How to Configure ClusterXL for L2 Link Aggregation

User Guide

15 January 2013

Classification: [Protected]
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://supportcenter.checkpoint.com/file_download?id=23341
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>14 January 2013</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 ClusterXL for L2 Link Aggregation User Guide).
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>Objective</td>
<td>5</td>
</tr>
<tr>
<td>Known Limitations</td>
<td>5</td>
</tr>
<tr>
<td>Supported Platforms</td>
<td>5</td>
</tr>
<tr>
<td>Assumed Knowledge</td>
<td>5</td>
</tr>
<tr>
<td>Related Documentation</td>
<td>6</td>
</tr>
<tr>
<td>Installation and Configuration</td>
<td>7</td>
</tr>
<tr>
<td>Topology</td>
<td>7</td>
</tr>
<tr>
<td>Installing SecurePlatform</td>
<td>8</td>
</tr>
<tr>
<td>Installing Gaia</td>
<td>9</td>
</tr>
<tr>
<td>Configuring Cluster Members - SecurePlatform</td>
<td>9</td>
</tr>
<tr>
<td>Configuring Cluster Members - Gaia</td>
<td>10</td>
</tr>
<tr>
<td>Configuring the Physical Interfaces</td>
<td>10</td>
</tr>
<tr>
<td>Configuring the Bond Interfaces</td>
<td>11</td>
</tr>
<tr>
<td>Configuring the Bridge</td>
<td>11</td>
</tr>
<tr>
<td>Configuring ClusterXL in SmartDashboard</td>
<td>11</td>
</tr>
<tr>
<td>Defining the Cluster Object</td>
<td>11</td>
</tr>
</tbody>
</table>
Objective

This document gives procedures for configuring the Layer 2 Bridge Mode with link aggregation in a ClusterXL environment.

- This document is only a guideline for a known working configuration of a Layer 2 clustering solution.
- This document is only available through the Check Point Solution Center procedure.
- The procedure requires service requests, Sales Force ID, business case and customer user center information.
- Quality Assurance tested this configuration to make sure that it works as documented. It is not a fully certified configuration.
- Customers implementing this configuration must use only the procedures described herein.
- Support for this configuration is on a best effort basis from the Technical Support Center.
- There is currently no Secure Knowledge information available for this topic.

Known Limitations

This solution has these known limitations:

- The bridge can contain only two bond interfaces.
- The bridge must not have a defined IP address.
- NAT is not supported.
- VPN is not supported.
- Some IPS features are not supported.
- Traffic cannot be routed between bridged interfaces to other Security Gateway IP addresses or other bridged interfaces.

Supported Platforms

ClusterXL for Layer 2 Link Aggregation is supported on these platforms only:

- SecurePlatform
- Gaia

This solution has not been tested for IPv6.

Assumed Knowledge

This solution requires a working knowledge of:

- ClusterXL concepts and procedures
- Link aggregation concepts and implementation
- Installing and configuring Security Gateways on SecurePlatform or Gaia platforms
- SmartDashboard configuration procedures
Related Documentation

- ClusterXL Administration Guide for your version.
- Installation and Upgrade Guide for your version.
Installation and Configuration

This section explains how to configure ClusterXL with link aggregation and layer 2 bridges.

Topology

The topology of this solution is:

- A ClusterXL deployment with only two members.
- Each member has one management interface and one sync interface.
- Each member has two high availability link aggregation bonds.
  - Each link aggregation bond contains two physical interfaces, each connected to a different switch.
  - One bond is for traffic coming into the cluster and the other is for traffic going out of the cluster.
- Each member has one bridge connecting the two bonds.
- Packet forwarding is based on STP decisions made by the switches.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Member 1</td>
</tr>
<tr>
<td>B</td>
<td>Member 2</td>
</tr>
<tr>
<td>1</td>
<td>Switch</td>
</tr>
</tbody>
</table>
## Installing SecurePlatform

This section explains how to install SecurePlatform on a new gateway computer. There can be variations for different Check Point releases. See the *Installation and Upgrade Guide* for the release that you are using.

### To install on SecurePlatform using a DVD:

1. Boot the computer from the DVD.
2. When the boot screen shows, press *Enter*. You must press *Enter* in 90 seconds, or the computer will try to boot from the hard drive. If error messages show during the hardware compatibility scan, correct the problems and then restart the procedure from step 1.
3. When the **SecurePlatform Installation** screen shows, do these optional steps if necessary. Select OK to continue with the installation.
   - **Device List**: Select to open the *Hardware Scan Details* window, which includes options for saving the hardware scan results. This is useful for resolving hardware compatibility issues.
   - **Add Driver**: Select to install a device driver from a floppy disk. Use this option only in consultation with Technical Support.
4. In the **Keyboard Selection** window, select a keyboard language and then select OK.
5. From the **Networking Device** window, select an interface to be the management interface and then select OK.
6. In the **Network Interface Configuration** window, define these settings for the management interface and then select OK:
   - IP address
   - Net mask
   - Default gateway
   
   Do not configure IP addresses for other interfaces at this time.
7. In the **HTTPS Server Configuration** window, activate or deactivate web-based connections to the WebUI. Define an IP port (default is 443) to connect to the WebUI client. Select OK.

   **Note** - If you are going to deploy remote access or Endpoint Security software, you must select a port other than the default value (443).
8. Select OK to format your hard drive and install SecurePlatform.

   **Important** - This action deletes all data on your hard drive.
9. When the **Complete** window opens, remove the DVD and press *Enter* to reboot.

When the computer reboots, you can configure SecurePlatform and install Check Point Software Blades and products.
Installing Gaia

This section explains how to do a clean installation of Gaia as a Security Gateway.

**To do a new installation of Gaia using the DVD:**
1. Start the computer from the DVD.
2. When the boot screen shows, select **Install Gaia on the system**,
3. Press **Enter** to continue.
   You must press **Enter** in 90 seconds, or the computer will try to start from the hard drive.
4. Do the instructions on the screen to install Gaia.
   - Optionally select **Machine Info** to see the results of the hardware scan. You save this information to a USB or serial device.
   - Select a keyboard language. English US is the default.
   - Optionally change the default disk space allocation.
   - Enter and confirm the password for the **admin** account.
   - Select the management interface (default = eth0).
   - Configure the management IP address, net mask and default gateway. You can optionally define the DHCP server on this interface.
5. When prompted, restart the computer.
   You can continue to install and configure your Check Point products.

Configuring Cluster Members - SecurePlatform

Do these steps to configure the two Security Gateway cluster members. It is very important to do these steps as written.

1. **Use sysconfig** or the WebUI to configure the IP addresses for the synchronization interface.
2. Do this procedure to configure the bond interfaces:
   a) Run **sysconfig**.
   b) Go to **Network Connections > Add new connection > Bond**.
   c) Select two interfaces to include in the bond and then enter **n**.
   d) Select **High Availability**.
   e) Select **Use default advanced parameters**.
   f) When prompted to add a primary slave interface, enter **y**.
   g) Select one interface as the primary slave.
   h) When prompted to assign an IP address to this bond, enter **n**. Do not assign an IP address to this bond.
   Do these steps for each bond.
3. Do this procedure to configure the bridge:
   a) In **sysconfig**, go to **Network Connections > Add new connection > Bridge**.
   b) Select the two bonds (typically bond0 and bond1) that you created in step 2.
   c) Enter **n**.
   d) When prompted for an IP address, enter **c** to cancel. Do not assign an IP address to the bridge.
   e) Run **ifconfig br0** to make sure that the bridge interface was created correctly.
f) Run `brctl show` from the expert mode to see the attached bridge interfaces.

<table>
<thead>
<tr>
<th>bridge name</th>
<th>bridge id</th>
<th>STP enabled</th>
<th>interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>br0</td>
<td>8000.005056940ef4</td>
<td>no</td>
<td>bond0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>bond1</td>
</tr>
</tbody>
</table>

4. Using a text editor, add the four physical interfaces included in the bonds to the `$FWDIR/conf/discntd.if` file. If this file does not exist, create it. This step disables monitoring for these interfaces.

5. Restart the cluster member.

You must do this procedure for each of the two cluster members.

### Configuring Cluster Members - Gaia

**To Configure a Security Gateway cluster member:**

1. Using your browser, log in to the Gaia WebUI. You must use the management IP address that you defined during the preceding installation steps. The URL must be in this format:
   
   `https://<ip address>`

2. In the First Time Wizard:
   
   - Change the date and time or configure Network Time Protocol.
   - Configure the host name, domain name and DNS servers.
   - Make sure that the management interface connection is correct.


4. Select Unit is part of a cluster and then select ClusterXL.


6. On the Secure Internal Communication page, enter and confirm the SIC activation key.

7. Click Finish to continue.

8. When prompted, click OK to restart the computer.

Do this procedure for the two cluster members. Do not configure IP addresses for other interfaces at this time.

### Configuring the Physical Interfaces

To configure the physical interfaces:

1. In the Gaia WebUI, go to Network Interfaces. All physical interfaces discovered by Gaia show in the Interfaces window.

2. Open the Edit Interface window and do these steps for the management and sync interfaces:
   
   a) Select the Enable option.
   
   b) Enter the IPv4 address and subnet mask in the applicable fields.

3. Open the Edit Interface window and do these steps for all interfaces that are to be included in bonds:
   
   a) Select the Enable option.
   
   b) Make sure that no IP addresses are defined for these interfaces.

Do these steps for the two cluster members.
Configuring the Bond Interfaces

To configure the link aggregation bond interfaces:
1. In the Network Interfaces window, click Add > Bond.
2. On the WebUI Network Interfaces page, click Enable.
3. On the Bond tab, select or enter a Bond Group name. This parameter is an integer between 1 and 1024.
4. Double-click two slave interfaces from the Available Interfaces.
5. Select the Active-Backup operation mode.
6. On the Advanced tab, select the Primary Interface.

Configuring the Bridge

To configure the bridge:
1. In the Network Interfaces window, click Add > Bridge.
2. On the Bridge tab, select or enter a Bridge Group name. This parameter is an integer between 1 and 1024.
3. Double-click the two bond interfaces from the Available Interfaces list.
4. Run ifconfig br0 to make sure that the bridge interface was created correctly.
5. Run brctl show from the expert mode to see the attached bridge interfaces.

```
br0         Link enclave: Ethernet T Waddle 00:50:56:94:0E:F4
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overrunds:0 frame:0
TX packets:599 errors:0 dropped:0 overrunds:0 carrier:0
collisions:0 thereunder:0
RX bytes:0 (0.0 b) TX bytes:46714 (45.6 Kb)
```
6. Using a text editor, add the four physical interfaces included in the bonds to the $FWDIR/conf/discntd.if file. If this file does not exist, create it.

   This step disables monitoring for these interfaces.

Configuring ClusterXL in SmartDashboard

Defining the Cluster Object

To define the cluster object:
1. In SmartDashboard, create a new cluster object using the classic mode.
2. On General page, enter the cluster name, cluster IP address and select the applicable blades.

   **Important** - VPN, NAT and some IPS features are not supported for this configuration.

1. On the Cluster Members page, add and configure the two members. Make sure that the member IP addresses are correct.
2. On the Topology tab, click Edit Topology.
   a) Add the management interface and IP address to the two members using the Monitored Private objective. You can click the Get button to do this.
   b) Add the sync interface and IP address to the two members using the 1st Sync objective.
c) Make sure that none of the bonded interfaces shown in the topology table have defined IP addresses. If they do, delete the IP addresses.

<table>
<thead>
<tr>
<th>Network Objective</th>
<th>MyL2_Cluster</th>
<th>mem101</th>
<th>mem102</th>
<th>Topology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Monitored Private</td>
<td>eth0</td>
<td>eth0</td>
<td></td>
</tr>
<tr>
<td>IPv4 Address</td>
<td>192.168.0.101</td>
<td>192.168.0.102</td>
<td>External</td>
<td></td>
</tr>
<tr>
<td>Net Mask</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prefix length</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>1st Sync</td>
<td>eth5</td>
<td>eth5</td>
<td></td>
</tr>
<tr>
<td>IPv4 Address</td>
<td>6.6.6.101</td>
<td>6.6.6.102</td>
<td>Internal</td>
<td></td>
</tr>
<tr>
<td>Net Mask</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prefix length</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3. On the ClusterXL page, select these options:

   **High Availability**

   **New** mode

   **Maintain current active Cluster Member**

   **Use State Synchronization**

   These are typically the default options.

4. Click **OK** to save the new cluster object.