How To Configure Policy Based Routing

24 April 2012
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=12298
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/24/2012</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 Configure Policy Based Routing).
# Important Information

How to Configure Policy Based Routing (PBR)

<table>
<thead>
<tr>
<th>Objective</th>
<th>How can Policy Based Routing (PBR) be useful in a network?</th>
<th>Supported Versions</th>
<th>Supported OS</th>
<th>Supported Appliances</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Before You Start</td>
<td>Related Documentation and Assumed Knowledge</td>
<td>Impact on the Environment and Warnings</td>
<td>Is PBR supported on VRRP &amp; IPSO-Clustering?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration</td>
<td>Configure the Policy Based Routing (PBR) Table</td>
<td>Configure the Access Lists (ACL)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Completing the Procedure</td>
<td></td>
<td></td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Verifying</td>
<td></td>
<td></td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Index</td>
<td></td>
<td></td>
<td>13</td>
<td></td>
</tr>
</tbody>
</table>
How to Configure Policy Based Routing (PBR)

Objective

The objective of this document is to give you the ability to exert detailed control over the traffic forwarding mechanism of IPSO. This feature was introduced in IPSO 4.2 – 069 and later.

Policy Based Routing (PBR) lets you create routing tables that enable IPSO to direct traffic to appropriate destinations by using an Access Control List (ACL) to filter the traffic based on one or more of the following:

- Source address
- Source mask length
- Destination address
- Destination mask length
- Source port
- Destination port
- Protocol type

How can Policy Based Routing (PBR) be useful in a network?

Based on the above description, PBR can be used to direct traffic based on where it is from (this may include single hosts to entire networks) to where it is going and it can even be granular enough to filter that traffic based on specific ports (services). This greatly improves the control that network administrators have in regards to the routing of traffic through a network. For example, a company may want all http traffic to use a certain route instead of using the default gateway or traffic from certain hosts or segments to take a route other than the default route.

It should be noted that the Access Control List (ACL) which is implemented in PBR takes precedence over the standard IPSO routing. This means that the last rule in the ACL should always be an ‘accept’ rule to allow any traffic not affected by PBR to pass through the standard IPSO routing.

Supported Versions

This is an OS dependent feature and is not impacted by the Firewall version.

Supported OS

- IPSO 4.x
- IPSO 6.x

Supported Appliances

This document only relates to IP appliances.
Before You Start

Related Documentation and Assumed Knowledge

Review these SK articles and documents for reference information:

- sk44420 (http://supportcontent.checkpoint.com/solutions?id=sk44420)
- sk38637 (http://supportcontent.checkpoint.com/solutions?id=sk38637)
- sk44399 (http://supportcontent.checkpoint.com/solutions?id=sk44399)
- sk39204 (http://supportcontent.checkpoint.com/solutions?id=sk39204)
- sk44520 (http://supportcontent.checkpoint.com/solutions?id=sk44520)
- Voyager Reference Guide

Impact on the Environment and Warnings

Policy Based Routing (PBR) can be configured via Voyager as well as via the CLI. The configuration process contains two parts:

- Configuring the PBR Table
- Configuring the ACL

Is PBR supported on VRRP & IPSO-Clustering?

PBR is supported on both VRRP & IPSO-Clustering. However, the configuration of the PBR Table and the ACLs vary slightly in different configurations:

- To use PBR in a VRRP configuration, you must configure PBR and the ACL on the master and backup nodes.
- With IP clustering, you can use Cluster Voyager to configure PBR (so that you configure it only once), but you must configure an ACL on the individual nodes.
- If you use PBR with IP clustering in forwarding mode, apply the PBR ACL on the cluster protocol network interfaces.
Configuration

Before you configure PBR, make sure that the Firewall has been configured and is working.

Configure the Policy Based Routing (PBR) Table
2. Enter a name for the Policy Based Routing (PBR) table (for example, ISP1).
3. Click Apply/Save.
4. Enable the Default Gateway option by clicking the on option.
5. Click **Apply/Save**.

8. Enter the Gateway Address.

6. From the **Gateway Type** list, select address.

7. Click **Apply/Save**.

8. Enter the Gateway Address.
9. Click **Apply/Save**.

   ![Policy Based Routing](image1)

   It is important to note at this point that the Gateway Address entered in Step 8 is the address of the upstream router for ISP1.

**Configure the Access Lists (ACL)**

1. Open **Voyager > Configurations > Traffic Management > Access List**.
2. Enter a name for the Access List (ACL) (for example, pbr_acl).
3. Click **Apply/Save**.

   ![Access List Configuration](image2)

   4. By default the **Bypass** option should be set to No. This is the option that must be set to for the Access List to be utilized.
5. Click on the name of the Access List to edit it.

6. Select the **Add Rule Before** check box.
7. Click **Apply/Save**.

8. Select **PBR** from the list in the **Action** column.

9. Click **Apply/Save**.
Completing the Procedure

For a company's requirements, you may need to split the internal network into two parts. Make sure that you enter the mask length in Step 11 accordingly. Also note that the system takes the path of the least restrictive matching ACL rule. Therefore, to make sure that all FTP traffic is routed through ISP1, place the FTP rule above the other rules.

Make sure that you use the appropriate destination port (FTP). Exclude this port from the port ranges of the other rules. Use this syntax: 0-21, 22-65535.

After you configure ISP1, configure similar ACLs for ISP2 and FTP. It is imperative that the last rule in the ACL be an 'Accept' rule that allows any traffic not affected by the ACL or PBR to be handed over to the standard IPSO routing process.

The last step in this procedure is to apply this ACL to an interface. From the Add Interface drop down menu, select an interface (for example, select the internal interface for which all traffic that enters this interface will be applied to PBR). Select Input from the Direction list after you select the internal interface. Once you complete the configuration, you can test it.

Verifying

Send traffic from different source IPs and run tcpdump to make sure it is working correctly.
Index

B
Before You Start • 6

C
Completing the Procedure • 12
Configuration • 7

H
How to Configure Policy Based Routing (PBR) • 5

I
Impact on the Environment and Warnings • 6
Important Information • 3

O
Objective • 5

R
Related Documentation and Assumed Knowledge • 6

S
Supported Appliances • 5
Supported OS • 5
Supported Versions • 5

V
Verifying • 12