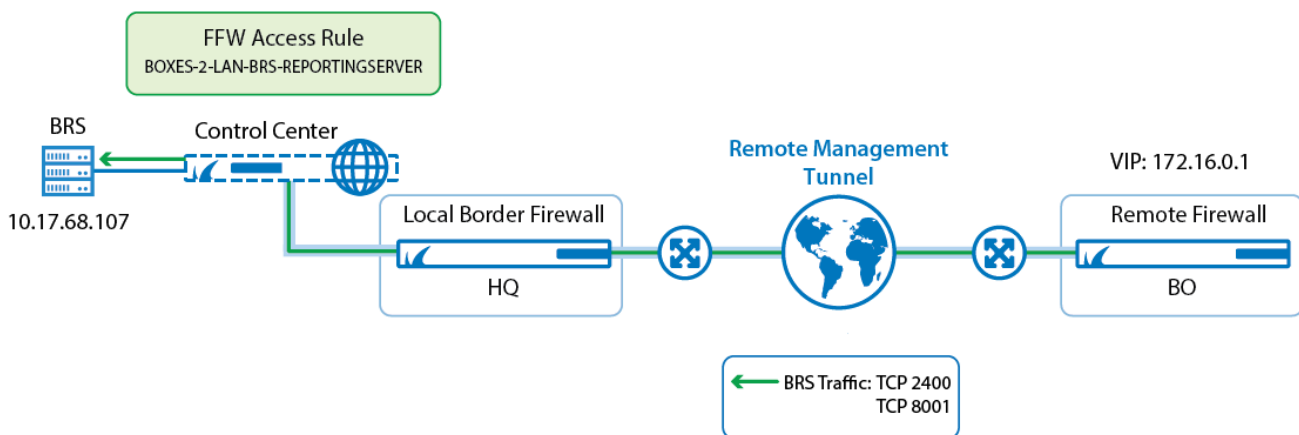


How to Stream Data to a BRS via a Remote Management Tunnel

<https://campus.barracuda.com/doc/78808982/>

In certain cases it can be necessary to stream data from a remote firewall to a Barracuda Reporting Server (BRS) that is located behind a local border firewall. In the following setup, streaming data is sent from a remote firewall through the remote management tunnel over the Internet and through the local border firewall to the Control Center, which forwards the traffic to the BRS.



Before You Begin

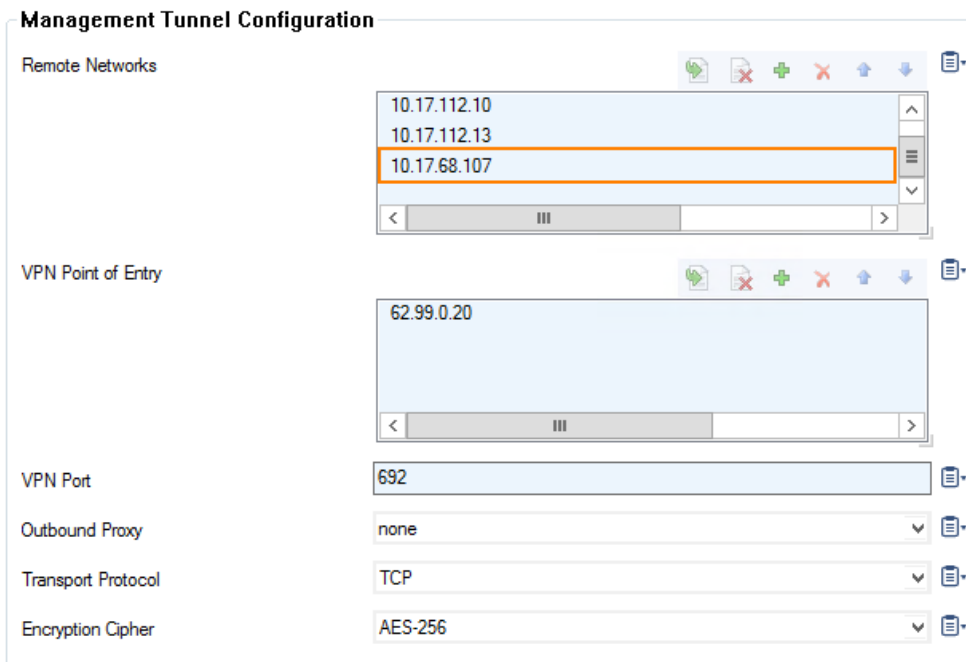
You must complete all necessary steps for the BRS integration. For more information, see [Barracuda Reporting Server \(BRS\) Integration](#).

- If you deploy a firewall via the Control Center with a default configuration set from firmware version 7.2, the service object 'BRS', the host access rule 'BOX-BRS-REPORTINGSERVER-MGMT-NAT' and the forwarding access rule 'BOXES-2-LAN-BRS-REPORTINGSERVER' are already preconfigured.
- If you migrate a stand-alone firewall to firmware version 7.2, these items are not preconfigured, and you must create them according to the following description.

Step 1. Add the BRS to the Remote Network Addresses for Tunnels

You must add the BRS to the remote network addresses list as a target in order to forward traffic through the management tunnel.

1. Go to **CONFIGURATION > Configuration Tree > Multi Range > your range > your cluster > your remote box > Network**.
2. In the left navigation bar, click **Management Access**.
3. Click **Lock**.
4. In the **Remote Management Tunnel** section, click **Show...** for **Tunnel Details**.
5. The **Tunnel Details** window is displayed.
6. Click **+** for **Remote Networks**.
7. Enter the IP address of the BRS to the list, e.g., 10.10.68.107.



Management Tunnel Configuration

Remote Networks

- 10.17.112.10
- 10.17.112.13
- 10.17.68.107

VPN Point of Entry

- 62.99.0.20

VPN Port

- 692

Outbound Proxy

- none

Transport Protocol

- TCP

Encryption Cipher

- AES-256

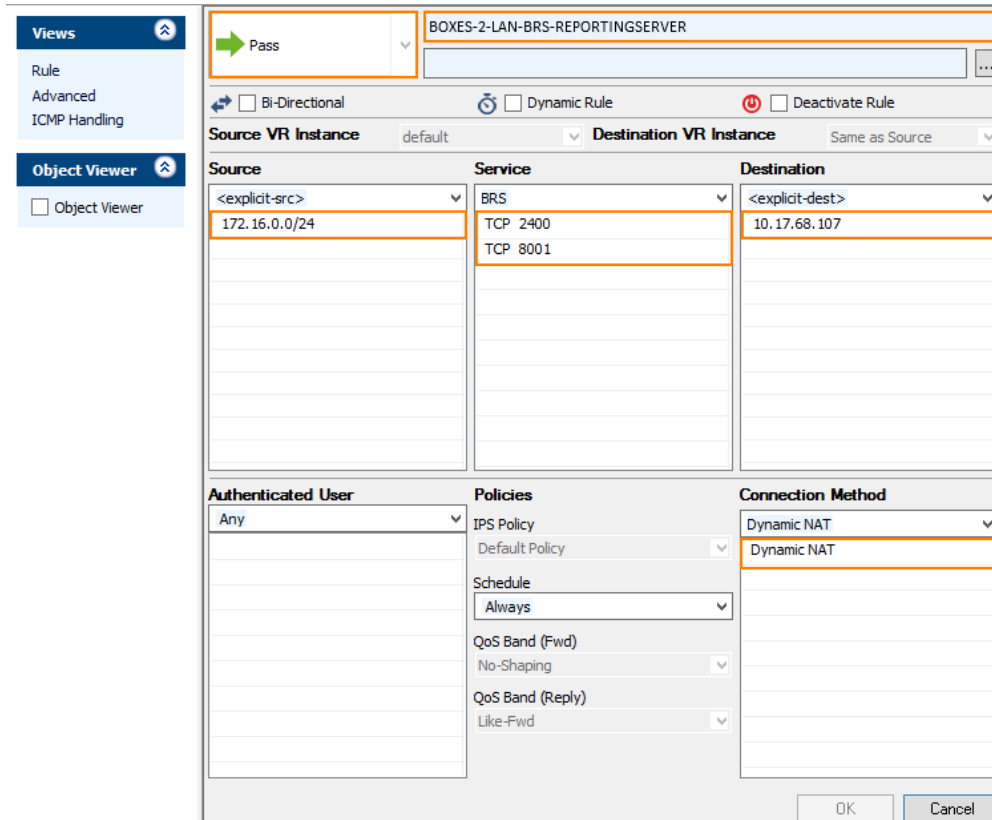
Step 2. On the Control Center, Allow BRS Traffic to the BRS by an Access Rule

If you have deployed both your local and remote border firewall with a default configuration set from firmware version 7.2 via the Control Center, the host access rule 'BOXES-2-LAN-BRS-REPORTINGSERVER' is already present and you can omit this step. However, you must activate the access rule 'BOXES-2-LAN-BRS-REPORTINGSERVER' in the list view for forwarding access rules.

To forward the BRS traffic from the Control Center to the BRS, you must create the following access rule:

1. Log into your Control Center on box level.
2. Go to **CONFIGURATION > Configuration Tree > Multi Range > Virtual Servers > Firewall > Forwarding Rules**.
3. Click **Lock**.
4. Click **+**.
5. Enter the values for the rule:

- **Connection Type** – Pass.
 - **Name** – BOXES-2-LAN-BRS-REPORTINGSERVER.
 - **Source** – Enter the address for the VIP net used for the remote managed firewall.
 - **Service** – Enter TCP 2400 and TCP 8001.
 - **Destination** – Enter the IP address for the BRS, e.g., 10.17.68.107.
 - **Connection Method** – Dynamic NAT.
6. Click **OK**.
 7. Click **Send Changes**.
 8. Click **Activate**.



The screenshot shows the configuration page for a rule named "BOXES-2-LAN-BRS-REPORTINGSERVER". The rule is set to "Pass" and is not bi-directional, dynamic, or deactivated. The source VR instance is "default" and the destination VR instance is "Same as Source".

Source	Service	Destination
<explicit-src>	BRS	<explicit-dest>
172.16.0.0/24	TCP 2400 TCP 8001	10.17.68.107

Additional configuration details:

- Authenticated User:** Any
- Policies:** IPS Policy (Default Policy), Schedule (Always), QoS Band (Fwd) (No-Shaping), QoS Band (Reply) (Like-Fwd)
- Connection Method:** Dynamic NAT

Buttons: OK, Cancel

The remote firewall can now stream data to the BRS via the remote management tunnel.

Figures

1. brs_01.1.png
2. brs_add_brs_to_rmts.png
3. brs_forward_traffic_cc_to_brs.png

© Barracuda Networks Inc., 2019 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.