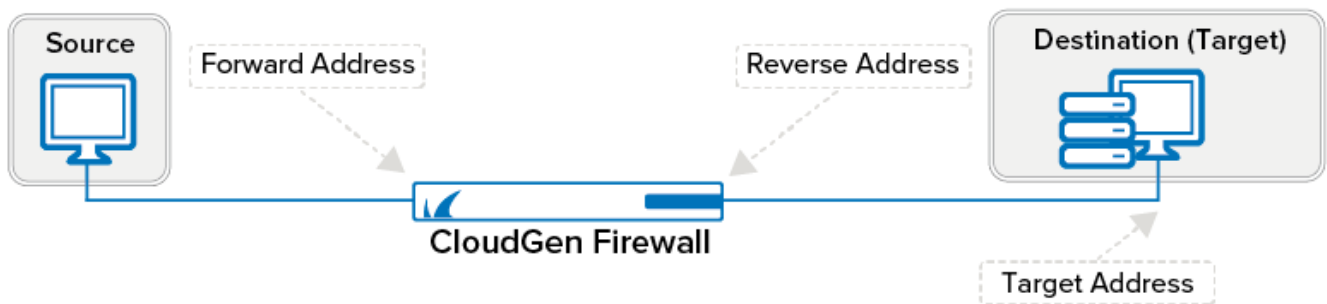


How to Configure ICMP Settings

<https://campus.barracuda.com/doc/98210245/>

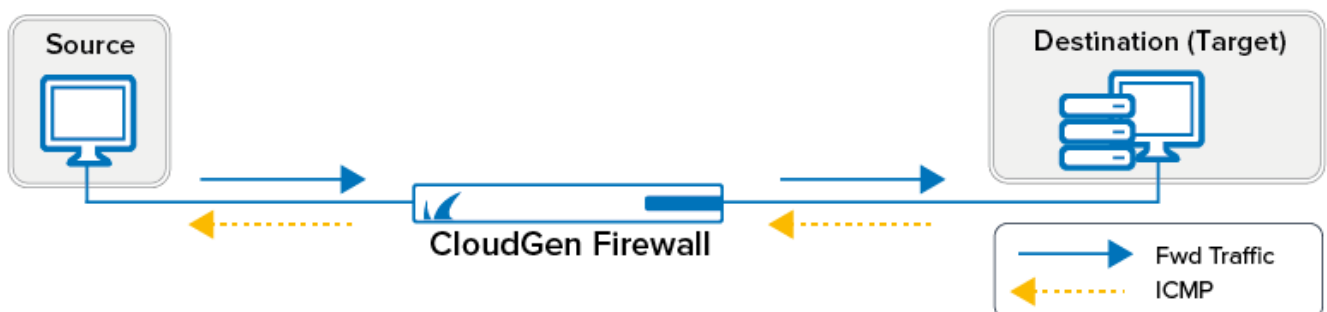
ICMP (Internet Control Message Protocol) is used for diagnostic or control purposes. Network devices send one of the 24 ICMP errors directed at the source IP of a packet, for example, to let the source device know that it is currently not available or the desired destination cannot be reached. The Barracuda CloudGen Firewall uses the following terms to describe the IP addresses involved in an ICMP reply:

Forward / Reverse / Target IP Addresses



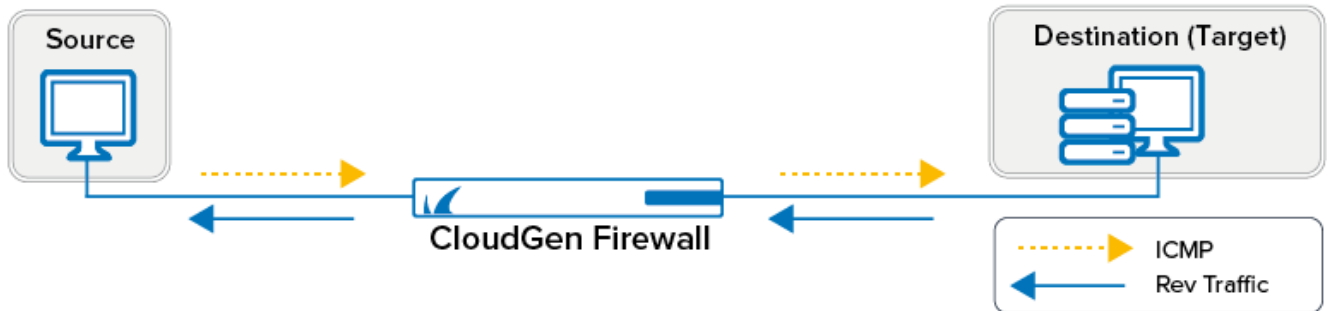
Forward Policy

The forward policy affects ICMP messages that are caused by traffic from the source to the destination.



Reverse Policy

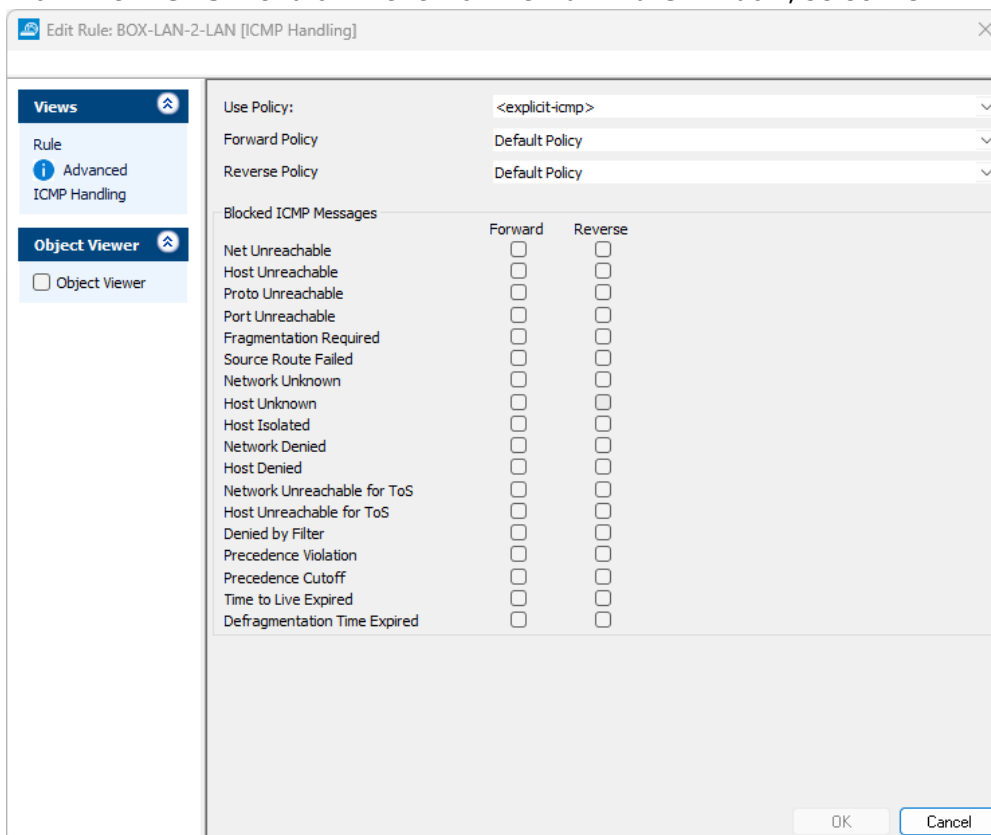
The reverse policy affects ICMP messages that are caused by traffic from the destination back to the source.



Configure ICMP Handling Policy

ICMP handling policy is configurable per firewall rule:

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. From the **Views** menu on the left of the **Edit Rule** window, select **ICMP Handling**.



The screenshot shows the 'Edit Rule: BOX-LAN-2-LAN [ICMP Handling]' window. On the left, the 'Views' menu is expanded, showing 'Rule', 'Advanced', 'ICMP Handling', and 'Object Viewer'. The 'ICMP Handling' view is selected. The main area displays the following configuration:

Use Policy:	Forward Policy	Reverse Policy
<explicit-icmp>	Default Policy	Default Policy

Below this, there is a section for 'Blocked ICMP Messages' with two columns: 'Forward' and 'Reverse'. Each column contains a list of ICMP message types with checkboxes for blocking them.

Blocked ICMP Messages	Forward	Reverse
Net Unreachable	<input type="checkbox"/>	<input type="checkbox"/>
Host Unreachable	<input type="checkbox"/>	<input type="checkbox"/>
Proto Unreachable	<input type="checkbox"/>	<input type="checkbox"/>
Port Unreachable	<input type="checkbox"/>	<input type="checkbox"/>
Fragmentation Required	<input type="checkbox"/>	<input type="checkbox"/>
Source Route Failed	<input type="checkbox"/>	<input type="checkbox"/>
Network Unknown	<input type="checkbox"/>	<input type="checkbox"/>
Host Unknown	<input type="checkbox"/>	<input type="checkbox"/>
Host Isolated	<input type="checkbox"/>	<input type="checkbox"/>
Network Denied	<input type="checkbox"/>	<input type="checkbox"/>
Host Denied	<input type="checkbox"/>	<input type="checkbox"/>
Network Unreachable for ToS	<input type="checkbox"/>	<input type="checkbox"/>
Host Unreachable for ToS	<input type="checkbox"/>	<input type="checkbox"/>
Denied by Filter	<input type="checkbox"/>	<input type="checkbox"/>
Precedence Violation	<input type="checkbox"/>	<input type="checkbox"/>
Precedence Cutoff	<input type="checkbox"/>	<input type="checkbox"/>
Time to Live Expired	<input type="checkbox"/>	<input type="checkbox"/>
Defragmentation Time Expired	<input type="checkbox"/>	<input type="checkbox"/>

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

3. In the **Use Policy** drop-down field, select one of the following options:

- **Default Policy** – The default policy decides automatically whether to use forward or target address:
 - **With NAT** – The forward address is used (no internal IP address is visible).
 - **Without NAT** – The target address is used.
 - **NO ICMP AT ALL** – Block all ICMP settings.
 - **Use Forward Address** – The forward address is used for ICMP messages.
 - **Use Reverse Address** – The reverse address is used for ICMP messages.
 - **Use Target Address** – The target address is used for ICMP messages.
4. Select which replies are blocked in the **BLOCKED ICMP Messages** section.
- To configure a policy template, select **New ICMP Param Object** in the **ICMP** tab of the **Object Viewer**.
5. Click **OK**.
6. Click **Send Changes** and **Activate**.

Figures

1. fw_icmp01.png
2. fw_icmp02.png
3. fw_icmp03.png
4. icmp_01.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.