How to Set Up a Default Route Through a Site-to-Site VPN Tunnel

https://campus.barracuda.com/doc/43846990/

In this example scenario, a Barracuda NG Firewall in the internal LAN requires an Internet connection. A second Barracuda NG Firewall (the external system) has direct Internet access and is therefore used to tunnel the Internet traffic to the internal system.

In this article:

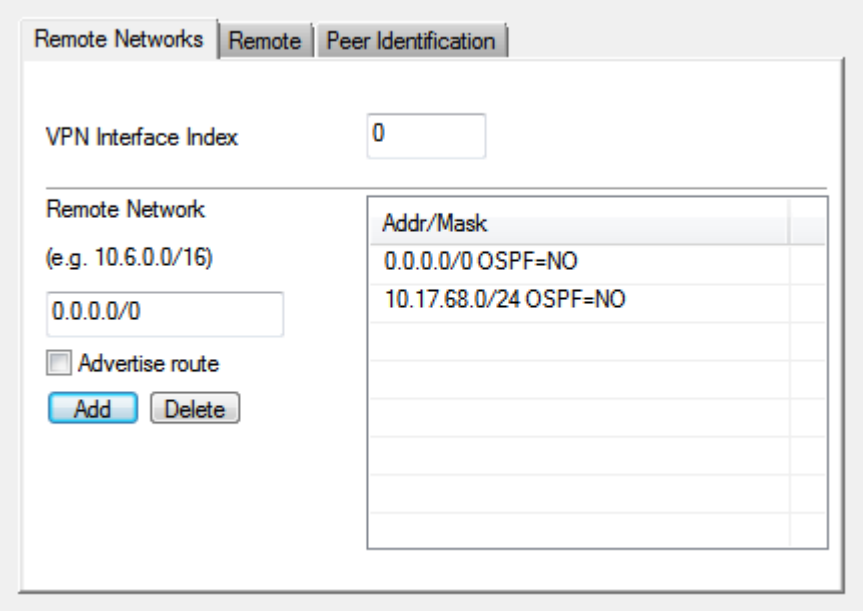
1. Configure a Site-to-Site VPN Tunnel

Make sure that you have correctly configured the site-to-site VPN tunnel between both Barracuda NG Firewalls. For more information, see How to Create a TINA VPN Tunnel between Barracuda NG Firewalls.

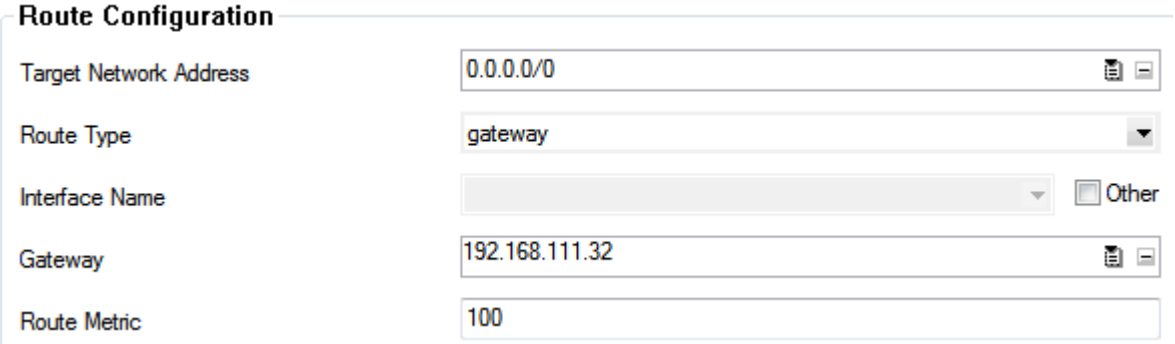
2. Configure the Internal Barracuda NG Firewall

To configure the Barracuda NG Firewall in the internal LAN:

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > Site to Site**.
2. Click **Lock**.
3. Open the TINA tunnel and configure 0.0.0.0/0 as the **Remote Network**.



4. Create a dummy default route to prevent packets from being dropped in the forwarding firewall.

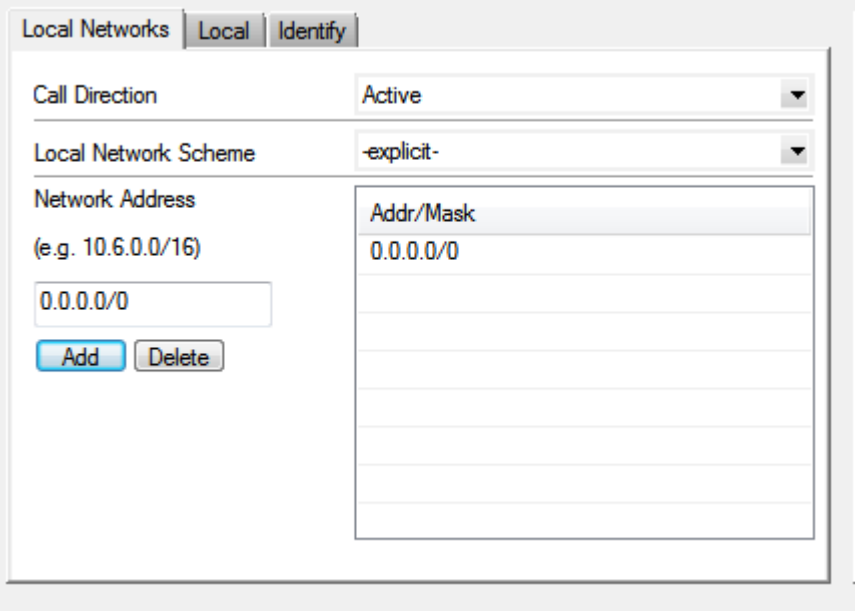


5. Click **Send Changes** and **Activate**.

3. Configure the External Barracuda NG Firewall

To configure the external Barracuda NG Firewall:

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > Site to Site**.
2. Click **Lock**.
3. Open the TINA tunnel and add 0.0.0.0/0 (the default route) in the **Local Networks** table.



4. Click **Send Changes** and **Activate**.

4. Configure Firewall Rules for the Tunnel

Remember to also create firewall rules on both Barracuda NG Firewalls for the tunnel traffic. For more information, see How to Create Access Rules for Site-to-Site VPN Access.

If NAT is turned on in firewall rules for the internal unit, the dummy route is used instead of the VPN tunnel. Therefore, make sure that the rules have **No Src NAT** configured for Internet traffic traversing the VPN tunnel.

Troubleshooting

If you have issues with the default route for the site-to-site VPN tunnel, try the following solutions:

Issue	Solution
No traffic passes through the default route.	Verify whether the VPN connection itself works by setting up clients on both ends of the tunnel. Note that locally transmitted ICMP pings are not redirected through the tunnel. The client on the external system can also be an external web server.

ICMP traffic passes through the VPN tunnel in one direction but the reply does not.	Try enabling NAT on the external Barracuda NG Firewall.
There is no connection to the Internet.	Make sure that a valid default route also appears in the regular network configuration of the external Barracuda NG Firewall and that this default route points to a working Internet gateway.

Figures

1. defroutvpnint.png
2. howtocreadefroutvpndummy.png
3. howtocredefroutext.png