How To Configure Netflow Services in IPSO 6.2

Technical Reference Guide

5 June 2011
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=12294
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>05 June 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 Configure Netflow Services in IPSO 6.2 Technical Reference Guide).
Important Information........................................................................................................3
Objective ..........................................................................................................................5
  Details ............................................................................................................................5
    Supported Versions .....................................................................................................5
    Supported OS ..............................................................................................................5
    Supported Appliances ..............................................................................................5
    Related Documentation and Assumed Knowledge ......................................................5
  Impact on the Environment and Warnings ..................................................................5
Configuring Netflow Services ..........................................................................................6
  Configuring ACL Mode ...............................................................................................7
  Configuring Netflow Collector ....................................................................................7
Troubleshooting ...............................................................................................................7
Objective

In this document we go through the steps of configuring Netflows in IPSO 6.2.

You can use the Netflow support in IPSO to collect data about network traffic patterns and volume. IPSO tracks network flows. A flow is a unidirectional stream of packets that share a given set of characteristics.

Details

Supported Versions

- IPSO 6.2 and higher

Supported OS

- IPSO 6.2 and higher

Supported Appliances

- All IP Appliances that support IPSO 6.2 and higher.

Related Documentation and Assumed Knowledge

- Network Voyager Reference Guide

Impact on the Environment and Warnings

When you enable flows mode, IPSO automatically reduces the concurrent connection capacity by 25%. If you later disable flows mode, IPSO automatically increases the connection capacity to the previous value. When you enable or disable this mode, you should make the same adjustment in Check Point SmartDashboard.
Configuring Netflow Services

To access the Netflow Configuration page:
1. Open Voyager.
2. Click Configuration > Traffic Management > Netflow.

<table>
<thead>
<tr>
<th>Netflow Configuration</th>
<th>Description</th>
<th>Valid Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collector IP</td>
<td>IP address of the Netflow data collector</td>
<td>Dotted-quad [0-255].[0-255].[0-255].[0-255] unicast address</td>
</tr>
<tr>
<td>Collector Port</td>
<td>Port number for the Netflow collector</td>
<td>1-65535</td>
</tr>
<tr>
<td>Source IP</td>
<td>IP address of the source IP in Netflow packets</td>
<td>Dotted-quad [0-255].[0-255].[0-255].[0-255] unicast address</td>
</tr>
<tr>
<td>Metering Mode ACL</td>
<td>Enable/Disable ACL metering mode</td>
<td>Supported only for non-ADP interfaces Default - disabled</td>
</tr>
<tr>
<td>Metering Mode Flows</td>
<td>Enable/Disable Flows metering mode</td>
<td>Default - disabled</td>
</tr>
<tr>
<td>Active Timeout</td>
<td>Active timeout to send Netflow records</td>
<td>1-3600 seconds Default - 1800</td>
</tr>
<tr>
<td>Inactive Timeout</td>
<td>Inactive timeout to send Netflow records</td>
<td>1-3600 seconds Default - 15</td>
</tr>
<tr>
<td>Export Format</td>
<td>Select a export format for the Netflow packets</td>
<td>None, Netflow_v5, Netflow_v9</td>
</tr>
</tbody>
</table>
Configuring ACL Mode

The most common use of Netflows is *Metering Mode Flows*. Metering mode analyzes data going through the appliance. In some configurations you want to analyze only data enforced on ACL rules.

**To configure ACL mode:**
1. Click **Configuration > Traffic Management > Access List**.
2. Select **Netflow Metering** for all ACLs on which Netflow will be enabled.
3. Click **Apply** and **Save**.

   **Note** - It is easy to forget to click **Apply** and **Save**. Make sure that you do so.

Configuring Netflow Collector

IPSO exports data about flows in flow records. To collect and analyze flow records, you must export them to a Netflow collector. Check Point has tested these collectors:

- Scrutinizer (Plixer International): supports Versions 5 and 9
- NetFlow Analyzer (AdventNet, Inc): supports Versions 5 and 9

Enter the IP address and application port number for your collector in the **Collector IP** and **Collector Port** fields.

Enter the source (local) IP address to be used in export flow records. If you do not define the Source IP, the IP address is chosen from the route to the collector's address.

Troubleshooting

- After you make sure that the configuration is correct, see the Collector software documentation.
- If you do not get reports do a `tcpdump` on the interfaces facing the Collector. For example: `tcpdump -i interface_name host ip_address_of_collector`
- Make sure that you see traffic destined for the collector coming from the firewall physical IP address. If you think that the firewall is dropign traffic, run: `fw ctl zdebug + drop > drop.txt` See if the output shows dropped communication between the firewall and the collector.
- Make sure that the firewall rulebase allows this communication.