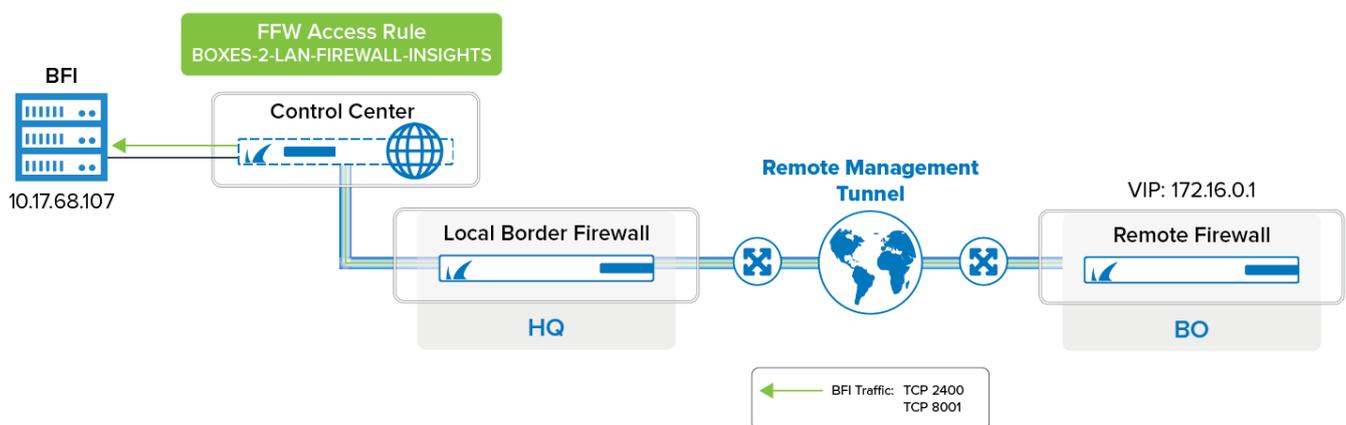


## How to Stream Data to Firewall Insights via a Remote Management Tunnel

<https://campus.barracuda.com/doc/96026567/>

In certain cases it can be necessary to stream data from a remote firewall to a Barracuda Firewall Insights device 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 Firewall Insights.



### Before You Begin

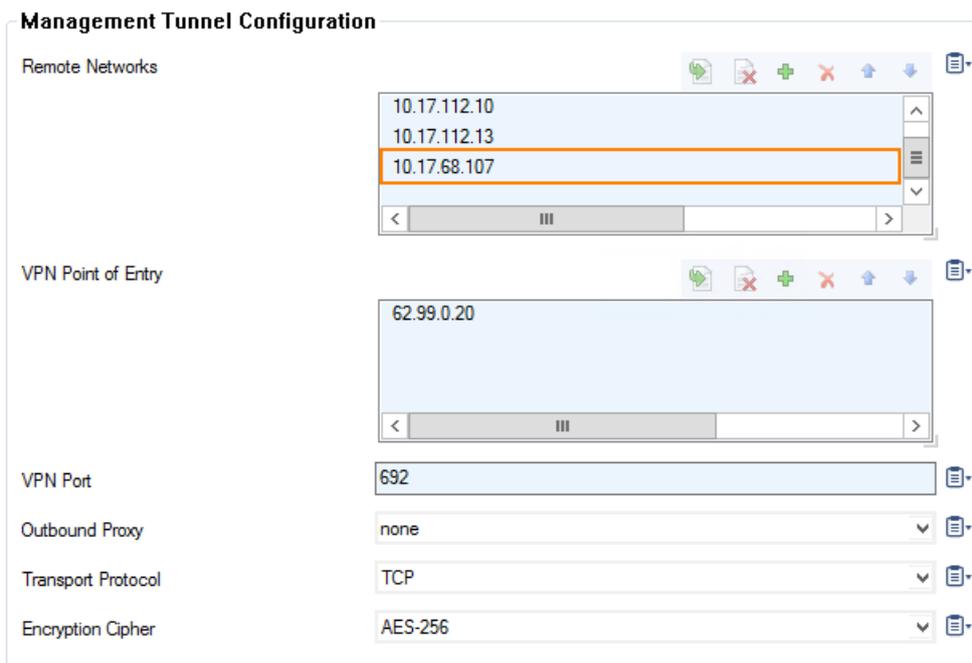
- You must complete all necessary steps for Firewall Insights integration. For more information, see [Barracuda Firewall Insights Integration](#).
- A remote management tunnel must be established. For more information, see [How to Configure a Remote Management Tunnel for a CloudGen Firewall](#).
- If you deploy a Control Center with a default configuration set from firmware version 8.0.1, the service object 'FIREWALL-INSIGHTS', the network object 'Firewall Insights' and the forwarding access rule 'BOXES-2-LAN-FIREWALL-INSIGHTS' are already preconfigured. You can therefore skip those steps.
- If you migrate a Control Center to firmware version 8.0.1, these items are not preconfigured, and you must create them according to the following description.

The Remote Firewall, the Border Firewall and the Control Center must have installed firmware version 8.0.1 or higher.

## Step 1. On the Remote Firewall, Add Firewall Insights to the Remote Network Addresses for Tunnels

You must add Firewall Insights 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 > Boxes > your remote box > Network.**
2. In the left navigation bar, click **Management Access.**
3. Click **Lock.**
4. In the **Remote Management Tunnel** section, click **Edit...** next to **Tunnel Details.**
5. The **Tunnel Details** window is displayed.
6. Click **+** in the **Remote Networks** section.
7. Enter the IP address of Firewall Insights to the list, e.g., **10.17.68.107**



The screenshot shows the 'Management Tunnel Configuration' window. It has several sections:

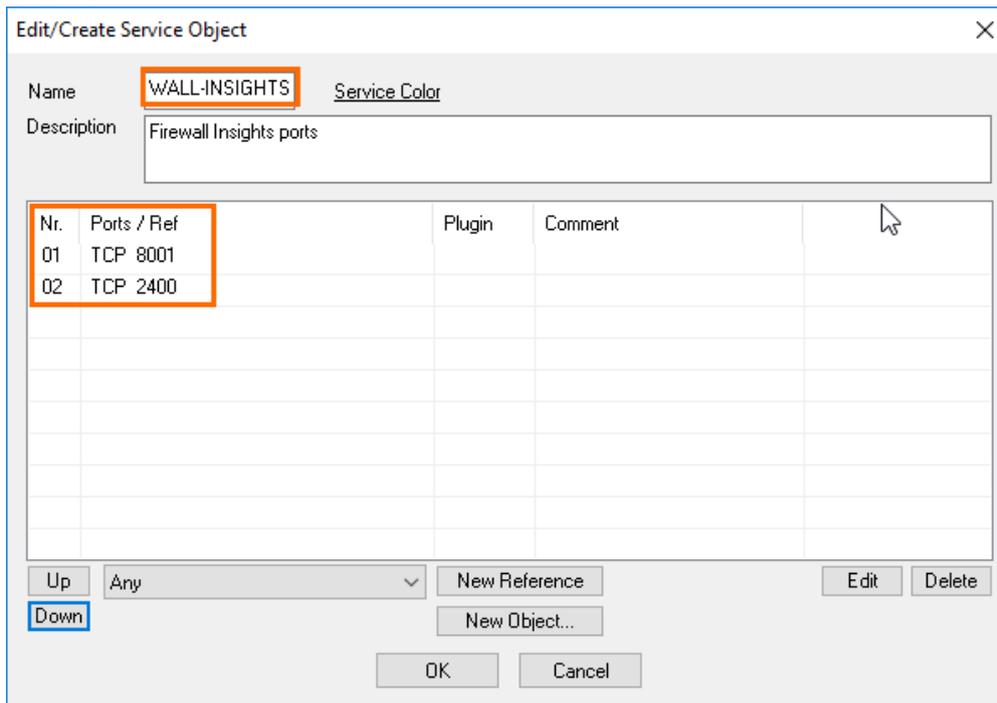
- Remote Networks:** A list of IP addresses: 10.17.112.10, 10.17.112.13, and 10.17.68.107. The last one is highlighted with an orange border.
- VPN Point of Entry:** A single IP address: 62.99.0.20.
- VPN Port:** A text input field containing '692'.
- Outbound Proxy:** A dropdown menu set to 'none'.
- Transport Protocol:** A dropdown menu set to 'TCP'.
- Encryption Cipher:** A dropdown menu set to 'AES-256'.

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

## Step 2. (Optional, only if not preconfigured) On the Control Center, Create Service Object Firewall-Insights

1. Log into your Control Center on box level.
2. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > CCFW (Firewall) > Forwarding Rules**

3. In the left navigation bar, click **Services**
4. Click **Lock**.
5. In the right section where the services are displayed, right-click and select **New**.
6. The **Edit/Create Service Object** window is displayed.
7. Enter the **Name** for the service object, e.g., FIREWALL - INSIGHTS.
8. Enter Firewall Insights ports for **Description**.
9. Click **New Object...**
10. The Service Entry Parameters window is displayed.
11. Verify that 006 TCP is selected for **IP Protocol**.
12. For **Port Range**, enter 2400.
13. Click **OK**.
14. Click **New Object...**
15. The Service Entry Parameters window is displayed.
16. Verify that 006 TCP is selected for **IP Protocol**.
17. For **Port Range**, enter 8001.
18. Click **OK**.



Edit/Create Service Object

Name: WALL-INSIGHTS    Service Color:

Description: Firewall Insights ports

Nr.	Ports / Ref	Plugin	Comment
01	TCP 8001		
02	TCP 2400		

Up    Any    New Reference    Edit    Delete

Down    New Object...

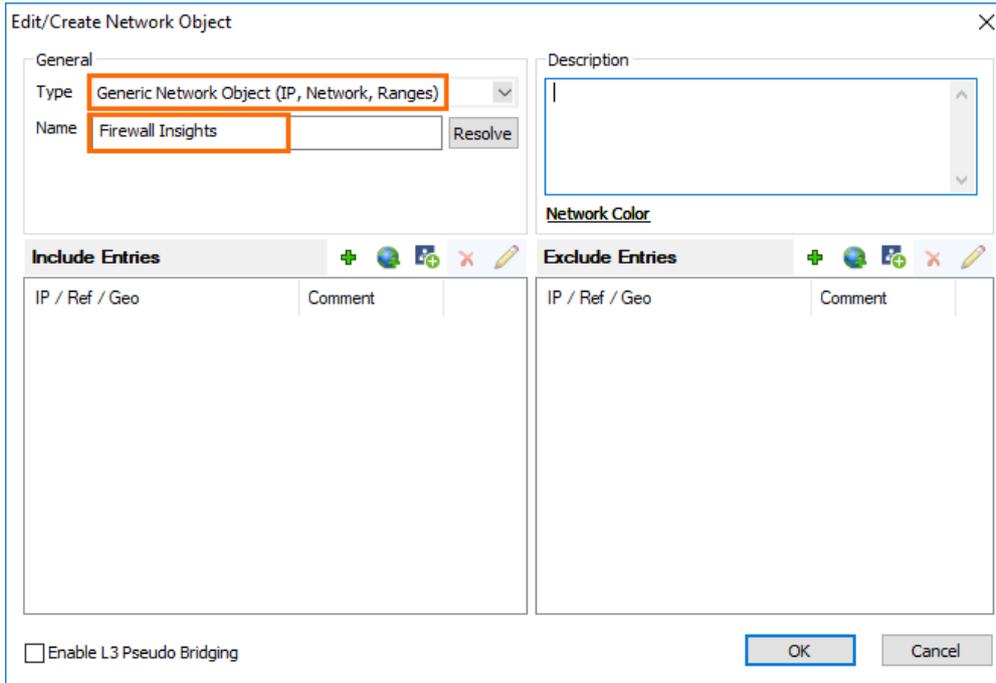
OK    Cancel

19. Click **Send Changes** and **Activate**.

### Step 3. (Optional, only if not preconfigured) On the Control Center, Create Network Object Firewall Insights

1. Log into your Control Center on box level.
2. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > CCFW (Firewall) > Forwarding Rules**

3. In the left navigation bar, click **Networks**.
4. Click **Lock**.
5. In the right section where the networks are displayed, right-click and select **New**.
6. The **Edit/Create Network Object** window is displayed.
7. For **Type** select **Generic Network Object (IP, Network, Ranges)**.
8. Enter Firewall Insights for the name.
9. Click **OK**.

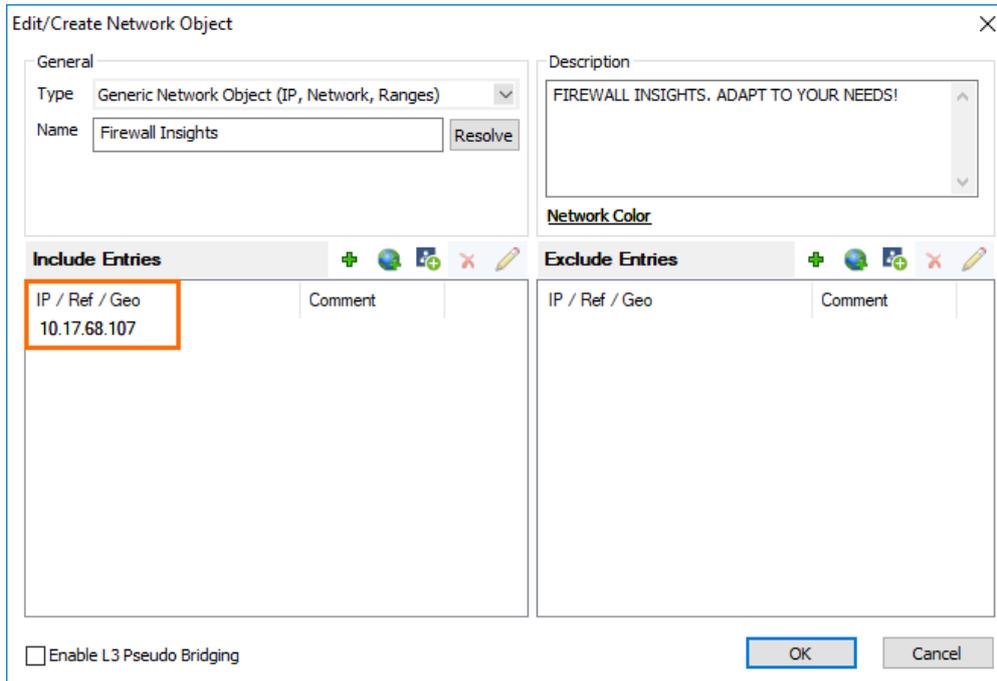


The screenshot shows the 'Edit/Create Network Object' dialog box. The 'General' section has 'Type' set to 'Generic Network Object (IP, Network, Ranges)' and 'Name' set to 'Firewall Insights'. The 'Description' field is empty. Below the 'General' section are two tables: 'Include Entries' and 'Exclude Entries', both of which are empty. At the bottom, there is a checkbox for 'Enable L3 Pseudo Bridging' which is unchecked, and 'OK' and 'Cancel' buttons.

10. Click **Send Changes** and **Activate**.

#### Step 4. On the Control Center, Enter the IP Address of Firewall Insights in the Network Object Firewall Insights

1. Log into your Control Center on box level.
2. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > CCFW (Firewall) > Forwarding Rules**
3. In the left navigation bar, click **Networks**.
4. Click **Lock**.
5. In the right section where the networks are displayed, double-click **Firewall Insights**.
6. The **Edit/Create Network Object** window is displayed.
7. If the IP address 0.0.0.0 is entered, click the **x** to remove it.
8. Click **+** to enter the IP address of your Firewall Insights device, e.g., 10.17.68.107.
9. Click **Insert and Close**.
10. Click **OK**.



11. Click **Send Changes** and **Activate**.

### Step 5. (Optional, only if not preconfigured) On the Control Center, Allow Firewall Insights Traffic to Firewall Insights by an Access Rule

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

1. Log into your Control Center on box level.
2. Go to **CONFIGURATION > Configuration Tree > Multi Range > Assigned Services > CCFW (Firewall) > Forwarding Rules**
3. Click **Lock**.
4. Click **+**.
5. Enter the following values for the rule:
  - o **Connection Type** - Pass.
  - o **Name** - BOXES-2-LAN-FIREWALL-INSIGHTS.
  - o **Source** - Select any from the drop-down menu.
  - o **Service** - Select FIREWALL-INSIGHTS from the drop-down menu.
  - o **Destination** - Select Firewall-Insights from the drop-down menu.
  - o **Connection Method** - Select Original Source IP from the drop-down menu.
6. Click **OK**.

**Edit Rule: BOXES-2-LAN-FIREWALL-INSIGHTS [Rule]**

Views: Rule, Advanced ICMP Handling, Object Viewer (checked)

Action: **Pass** (Allows limited LAN access from managed firewalls to Firewall Insights.)

Options:  Bi-Directional,  Dynamic Rule,  Deactivate Rule

Source VR Instance: default | Destination VR Instance: default

Source	Service	Destination
Any 0.0.0.0/0	FIREWALL-INSIGHTS TCP 8001 TCP 2400	Firewall Insights 10.17.68.107

Authenticated User: Any

Policies: IPS Policy: No Scan, Schedule: Always, QoS Band (Fwd): VoIP (ID 2), QoS Band (Reply): Like-Fwd

Connection Method: Original Source IP (same port)

Buttons: OK, Cancel

7. Click **Send Changes** and **Activate**.

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

## Figures

1. bfi\_remote.png
2. brs\_add\_brs\_to\_rmts.png
3. bfi\_service\_ports.png
4. bfi\_network.png
5. bfi\_network\_ip.png
6. bfi\_cc\_fw\_rule.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.