

## Example - Blocking ICMP Traffic

<https://campus.barracuda.com/doc/14319828/>

If you use the default rule set, all traffic is allowed from the LAN to the Internet. If you keep the rules that include the parameter **Service** set to **Any**, you might want to add access rules that **BLOCK** or **RESET** traffic with specific profiles. For example, you can deny specific service types or traffic from certain users. Using **BLOCK** causes the Barracuda NextGen Firewall X-Series to simply not respond to the connection request. The source client will then receive a timeout. To actively deny access, select **RESET**. The connection is then closed by the X-Series Firewall as soon as a connection attempt is made.

This article provides an example of how to configure an access rule that blocks all ICMP traffic from the local LAN to the Internet.

### Step 1. Create an Access Rule to Block ICMP Traffic

1. Go to the **FIREWALL > Firewall Rules** page.
2. Click **Add Access Rule** to create a new access rule.
3. In the **Add Access Rule** window, enter a name and description for the rule.
4. Specify the following settings:

Action	Source	Network Services	Destination
Block	Trusted LAN	ICMP	Internet


  

**ADD ACCESS RULE**
Help

General

ADVANCED

Action: Block



DNAT (port forwarding) - Redirect traffic to a specific IP address.  
 Redirect to Service - Redirect traffic to a service on the Barracuda Firewall.  
 Bi-directional - Source and destination networks are interchangeable.

Name: BlockICMP-Traffic

Description:

Connection: Default (SNAT)
 

Adjust Bandwidth: Internet

Bi-directional: ☐ Yes ☒ No
 

Disable: ☐ Yes ☒ No

IPS: ☒ Yes ☐ No

Application Control: ☐ Yes ☒ No
 

URL Filter: ☐ Yes ☒ No

Virus Protection: ☐ Yes ☒ No

SSL Inspection: ☐ Yes ☒ No

SOURCE

Help

Internet

+

Ref: Trusted LAN

-

☒ Network Objects
 ☐ IP Address
 ☐ Geo Loc.

NETWORK SERVICES

Help

HTTPS

+

ICMP

-

☒ Network Objects
 ☐ IP Address
 ☐ Geo Loc.

DESTINATION

Help

Any

+

Ref: Internet

-

☒ Network Objects
 ☐ IP Address
 ☐ Geo Loc.

5. At the top of the **Add Access Rule** window, click **Save**.

## Step 2. Verify the Order of the Access Rules

---

New rules are created at the bottom of the firewall rule set. Rules are processed from top to bottom in the rule set. Drag your access rule to a slot in the rule list so that no access rules before it matches this traffic. Verify that your rules are placed above the BLOCKALL rule. Otherwise, the rule never matches.

After adjusting the order of rules in the rule set, click **Save**.

## Figures

1. block\_icmp.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.