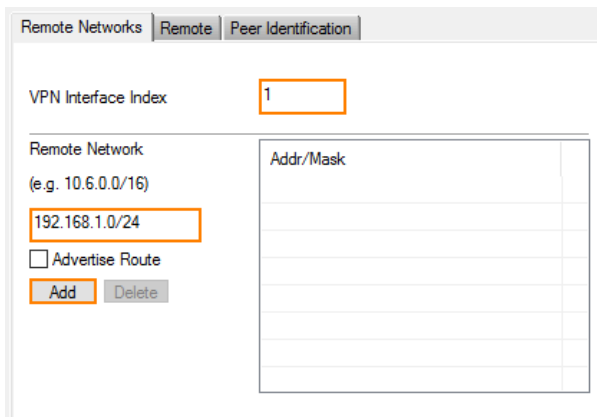
15. In the **Remote Networks** tab, enter 1 for the **VPN Interface Index**.
16. For the **Remote Network**, enter the network address for the private network behind the remote firewall, e.g., 192.168.1.0/24.
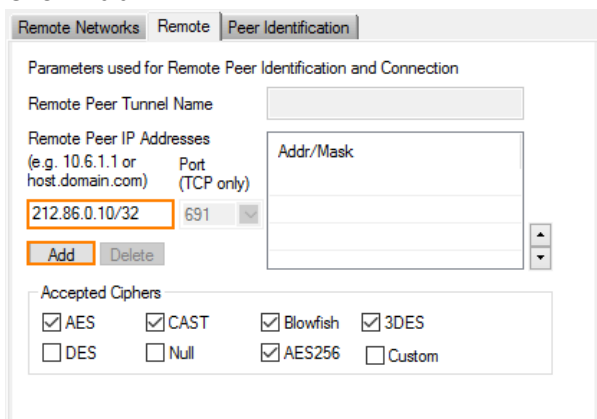17. Click **Add**.

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

3 / 11

18. Click the **Remote** tab and enter the **Remote Peer IP Address**, e.g., 212.86.0.10.
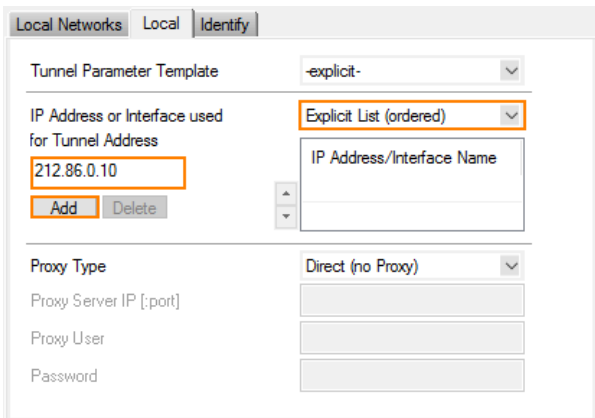19. Click **Add**.
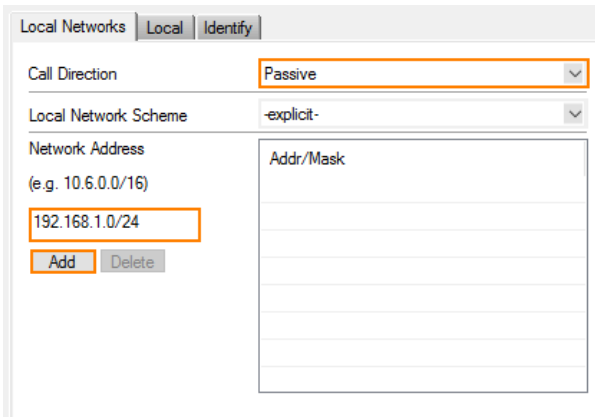
20. Click **OK** to leave the **TINA Tunnel** window.
21. When you are informed that the identification information between the two sites has not been set, click **OK** to proceed. This information will be configured in a following step.

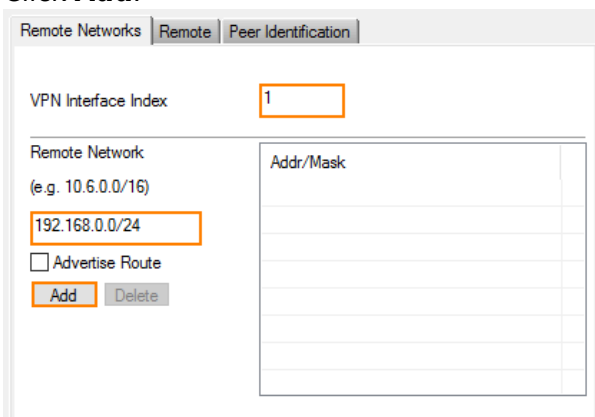## Create a VPN TINA Tunnel on the Remote Firewall

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**.

How to Create a VPN TINA Tunnel for Forwarding Traffic from a Local Default Router Instance to a Remote Default Router Instance
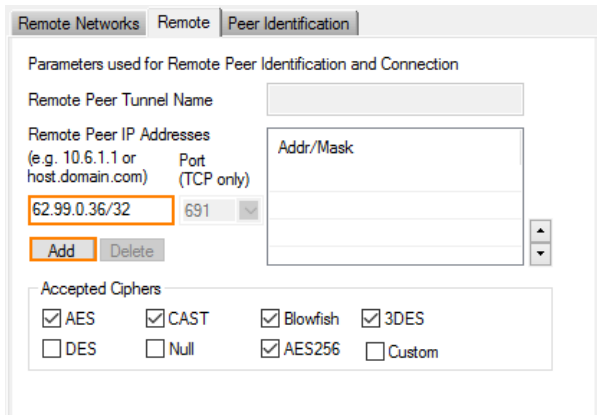
4 / 11

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**.

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**.

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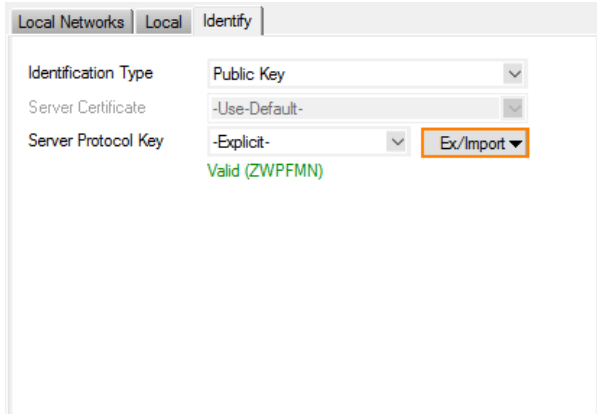19. Click **Add**.

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

5 / 11

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.

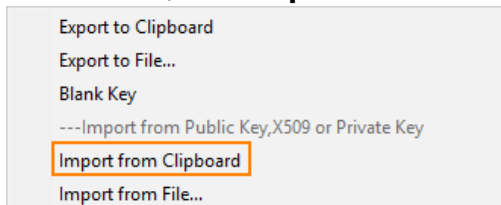1. Click the **Identify** tab.
2. Click **Ex/Import**.

3. In the menu, click **Export Public Key to Clipboard**.

4. Click **OK** to close the **TINA Tunnel** window.
5. Go to **CONFIGURATION** > **Configuration Tree** > **Box** > *your local firewall* > **Assigned**

How to Create a VPN TINA Tunnel for Forwarding Traffic from a Local Default Router Instance to a
Remote Default Router Instance
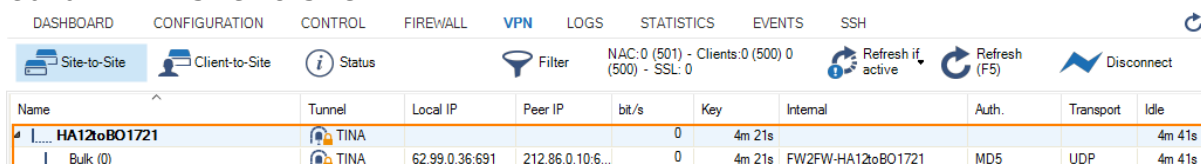
6 / 11

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**.
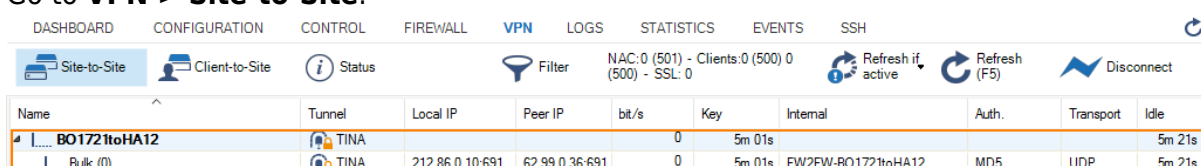25. Click **OK** to close the **TINA Tunnel** window.

Verify that the VPN TINA Tunnel is up

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

3. Log into your remote firewall.
4. Go to **VPN > Site-to-Site**.
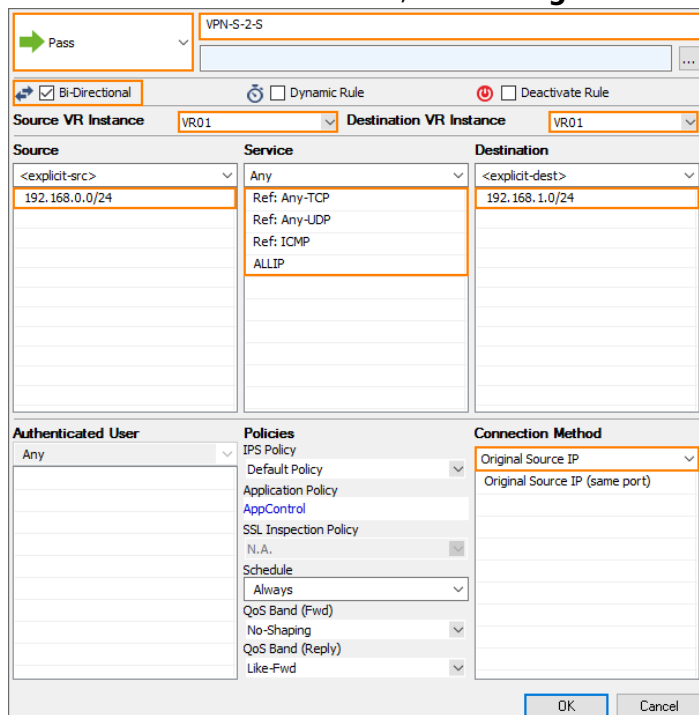
How to Create a VPN TINA Tunnel for Forwarding Traffic from a Local Default Router Instance to a
Remote Default Router Instance

7 / 11

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`.
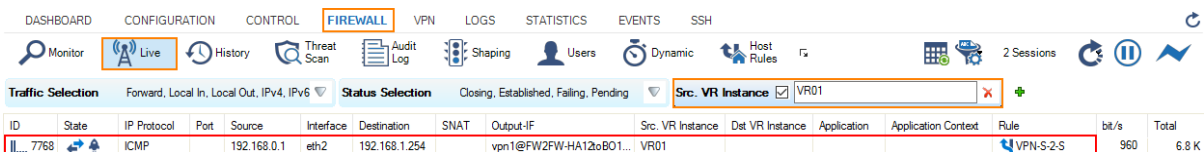12. For the **Connection Method**, select **Original Source IP**.

13. Click **OK**.

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

8 / 11
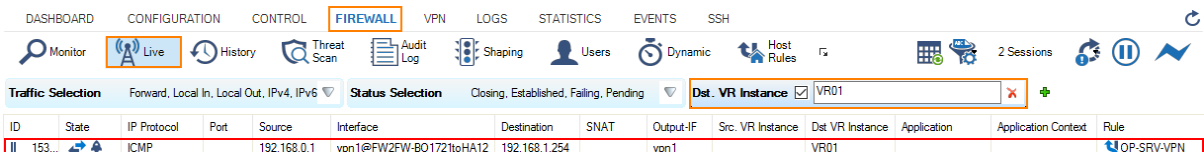
Repeat the previous steps for the remote firewall.

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.

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.

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.

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

9 / 11

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.

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

10 / 11

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

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

11 / 11