How To Create Bidirectional Static NAT Rule

27 April 2011

softwareblades™

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.
Important Information

**Latest Software**

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

**Latest Documentation**

The latest version of this document is at: [http://supportcontent.checkpoint.com/documentation_download?ID=12115](http://supportcontent.checkpoint.com/documentation_download?ID=12115)

For additional technical information, visit the Check Point Support Center ([http://supportcenter.checkpoint.com](http://supportcenter.checkpoint.com)).

**Revision History**

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/17/2011</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

**Feedback**

Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments ([mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on How To Create Bidirectional Static NAT Rule](mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on How To Create Bidirectional Static NAT Rule)).
How To Create Bidirectional Static NAT Rule

Objective

This document demonstrates how to create a bidirectional static NAT rule.

Supported Versions

- R60-R75

Supported OS

- SecurePlatform, IPSO, Solaris, Crossbeam, Linux, Windows

Supported Appliances

- Any
Before You Start

Related Documentation and Assumed Knowledge

- Firewall Admind Guide, Smartcenter Admin guide

Impact on the Environment and Warnings

- If the NAT is set incorrectly, Other NATed connections could be affected by the improper rule
Background Information

This section explains Automatic and Manual NAT rule Methods.

In this section:

- Automatic NAT Rules
- Manual NAT Rules

Automatic NAT Rules

When NAT is defined for a network object, an automatic NAT rule is generated which performs the required translation. If there are two such objects and one is the source of a connection and the other the destination, then without Bidirectional NAT, only one of these objects will be translated, because only one of the automatically generated NAT rules will be applied, and so a connection between the two objects will only be allowed in one direction. With Bidirectional NAT, both automatic NAT rules are applied, and both objects will be translated, so connections between the two objects will be allowed in both directions.

Marking the Allow bi-directional NAT checkbox in the Global Properties > NAT window, applies to automatic NAT rules in the NAT Rule Base, and allows two automatic NAT rules to match a connection. Without Bidirectional NAT, only one automatic NAT rule can match a connection.

Bidirectional Static NAT

When dealing with a bidirectional Static NAT rule you must remember to use Static NAT only. Hide NAT will not create a bidirectional rule.

With a bidirectional rule it is best to use a host object and not a network object. When using a network object you are creating a 1 to many scenario: i.e., if you use 12.12.10.1 as your Static IP and create a NAT rule for a Network object like 192.168.1.0, this in turn would place the static NAT on each IP address in the 192.168.1.0 range.

1. The easiest way to create a bidirectional Static NAT is with a combination of global properties settings and using an Automatic Static NAT for a specific Host object (if this NAT requires more than one object or a group then a manual NAT rule will be needed, Skip to the Manual NAT rule section).
2. Ensure that the appropriate options are configured in the policy, Global properties Section (see the screen shot below)

3. Edit your host object. The screen shot below shows the host object we are working with, when you select the NAT tab on the object you can change the drop-down menu to Static and set the proper IP

4. The screen shot below shows the automatic NAT rule that is created automatically when you set the option on the host object. Now you cannot modify the Automatic NAT rule. This in turn makes the automatic NAT an "Any" rule for the host object. If you need to specify specific services or group of services you will need to create a manual NAT rule.
Manual NAT Rules

All manual NAT rules must be placed above any Automatic NAT rule.

To create a manual NAT rule:
1. Select the NAT tab.
2. Inside the NAT tab, add your first part of the Bidirectional NAT rule (If there is no Manual NAT rule you will need to add the rule by selecting Rules from the menu list and then select Add Rule and then Select Top).

NAT Rule Creation Procedure

Say you have a Web server (its internal IP is: 192.168.15.254), and you need to assign an External Routable IP Address to it, and your EXT address is 12.12.10.1.

- You will need 2 host objects:
  - One with the internal IP - 192.168.15.254
  - The other with the EXT IP - 12.12.10.1
- You want the server to access and be accessed by the Internet but only to do the NAT on HTTP and HTTPS

In the first rule you create you will allow the source of Any address to the EXT IP address with your HTTP and HTTPS service’s listed (this part is in the Original packet section).

Then you will modify the Translated packet section, Here you will leave the source as original but change the destination to the internal IP of the web server setting it as a static NAT and leaving the service original.

Once the above rule is in place you can now create a second rule below it. This new rule will be the reverse of rule 1 in turn creating a bidirectional NAT. The source in this new rule will be your web server’s internal IP with a destination of any and a service of HTTP (if you wish to restrict the NAT to HTTP). On the second part in the Translated packet section you will change the source to the Web server’s EXT IP as a static IP with the Destination and service staying original.
Manual Static NAT:

If for whatever reason you are unable to create Automatic Static NAT rules, then the only way that you can get this "Manual Static NAT" working is with a local.arp file.

This local.arp file is located in:

- `$FWDIR/conf` directory on Linux/SecurePlatform
- `%FWDIR%\conf` directory on Windows

The file must have the following syntax:

- Ext NAT’d IP and the Ext MAC address of the firewall performing the NAT, one entry per line.
- Ex. 75.5.4.33 00:09:34:4d:3f:ad
- The entry must be in correct format (use ifconfig output as reference for MAC addr).
- If this file does not exist, create it and then reboot the gateway in question for the file to be recognized correctly.
- Any changes made to this file should work with a policy install.

Completing the Procedure

A Policy push is required to complete the NAT rule.

Verifying

Test the NAT rule, Smartview Tracker can be used to view the accepted traffic and to see if the Source or Destination was NAT’d.