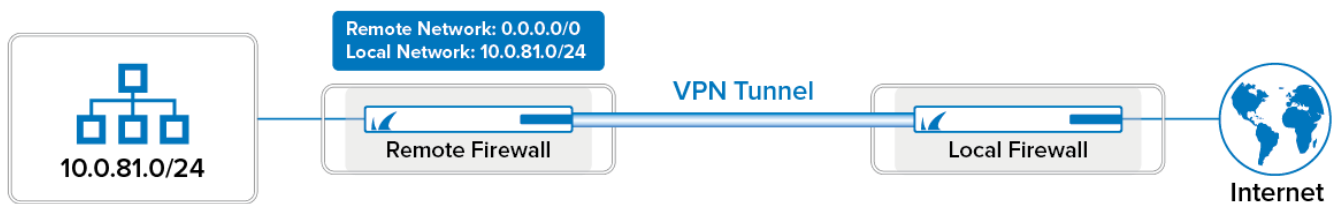


How to Set Up a Default Route Through a Site-to-Site VPN Tunnel

<https://campus.barracuda.com/doc/96026160/>

To move the Internet breakout for the branch office to one central location, connect the branch offices with site-to-site VPN tunnels configured to send all Internet traffic for the client behind the remote firewall through the VPN tunnel. The local firewall can then apply company-wide security policies in one location.



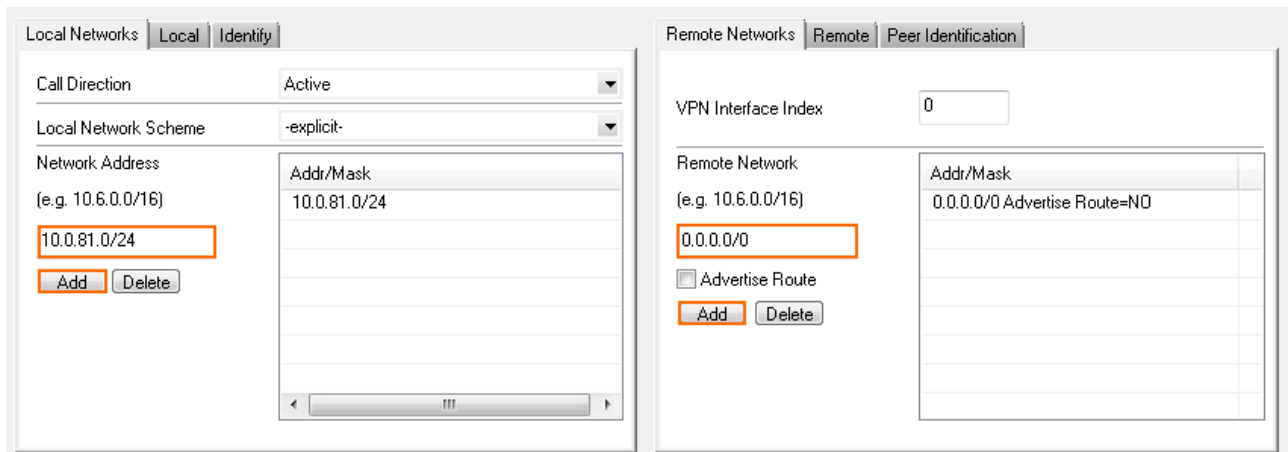
Before You Begin

Configure a TINA site-to-site VPN tunnel between the local and remote firewalls.

For more information, see [How to Create a TINA VPN Tunnel between CloudGen Firewalls](#).

Step 2. Configure the VPN Tunnel on the Remote Firewall

1. Log into the remote firewall.
2. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > Site to Site**.
3. Click **Lock**.
4. Double-click the VPN tunnel.
5. Configure the VPN tunnel between the remote and the local firewall:
 - **Local Networks** - Enter the networks you want to route through the VPN tunnel.
 - **Remote Networks** - Enter 0.0.0.0/0 as the remote network to forward all traffic through the site-to-site VPN tunnel to the remote firewall.



The screenshot shows the VPN configuration interface with two main sections: Local Networks and Remote Networks.

Local Networks:

- Call Direction: Active
- Local Network Scheme: -explicit-
- Network Address (e.g. 10.6.0.0/16): 10.0.81.0/24
- Buttons: Add, Delete

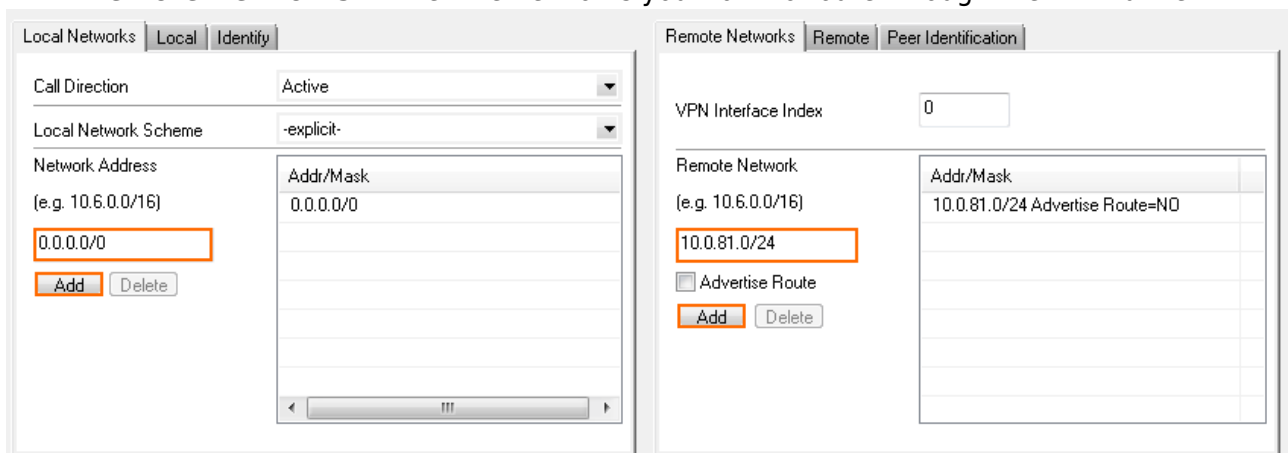
Remote Networks:

- VPN Interface Index: 0
- Remote Network (e.g. 10.6.0.0/16): 0.0.0.0/0 Advertise Route=NO
- Buttons: Add, Delete

6. Click **Send Changes** and **Activate**.

Step 3. Configure the VPN Tunnel on the Local 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. Double-click the VPN tunnel.
5. Configure the VPN tunnel between the local and the remote firewall:
 - **Local Networks** - Enter 0.0.0.0/0.
 - **Remote Networks** - Enter the networks you want to route through the VPN tunnel.



The screenshot shows the VPN configuration interface with two main sections: Local Networks and Remote Networks.

Local Networks:

- Call Direction: Active
- Local Network Scheme: -explicit-
- Network Address (e.g. 10.6.0.0/16): 0.0.0.0/0
- Buttons: Add, Delete

Remote Networks:

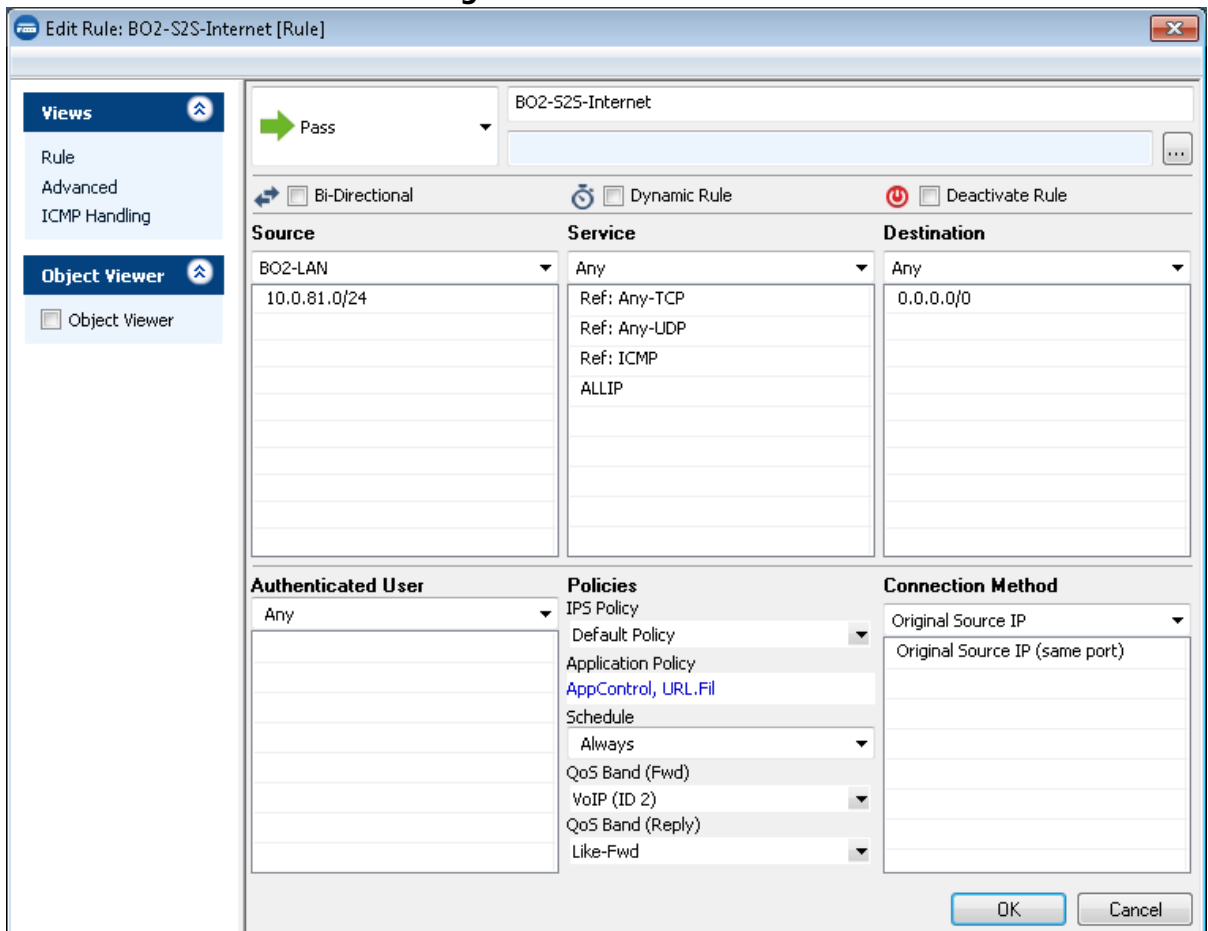
- VPN Interface Index: 0
- Remote Network (e.g. 10.6.0.0/16): 10.0.81.0/24 Advertise Route=NO
- Buttons: Add, Delete

6. Click **Send Changes** and **Activate**.

Step 4. Configure an Access Rule for the Remote Firewall

The remote firewall sends all Internet traffic through the VPN tunnel.

1. Log into the remote firewall.
2. On your firewall with no direct Internet access, go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
3. Click **Lock**.
4. Right-click the ruleset and select **New**. The **New Rule** window opens.
5. Enter a **Name** for the access rule.
6. Right-click the ruleset and select **New > Rule** to create an access rule to match the VPN traffic:
 - **Action** - Select **Pass**.
 - **Source** - Enter your private network used for the VPN tunnel.
 - **Service** - Select the services allowed to access the tunnel. Default: **Any**
 - **Destination** - Configure the route to the Internet as the destination so that traffic will be sent through the VPN tunnel to the remote firewall.
 - **Connection Method** - Select **Original Source IP**.



The screenshot shows the 'Edit Rule: BO2-S2S-Internet [Rule]' window. The interface includes a left sidebar with 'Views' (Rule, Advanced, ICMP Handling) and 'Object Viewer'. The main area contains the following fields:

- Action:** A dropdown menu showing 'Pass' with a green arrow icon.
- Name:** A text field containing 'BO2-S2S-Internet'.
- Bi-Directional:** A checkbox that is unchecked.
- Dynamic Rule:** A checkbox that is unchecked.
- Deactivate Rule:** A checkbox that is unchecked.
- Source:** A dropdown menu showing 'BO2-LAN' with a list of IP addresses below it, including '10.0.81.0/24'.
- Service:** A dropdown menu showing 'Any' with a list of services below it, including 'Ref: Any-TCP', 'Ref: Any-UDP', 'Ref: ICMP', and 'ALLIP'.
- Destination:** A dropdown menu showing 'Any' with a list of IP addresses below it, including '0.0.0.0/0'.
- Authenticated User:** A dropdown menu showing 'Any'.
- Policies:** A section with multiple dropdown menus: 'IPS Policy' (Default Policy), 'Application Policy' (AppControl, URL.Fil), 'Schedule' (Always), 'QoS Band (Fwd)' (VoIP (ID 2)), 'QoS Band (Reply)' (Like-Fwd), and 'Like-Fwd'.
- Connection Method:** A dropdown menu showing 'Original Source IP' with a list of options below it, including 'Original Source IP (same port)'.

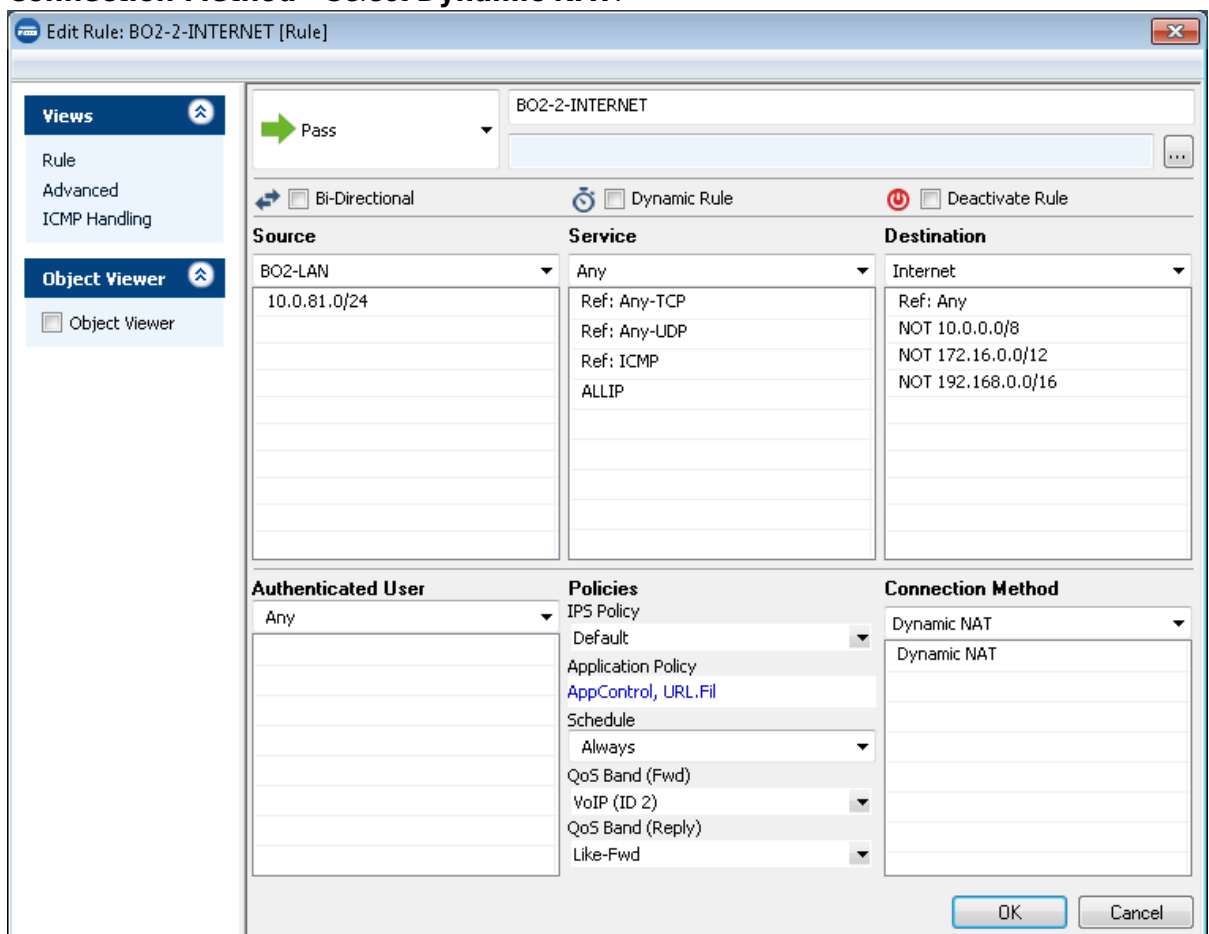
At the bottom right, there are 'OK' and 'Cancel' buttons.

7. Click **OK**.
8. Reorder the access rule by dragging it to the correct position in the Forwarding Firewall's ruleset. Make sure no access rule placed above it will match the traffic for the site-to-site access rule.
9. Click **Send Changes** and **Activate**.

Step 5. Configure an Access Rule for the Local Firewall

The local firewall forwards Internet traffic from the remote networks.

1. Log into the local firewall.
2. On your firewall with direct internet access, go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
3. Click **Lock**.
4. Right-click the ruleset and select **New**. The **New Rule** window opens.
5. Enter a **Name** for the access rule.
6. Right-click the rule set and select **New > Rule** to create an access rule to match the VPN traffic:
 - **Action** - Select **Pass**.
 - **Source** - Select your private local network.
 - **Service** - Select the services allowed to access the tunnel. Default: **Any**
 - **Destination** - Configure the route to the **Internet** as the destination.
 - **Connection Method** - Select **Dynamic NAT**.



Edit Rule: BO2-2-INTERNET [Rule]

Views: Rule, Advanced, ICMP Handling

Object Viewer: Object Viewer

Pass

BO2-2-INTERNET

☐ Bi-Directional ☐ Dynamic Rule ☐ Deactivate Rule

Source	Service	Destination
BO2-LAN 10.0.81.0/24	Any Ref: Any-TCP Ref: Any-UDP Ref: ICMP ALLIP	Internet Ref: Any NOT 10.0.0.0/8 NOT 172.16.0.0/12 NOT 192.168.0.0/16

Authenticated User	Policies	Connection Method
Any	IPS Policy Default Application Policy AppControl, URL.Fil Schedule Always QoS Band (Fwd) VoIP (ID 2) QoS Band (Reply) Like-Fwd	Dynamic NAT Dynamic NAT

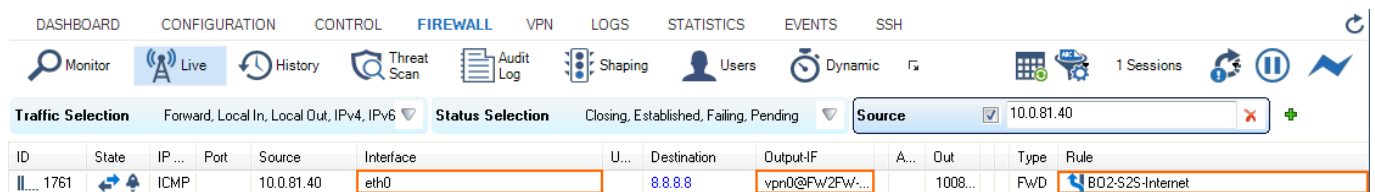
OK Cancel

7. Click **OK**.
8. Reorder the access rule by dragging it to the correct position in the Forwarding Firewall's ruleset. Make sure no access rule placed above it will match the traffic for the site-to-site access rule.

9. Click **Send Changes** and **Activate**.

The clients behind the remote firewall can now access the Internet via the site-to-site VPN tunnel. On the local and remote firewall, go to **FIREWALL > Live**. Verify that the Internet traffic for the clients behind the remote firewall is flowing through the VPN tunnel and that it is forwarded to the Internet on the local firewall.

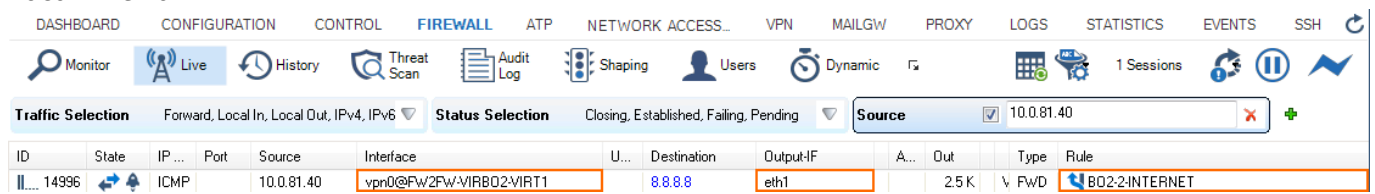
Remote firewall:



The screenshot shows the 'FIREWALL > Live' interface of a remote firewall. The 'Traffic Selection' dropdown is set to 'Forward, Local In, Local Out, IPv4, IPv6'. The 'Status Selection' dropdown is set to 'Closing, Established, Failing, Pending'. The 'Source' field is set to '10.0.81.40'. The table below shows a single entry with ID 1761, State 'Established', IP '10.0.81.40', Port 'ICMP', Source '10.0.81.40', Interface 'eth0', Destination '8.8.8.8', Output-IF 'vpn0@FW2FW...', and Rule 'B02-S2S-Internet'.

ID	State	IP ...	Port	Source	Interface	U...	Destination	Output-IF	A...	Out	Type	Rule
1761	Established	10.0.81.40	ICMP	10.0.81.40	eth0		8.8.8.8	vpn0@FW2FW...		1008...	FWD	B02-S2S-Internet

Local Firewall



The screenshot shows the 'FIREWALL > Live' interface of a local firewall. The 'Traffic Selection' dropdown is set to 'Forward, Local In, Local Out, IPv4, IPv6'. The 'Status Selection' dropdown is set to 'Closing, Established, Failing, Pending'. The 'Source' field is set to '10.0.81.40'. The table below shows a single entry with ID 14396, State 'Established', IP '10.0.81.40', Port 'ICMP', Source '10.0.81.40', Interface 'vpn0@FW2FW-VIRB02-VIRT1', Destination '8.8.8.8', Output-IF 'eth1', and Rule 'B02-2-INTERNET'.

ID	State	IP ...	Port	Source	Interface	U...	Destination	Output-IF	A...	Out	Type	Rule
14396	Established	10.0.81.40	ICMP	10.0.81.40	vpn0@FW2FW-VIRB02-VIRT1		8.8.8.8	eth1		2.5 K	FWD	B02-2-INTERNET

Troubleshooting

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

- **No traffic passes through the default route** – Verify that 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** – Use Dynamic NAT on the external CloudGen 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 CloudGen Firewall and that this default route points to a working Internet gateway.

Figures

1. s_to_s_default_rt.png
2. VPN_tunnel_firewall_internal_LAN.png
3. VPN_tunnel_firewall_with_internet_access.png
4. LAN-to-Internet-via-VPN.png
5. LAN-to-Internet.png
6. log_example_remote_fw.png
7. log_example_local_fw.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.