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=12153
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>5/9/2011</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 State Sync on IPSO Redundant Links).
Contents

Important Information ................................................................. 3
How To Configure State Sync on IPSO Redundant Links .................. 5
Before You Start ........................................................................... 5
Configuring Check Point State Sync on IPSO Redundant Links ........ 6
    State sync with Cross-over Cables on the IPSO redundant links ...... 6
    State Sync with a Switch Environment and IPSO Redundant Links .... 6
    Configuring the Switches ......................................................... 7
    Configuring the Firewalls .......................................................... 8
    Configure the State Sync Network in SmartDashboard .................. 12
Completing the Procedure .............................................................. 12
Verifying ..................................................................................... 13
How To Configure State Sync on IPSO Redundant Links

Objective
This document explains how to configure Check Point State Synchronization on IPSO Redundant Links.
- The intention of this procedure is to establish state sync resilience without needing to configure a second state synch network. This avoids potential issues with VRRP or cluster stability.

Supported Versions
- Version NGX R65 and higher

Supported OS
- IPSO 4.2 and IPSO 6.2

Supported Appliances
- Check Point IP Appliances (formerly Nokia IP Security Series)

Before You Start

Related Documentation and Assumed Knowledge
- Knowledge of configuring clusters in Voyager and VPN-1, and firewall and switch administration skills.
- For information on configuring clusters, search the Check Point Support Center: https://supportcenter.checkpoint.com/supportcenter/index.jsp

Impact on the Environment and Warnings
- Failure to properly follow the instructions in this document could lead to a failure of state synchronization. If fail over happens when state synchronization is not working, connections through the cluster will break.
- Configuring multiple state sync networks (such as a 1st sync network and a 2nd sync network) can cause VRRP or cluster instability.
Configuring Check Point State Sync on IPSO Redundant Links

Using IPSO redundant links, the state sync network between the cluster members can be connected either with direct cross-over cables or with switches.

**Note:** For illustration purposes, in this document:
- eth5 is used for the IPSO primary redundant interface (the active interface)
- eth6 is used for the IPSO secondary redundant interface (the backup interface).

State sync with Cross-over Cables on the IPSO redundant links

The simplest method for configuring state sync on IPSO redundant links is to use cross-over cables. Failure of an interface or cable on the Primary redundant interface on one member takes down the primary interface on both members and causes the secondary redundant link to take over.

![Diagram of state sync with cross-over cables](image)

State Sync with a Switch Environment and IPSO Redundant Links

The following switch topology configurations require VLANS and VLAN trunking to be configured on the switches, to transmit the sync traffic to the active sync interfaces. Note though that the VLAN itself can be considered as a single point of failure.
The configuration works for single and multiple switch scenario topologies:

**Scenario 1 - State Sync for a single switch per IPSO redundant link:**

```
Cluster Member A

IPSO Primary Redundant Interface
eth5
Switch 1

VLAN Trunk

IPSO Secondary Redundant Interface
eth6
Switch 2

Cluster Member B
```

**Scenario 2: State Sync for multiple switches per redundant IPSO link:**

```
Cluster Member A

IPSO Secondary Redundant Interface
eth5
Switch 1

VLAN Trunk

IPSO Secondary Redundant Interface
eth6
Switch 2

Switch 3

IPSO Secondary Redundant Interface
eth5

VLAN Trunk

Switch 4

IPSO Secondary Redundant Interface
eth6
```

Configuring the Switches

Configure VLANs and trunking on the switches so that the Primary and Secondary interfaces of both firewalls are all in the same broadcast domain and can communicate with each other. With this configuration, if a Primary sync interface fails on one firewall (i.e. eth5 in above diagrams) the Sync updates from/to the remaining Secondary interface (eth6) on this firewall will now be received/sent from/to the active redundant interface on the other firewall.

On Cisco switches it is recommended to configure portfast on the switch ports connected to the IPSO redundant link state sync interfaces.

**Note:** Do not configure VLANs or Trunks on the State Sync interfaces of the firewalls.
Configuring the Firewalls

In Network Voyager

1. Configure the speed and duplex settings for each of the firewall interfaces that are to be used in the redundant link configuration:

2. Create a Link Redundancy Group for the interfaces that are to be used for state sync:
3. From the ‘Bonded Port’ drop down, select the interfaces to include in the new Link Redundancy Group:

![Network Voyager configuration interface](image1)

After selecting the interfaces, the configuration should look similar to the following:

![Network Voyager configuration interface](image2)

4. Configure the IP address to be used for State Sync on this cluster member:
   - Go to the Network Voyager Configuration > Interface Configuration > Interfaces page
   - Click the Logical link for the redundancy interface:

![Network Voyager interface configuration](image3)
• In the Logical Interface page, type in the State Sync IP address and the Mask, and activate the interface:

5. Check the configuration of the redundancy interface in the Network Voyager Interfaces page:

The Network Voyager configuration is now complete on this member.

6. Save your configuration.
7. Repeat the entire configuration on the cluster partner firewall. Remember to assign the appropriate partner IP sync address on this member.
Configure the State Sync Network in SmartDashboard

Verify that cluster object has been properly configured by the administrator.

Configure the State Sync interface as follows:

1. Edit the cluster object in SmartDashboard.
2. In the Edit Topology window, perform ‘Get Topology’ for each member. This retrieves the new redundant interface. Assign the 1st Sync to the redundant interface.
3. Click OK
4. Save the change:

![SmartDashboard Topology Window](image)

Completing the Procedure

1. Install the policy on the cluster
2. Verify that State Sync is working normally by running the CLI command `cphaprob state`

The output of the `cphaprob state` should show the local and remote members as Active.

```
IP290[admin]# cphaprob stat
Cluster Mode:  Sync only (IPSO cluster)
Number  Unique Address  Firewall State (*)
1 (local)  192.168.1.1  Active
2  192.168.1.2  Active

(*) In IP Clustering/VRRP FW-1 also monitors the cluster status
```

IP290[admin]#
Verfying

1. Ensure all IPSO redundant interfaces are up on both cluster members. The following output is from one cluster member. Make sure you check both cluster members:

   ![Network Voyager Screenshot]

   **Link Redundancy Configuration**

   **Cluster Mode:** Sync only (IPSO cluster)

   **Number** | **Unique Address** | **Firewall State** (*)
   --- | --- | ---
   1 (local) | 192.168.1.1 | **Active**
   2 | 192.168.1.2 | **Active**

   (*) In IP Clustering/VRRP FW-1 also monitors the cluster status

   IP290[admin]# cphaprob stat

   Cluster Mode:  Sync only (IPSO cluster)

   **Number** | **Unique Address** | **Firewall State** (*)
   --- | --- | ---
   1 (local) | 192.168.1.1 | **Active**
   2 | 192.168.1.2 | **Active**

2. Check the state of State Sync by running the cphaprob state command. The local and remote should be active on both cluster members.

   **First cluster member:**

   IP290[admin]# cphaprob state

   Cluster Mode:  Sync only (IPSO cluster)

   **Number** | **Unique Address** | **Firewall State** (*)
   --- | --- | ---
   1 (local) | 192.168.1.1 | **Active**
   2 | 192.168.1.2 | **Active**

   (*) In IP Clustering/VRRP FW-1 also monitors the cluster status

   IP290[admin]#

   **Second cluster member:**

   IP390[admin]# cphaprob state

   Cluster Mode:  Sync only (IPSO cluster)

   **Number** | **Unique Address** | **Firewall State** (*)
   --- | --- | ---
   1 | 192.168.1.1 | **Active**
   2 (local) | 192.168.1.2 | **Active**

   (*) In IP Clustering/VRRP FW-1 also monitors

3. Remove the Primary State Sync interface from the Cluster Master.
Configure the State Sync Network in SmartDashboard

4. In the Network Voyager Configuration > Interface Configuration > Link Redundancy page, confirm that the primary interface on the Master is down.

5. Check that State Sync is still Active/Active on both members of the cluster:

   **First cluster member:**
   
   IP290[admin]# cphaprob stat
   
   Cluster Mode:   Sync only (IPSO cluster)
   
   Number Unique Address Firewall State (*)
   
   1 (local) 192.168.1.1   Active
   2 192.168.1.2   Active
   
   (*) In IP Clustering/VRRP FW-1 also monitors the cluster status
   
   IP290[admin]#

   **Second cluster member:**
   
   IP390[admin]# cphaprob state
   
   Cluster Mode:   Sync only (IPSO cluster)
   
   Number Unique Address Firewall State (*)
   
   1 192.168.1.1   Active
   2 (local) 192.168.1.2   Active
   
   (*) In IP Clustering/VRRP FW-1 also monitors
   
   IP290[admin]#

6. Remove the other Primary State Sync interface (i.e. eth5 from the member)
7. Check State Sync is Active/Active on both cluster members. On each cluster member, run:
   
   cphaprob state

8. Check IPSO redundant link recovery by plugging the two Primary State Sync interfaces back into the firewalls. Check the Primary interfaces are back up in Voyager,
9. Run `cphaprob state` on both cluster members. Confirm that State Sync still shows `Active/Active` on both cluster members.

10. In a IPSO Redundant Link switch environment, reboot any of the switches to simulate a switch failure and confirm State Sync remains `Active/Active` in `cphaprob state` on both cluster members.