Configuration of Clustering on Cisco FirePOWER 7000 and 8000 Series Devices

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Configuration](#)
[Adding a Cluster](#)
[Breaking a Cluster](#)
[Sharing the State](#)
[Troubleshooting](#)
[Device is not Properly Configured](#)
[All HA Members Must Have Up-to-date Policies](#)
[Related Documents](#)

Introduction

Clustering of device provides redundancy of configuration and networking functionality between two devices or stacks. This article describes how to configure clustering on Cisco Firepower 7000 and 8000 series devices.

Prerequisites

Before you attempt to establish a cluster, you must be familiar with various features of clustering. Cisco recommends you to read the Clustering Device section of the FireSIGHT System User Guide for more information.

Requirements

Both devices must have the following identical components:

1. Same hardware models
   Note: A stack and a single device cannot be configured in a cluster. They must be in stack of the same type or two similar single devices.
2. Same network modules (Netmod) in the exact same slots
   Note: Stacking netmods are not taken into consideration when the prerequisites of cluster are checked. They are considered the same as an empty slot.
3. Same licenses and they must be exactly the same. If one device has an additional license, the cluster cannot be formed.
4. Same software versions
5. Same VDB versions

6. Same NAT policy (If configured)

Components Used

- Two Cisco Firepower 7010 at version 5.4.0.4
- FireSIGHT Management Center 5.4.1.3

Note: The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

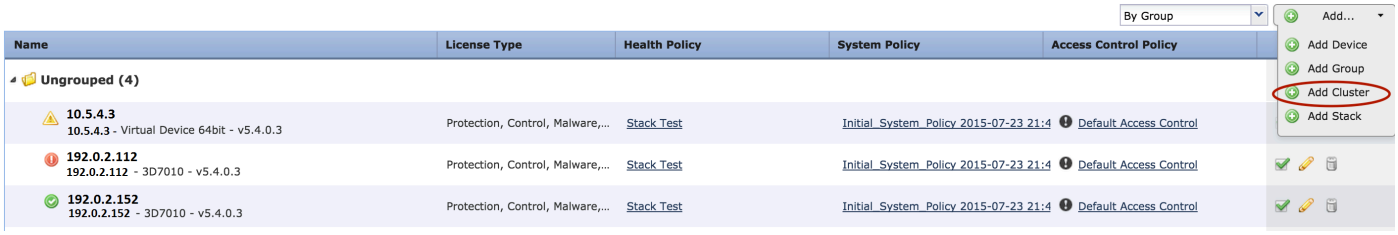
Configuration

Adding a Cluster

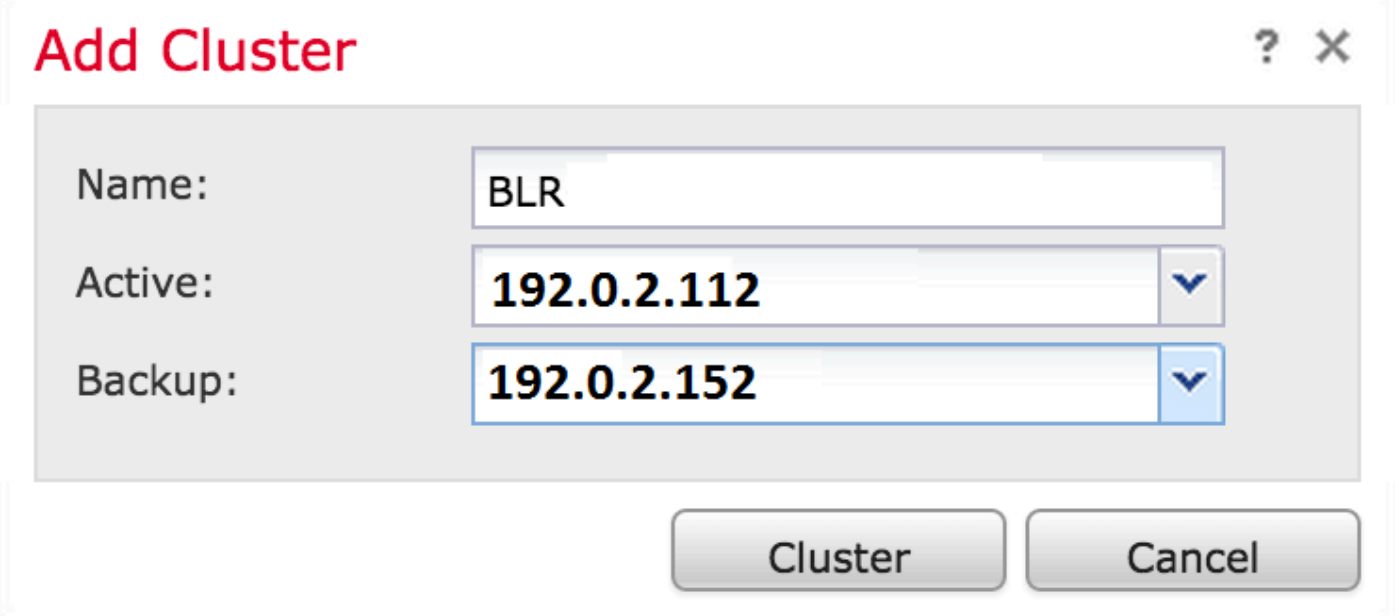
1. Navigate to **Device > Device Management.**

2. Select the devices you wish to cluster. At the top right of the page, select the **Add** drop down list.

3. Select **Add Cluster**.

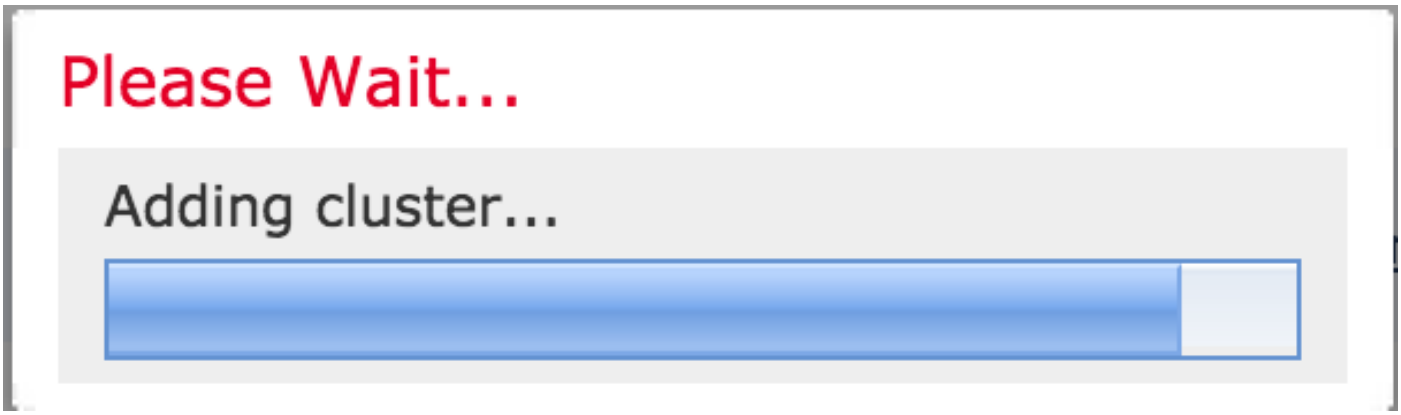


4. The **Add Cluster** popup window appears. You will see the following screen. Provide the IP addresses of the Active and Backup devices.

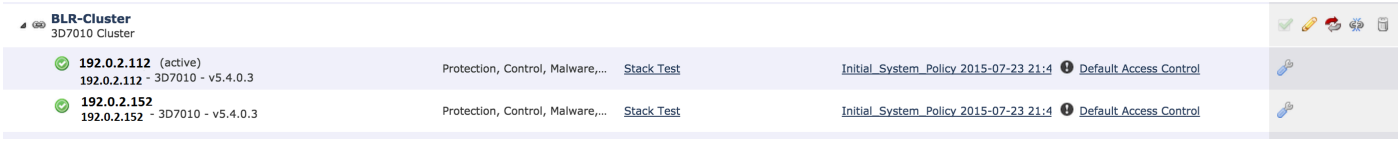


5. Click the **Cluster** button. If all the prerequisites are met, you will see the **Adding Cluster** status

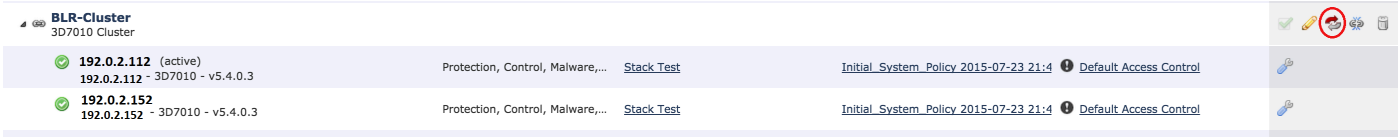
window for up to 10 minutes.



6. Once the cluster is successfully created, you will find the updated devices in **Device Management** page.

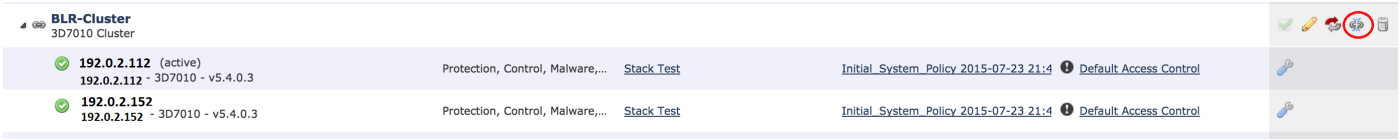


7. You can switch the active peer in a cluster by clicking on the rotating arrow besides the pencil icon.

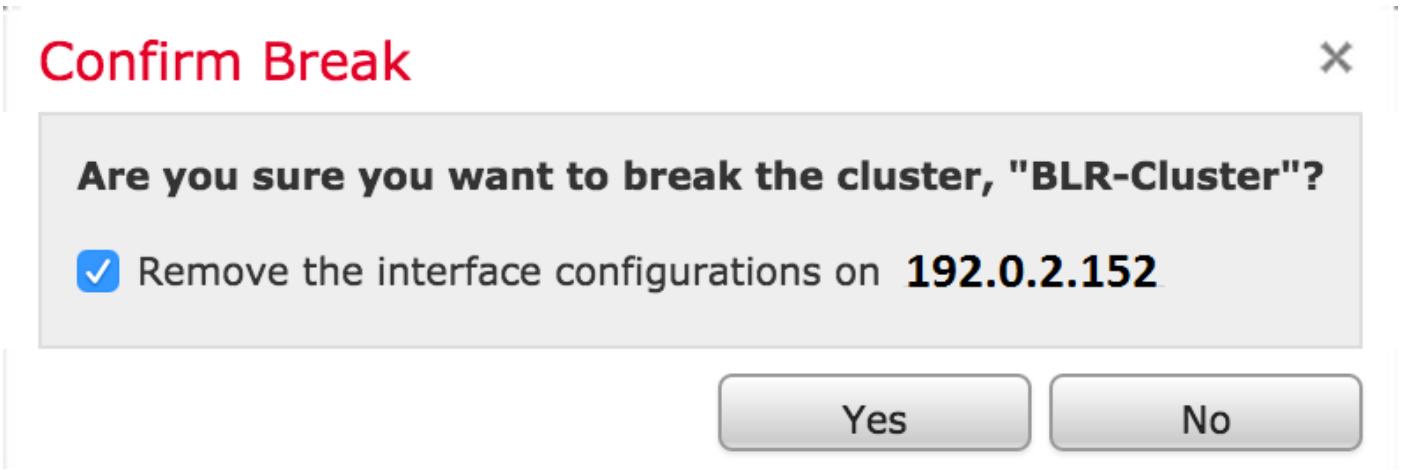


Breaking a Cluster

You can break a cluster by clicking on the Break cluster option besides the recycle bin icon.



After you click the recycle bin icon, you will be asked to remove the interface configuration from the backup device. Select **Yes** or **No**.



You can also delete a cluster and deregister the devices from the Management center by clicking on the **recycle bin**.

If your device has lost access to the Management Center, you can break clustering using the following command on the CLI:

```
> configure clustering disable
```

Sharing the State

Clustered state sharing allows the clustered devices or clustered stacks to synchronize the states, so that if one of the devices or stack fails, the other peer can take over with no interruption on traffic flow.

> **Note**: You must configure and enable the High Availability (HA) link interfaces on both devices or on the primary stacked devices in the cluster before you configure clustered state sharing.

> **Caution**: Enabling state sharing slows system performance.

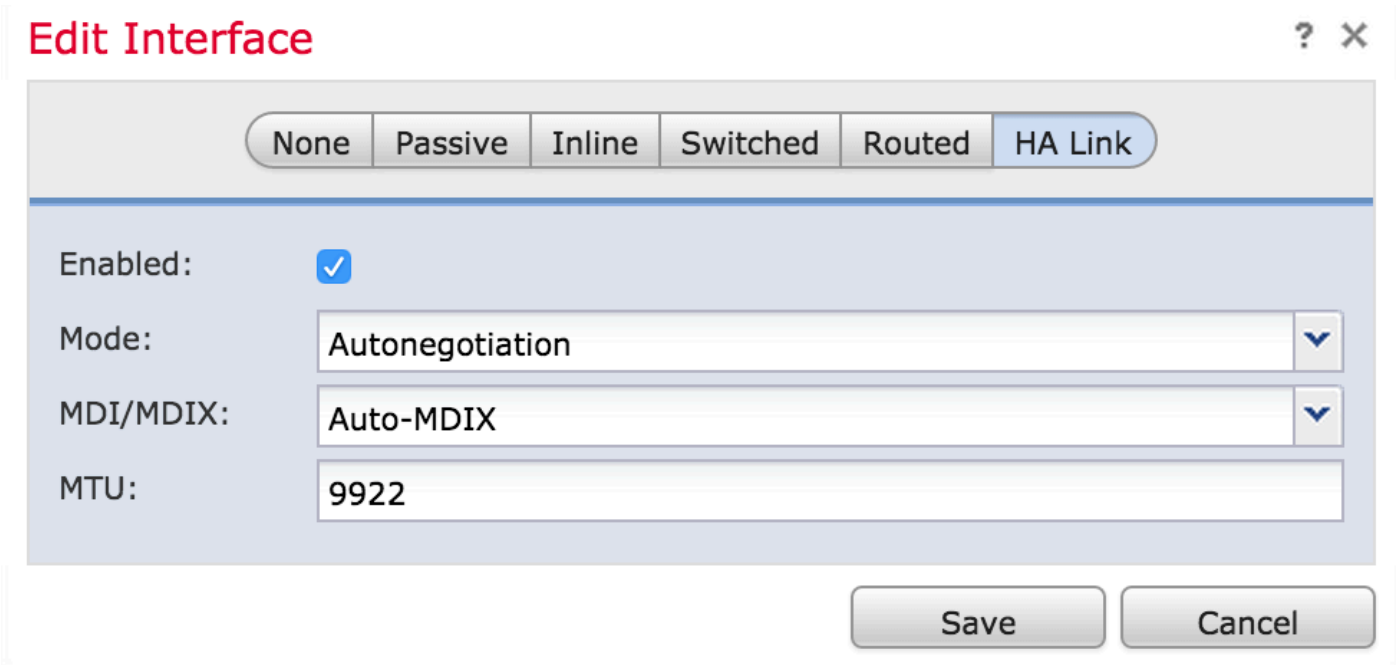
To enable the state sharing on an HA link, follow the steps below:

1. Navigate to **Devices > Device Management**. Select the cluster and edit.

2. Select the **Interfaces** tab.

3. Select the link you want to make as the HA link.

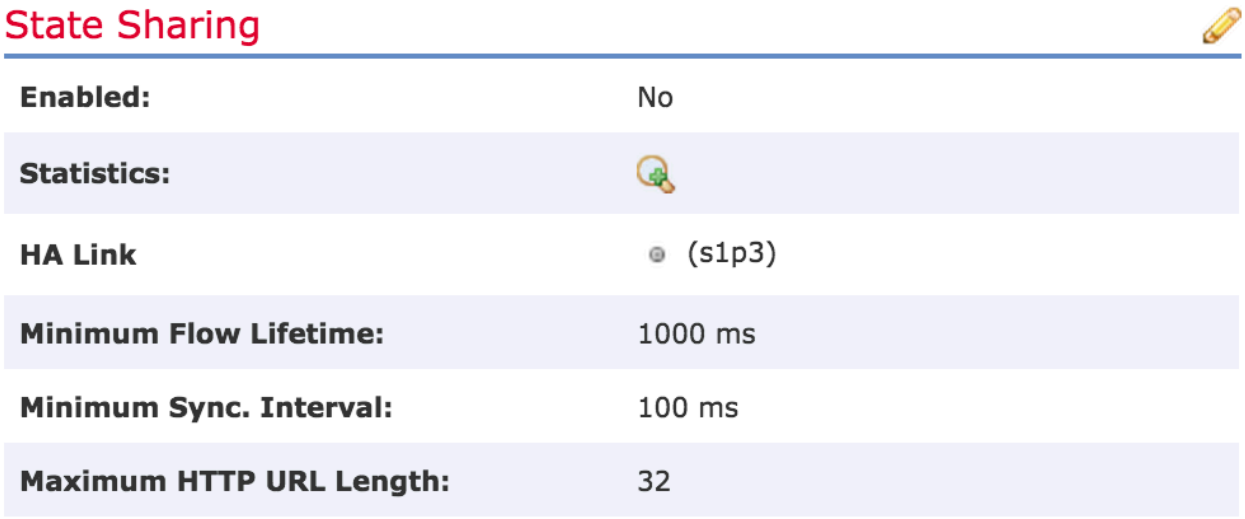
4. Click on **edit** (pencil icon). The **Edit Interface** window appears.



5. After you enable the link and configure other options, click **Save**.

6. Now navigate to the **Cluster** tab. You will see a section called **State Sharing** to the right section

of the page.

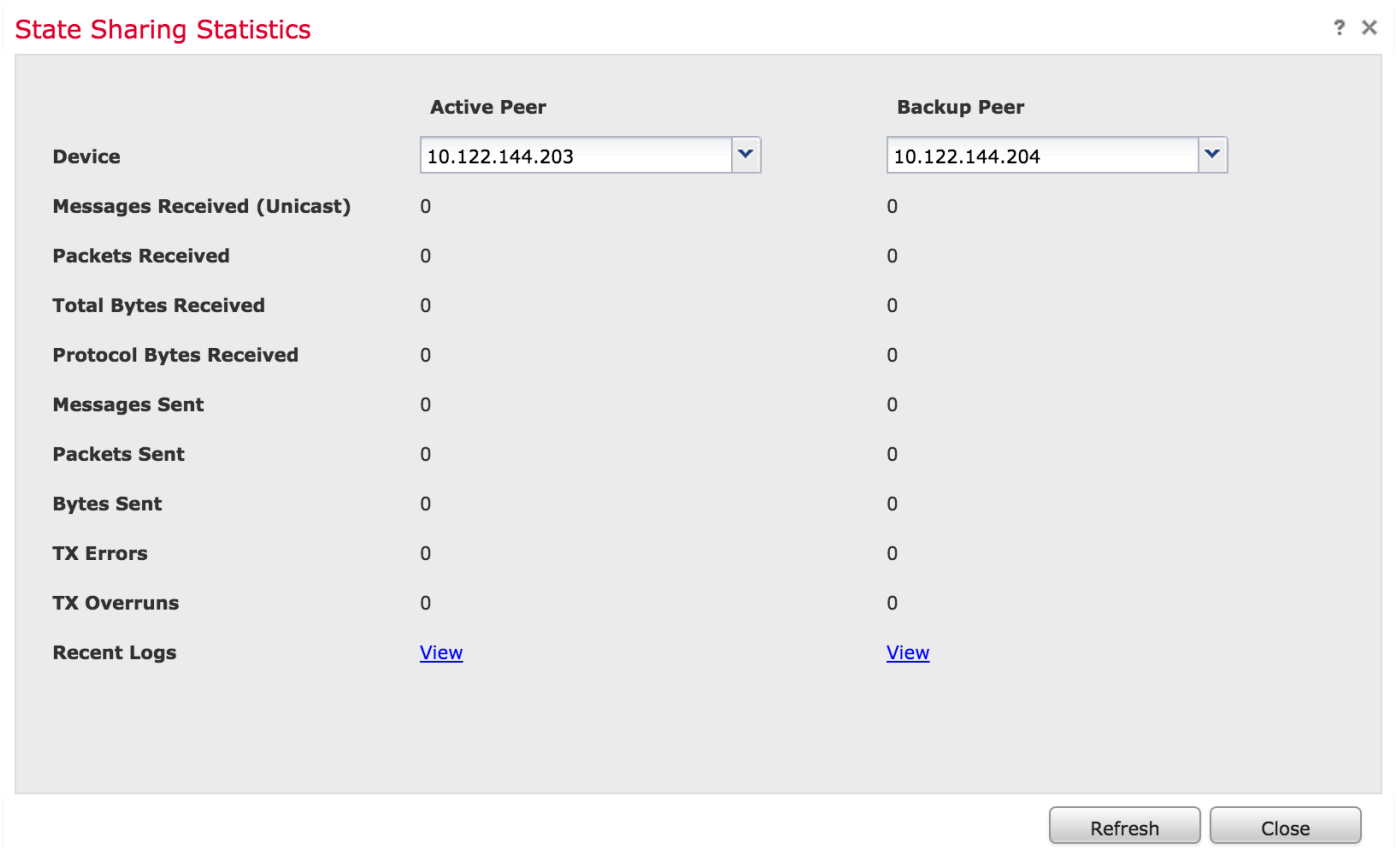


7. Click on the **pencil icon** to edit the state sharing options.

8. Make sure **Enabled** option is checked.

9. Optionally, you can change the Flow Lifetime, Sync Interval and Max HTTP URL Length.

State sharing is now enabled. You can check traffic statistics by clicking on the magnifying glass icon beside Statistics. You will see the traffic statistics for both the devices as shown below.

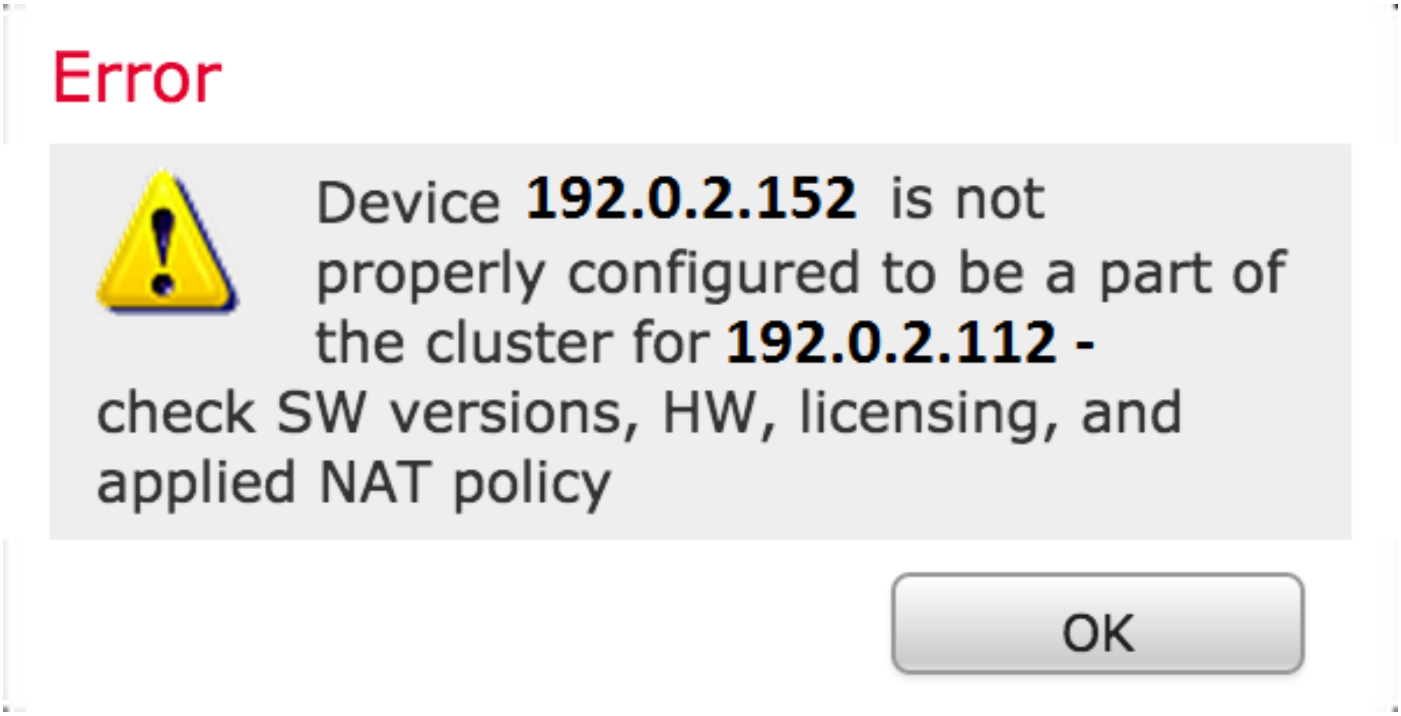


When State Sharing is enabled and an interface on the Active member goes down, all of the TCP connections are transferred to the Standby device which has now become Active.

Troubleshooting

Device is not Properly Configured

If one of the prerequisites are not fulfilled, the following error message appears:



On the Management Center, navigate to the **Devices > Device Management**, and verify if both of the devices have same software versions, hardware models, licenses, and policies.

Alternatively, on a device, you can run the following command to verify the applied access control policy and Hardware and software version:

```
> show summary
-----------------[ Device ]-----------------
Model                     : Virtual Device 64bit (69) Version 5.4.0.4 (Build 55)
UUID                      : 4dfa9fca-30f4-11e5-9eb3-b150a60d4996
VDB version               : 252
------------------------------------------------

------------------[ policy info ]-------------------
Access Control Policy     : Default Access Control
Intrusion Policy          : Initial Inline Policy
.
.
.
Output Truncated
.
```

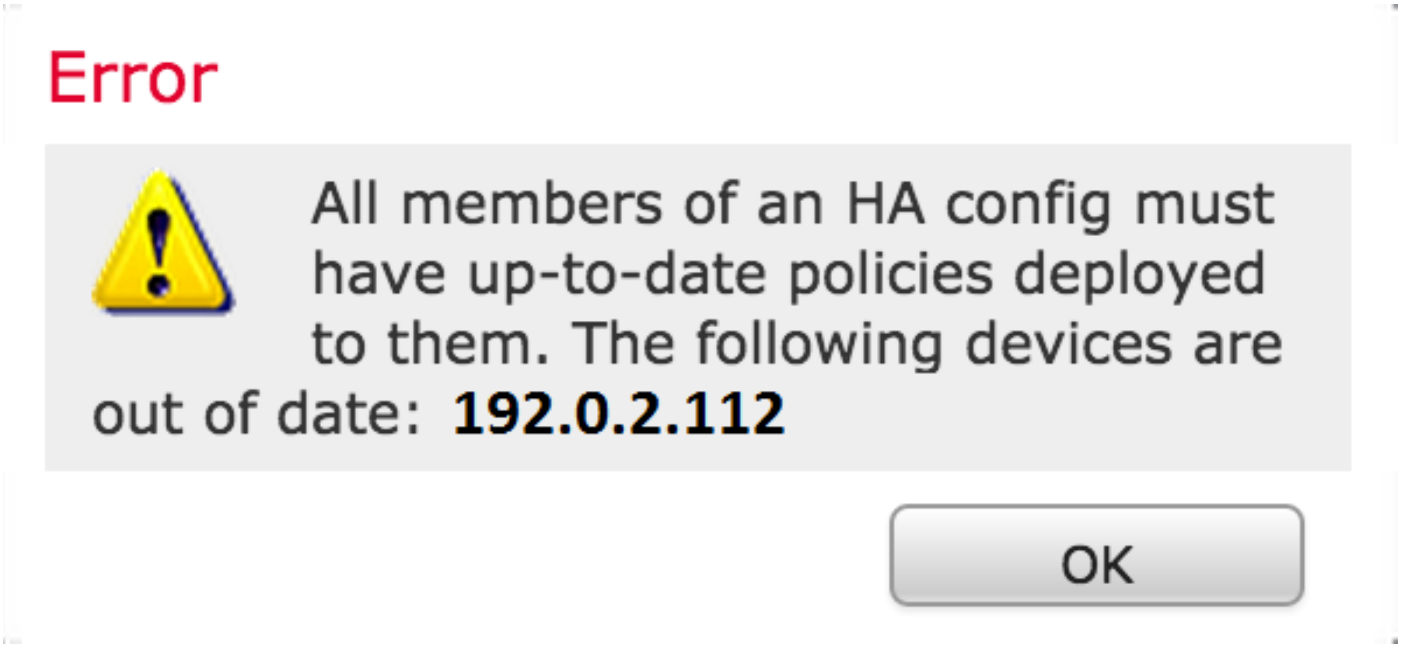
To verify the NAT policy, run the following command on the device:

```
> show nat config
```

> **Note**: The licenses can be checked only on the Management Center as the licenses are stored only on the Management Center.

All HA Members Must Have Up-to-date Policies

Another error that you may encounter is the following



This error occurs when the access control policies are not up to date. Reapply the policies and reattempt the cluster configuration.

Related Documents

- Clustering Device - The FireSIGHT System User Guide