How To Configure IPSO Clustering

27 August 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=16541
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>27 August 12</td>
<td>Updated cphaprob stat command</td>
</tr>
<tr>
<td>3 May 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 IPSO Clustering).

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>How To Configure IPSO Clustering</td>
<td>5</td>
</tr>
<tr>
<td>Objective</td>
<td>5</td>
</tr>
<tr>
<td>Supported Versions</td>
<td>5</td>
</tr>
<tr>
<td>Supported Operating Systems</td>
<td>5</td>
</tr>
<tr>
<td>Supported Appliances</td>
<td>5</td>
</tr>
<tr>
<td>Before You Start</td>
<td>5</td>
</tr>
<tr>
<td>Related Documents and Assumed knowledge</td>
<td>5</td>
</tr>
<tr>
<td>Impact on Environment and Warnings</td>
<td>5</td>
</tr>
<tr>
<td>Configuring IPSO Clustering</td>
<td>6</td>
</tr>
<tr>
<td>Verifying the Procedure</td>
<td>13</td>
</tr>
<tr>
<td>Improving Clustering Performance</td>
<td>13</td>
</tr>
</tbody>
</table>
How To Configure IPSO Clustering

Objective

This document explains how to configure IPSO Clustering on a pair (or more) of Check Point IP appliances.

Supported Versions

NGX R60 to R75.30

Supported Operating Systems

IPSO 4.0 to 6.2

Supported Appliances

Any IP appliance that supports IPSO.

Before You Start

- Make sure to use two IP appliances that are in the same mode, and have identical configuration and IPSO packages installed.
- Make sure your gateway pair has at least 3 configured interfaces with IPs.

Related Documents and Assumed knowledge

Nokia Network Voyager Reference Guide for IPSO 4.0
(http://supportcontent.checkpoint.com/documentation_download?ID=9095)/4.1
(http://supportcontent.checkpoint.com/documentation_download?ID=9097)/4.2
(http://supportcontent.checkpoint.com/documentation_download?ID=9844)/6.0
(http://supportcontent.checkpoint.com/documentation_download?ID=9308)/6.1
(http://supportcontent.checkpoint.com/documentation_download?ID=9932)/6.2

Impact on Environment and Warnings

- Make sure to use tested cables, and that the switch or switches are compatible with the type of IPSO clustering you configure. For example: Multicast.
- Make sure your cluster is fully functional in a lab environment before you use it in production.
- It is recommended to use the latest IPSO and Check Point versions:
  IPSO 6.2 Clustering Configuration Guide
  (http://supportcontent.checkpoint.com/documentation_download?ID=10294)
  R70 Installation and Upgrade Guide
Configuring IPSO Clustering

If the cluster is in service as soon as it becomes active, configure and enable NGX before you make the cluster active.

To Configure Check Point NGX for IPSO Clustering:
1. Make sure each cluster node uses exactly the same NGX version.
2. Make sure each node has exactly the same set of Check Point packages installed.
3. To configure NGX, run: cpconfig
4. Install NGX as an enforcement gateway (only) on each node.
5. When asked if you want to enable a Check Point cluster membership, select Yes.
6. Select to install a Check Point clustering product.
7. When prompted, reboot.
8. Resume cpconfig to finish the initial configuration of NGX.
9. When the option to enable Check Point SecureXL is available, do not select it.

To Create a Cluster:
In this example, a two member cluster is created.
1. Make sure a hostname is configured for this appliance and a host address entry with the same hostname and IP address is added. They must match the firewall object name and IP address exactly.
2. Make sure the date and time are synced to the time zone for both members and the management station.
3. Launch Voyager from the first gateway. This gateway is the Master.
4. In the Voyager tree view, select Configuration > High Availability > Clustering. The Clustering configuration window opens.
5. In the Cluster ID field, enter a number between 0-65535.
6. In the Cadmin Password field and in Verify Cadmin Password field, enter and re-enter the password.
7. Click Apply. A cluster is created.
8. To add the second gateway as a member:
   a) Launch Voyager from the gateway you want to add.
   b) In the Voyager tree view, select Configuration > High Availability > Clustering.
   c) In Join Existing IPSO Cluster, In the Cluster Member Address field, enter the IP address of the first gateway.
   d) Click Join. The cluster configuration is imported to the member.
   e) Activate the member.
If the import fails, repeat steps 4-7 (use the ID and password created then) and then click Manually Configure IPSO Cluster.
To Configure the Cluster:

1. Click Manually Configure IPSO Cluster.
2. Select from the Cluster Mode drop down list.
   If the routers and switches are on either side of the cluster support Multicast MAC addresses, you can select Multicast or Multicast with IGMP. If not, select Forwarding or Unicast.
3. In Work Assignment, select static or dynamic. For client to site VPNs, static is recommended.
4. Enter the details you choose in the Performance Rating and Failure Interval fields. For Cluster stability, increase the Failure Interval from the default 500 milliseconds to at least 4000.
5. To Configure the Cluster Interfaces (at least two, when one is configured as Primary Protocol Interface, and each with a cluster IP address), for each interface:
   a) In Interface Configuration, in the table, select the Select check box of the interface you want to include in the cluster.
   b) In the Cluster IP Address field, enter the IP address which must be in the same network as the IP address of the interface being configured.
c) For the interface that is to serve as the primary cluster protocol interface for the node, select the **Primary** check box.

   **Note** - The primary interfaces of all the cluster nodes must belong to the same network. This network should not carry any other traffic.

d) For the interface that is to serve as the secondary cluster protocol interface for the node, select the **Secondary** check box.

   **Note** - The secondary interfaces of all the cluster nodes must belong to the same subnet. This subnet should not carry any other traffic unless you use it to carry firewall synchronization traffic. Secondary interfaces are optional.

If you select **Multicast with IGMP** mode and do not want to use the default IP multicast group address, enter a new address in the range of 239.0.0.0 to 239.255.255.255.

6. In **FireWall related Settings**, select or clear the **Enable VPN-1/FW-1 Monitoring** check box:
   - If NGX operates on the node, enable the monitoring before you make the cluster active.
   - If NGX does not operate on the node, clear the monitoring before you make the cluster active (so that the cluster can be initialized). After the cluster is active, enable the monitoring so that the cluster monitors the firewall.

7. In the **Features to Share at Join Time** table, clear the check boxes of features that are not to be shared in the cluster.

8. In **Cluster Status**, in **Cluster State**, change the selection to **UP**.

9. Click **Save**.
To Configure the Cluster object in SmartDashboard:

1. In the SmartDashboard tree view, right click **Check Point**, and select **Security Cluster**. The **Gateway Cluster Properties** window opens.

2. In the **Network Security** tab, clear the **ClusterXL** check box.
3. In the window tree view, select **Cluster Members** and add the gateway objects.

4. A window that asks if you are sure you want to continue pops up. Click **Yes**.

5. Both gateways are added to the cluster object.
6. Select the 3rd Party Configuration tab, and in 3rd party solution, select IPSO IP Clustering.

7. Select Topology and get the topology from all the members. That includes Cluster Topology.
8. Make sure the cluster topology shows the correct IP addresses. All cluster interfaces should be set as Cluster.
9. Both cluster member objects show in the cluster object.


11. If the **VPN-1/FW-1 Monitoring** check box in step 6 of To Configure the Cluster is clear, select it.

### Verifying the Procedure

- To check the interfaces, from the command line of both gateways, run: `ifconfig -a`
  
  The master shows all the interfaces. The clustered interfaces have two IPs, an interface IP, and a Cluster virtual IP address with VIP MAC.
  
  **Note** - Since this is Forwarding mode, and only the cluster master responds to ARP requests, the member only shows `noarp` for the clustered interfaces. For example:
  ```
  ```

- To check IPSO Clustering status, on both members, run: `clish` and then `show clusters`

- To confirm Check Point state sync is operational, run: `cphaprof stat`
  
  The output should show that both members are active.

  OR

  Log into Voyager and from the tree view, select **Clustering Monitor**.

### Improving Clustering Performance

- IP Clustering provides both High Availability and scalability. IP Clustering is useful when the performance of one system alone is insufficient to provide the desired level of performance. For example, when an Appliance CPU reaches ~30%, it is recommended to add another Appliance to form a two-member cluster that can scale the firewall performance.

- IP Clustering is especially beneficial when you use SmartDefense features. With all SmartDefense features enabled, a two-member cluster HTTP transaction rate is about 40% higher than a standalone Appliance.

- Use dedicated interfaces for cluster protocol networks and state synchronization. Do not share interfaces with the production traffic.

- It is strongly recommended to use separate interfaces for cluster protocol network and firewall synchronization traffic so that they are separate broadcast domains.

- Use a bandwidth of at least 100 Mbps full duplex for IPSO sync interface(s). 1Gb is recommended.

- Use switches, not hubs, and never use crossover cables for IP Clustering protocol networks.
• Do not use IP Clustering Forwarding Mode when performance is a concern. Unicast and Multicast provide better performance and less latency. Forwarding Mode is a fallback mode, for when feature-poor network switches are in use.

• If IGMP snooping is in use on the switch, use Multicast with IGMP instead of Multicast.

• Use dynamic cluster work assignment for optimum load balancing. This allows the cluster to move active connections between nodes to periodically rebalance the load.

• Use delayed synchronization if your system processes many short lived connections and SXL templates are in use. A 30 second delay in connections synchronization can boost the performance by about 20%. If you use Check Point delayed notifications, you must also enable SecureXL delayed notifications.