Contents

Introduction

This document describes the configuration of High Availability(HA) for Series 3 Defense Centers(DC).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Firepower Technology
- Basic High Availability Concepts

Components Used

The information in this document is based on Firepower Defense Center Series 3 devices (DC1500,DC2000,DC3500,DC4000) running from software version 5.3 to software version 5.4.1.6

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.

Background Information

To ensure the continuity of operations, the high availability feature allows you to designate redundant Defense Centers to manage devices.The Defense Center maintains event data streams from managed devices and certain configuration elements of these devices. If one Defense Center

fails, you can monitor your network without interruption through the other Defense Center.

High availability Features

- HA synchronization is bi-directional which means even though there is a designated primary and secondary device, changes added on any one of the devices are replicated to the other.
- HA does not require the devices to be directly connected. The HA connection can be done over a switch but this connection needs to be in the same broadcast domain.
- HA devices communicate over their management IP at port 8305.
- HA synchronization time for a device is five minutes, which means that after every five minutes a device attempts to synchronize its configuration with its peer. Since the time required for synchronization is specific to devices, cumulatively, the synchronization time can be maximized to ten minutes.
- If a reimage is required for a specific HA peer it is recommended to break the HA and then reimage.
- If you plan to upgrade the HA cluster it is not necessary to break the HA .When you upgrade from version 5.3.0 to 5.4.0, upgrade the devices one by one and once they are upgraded perform a synchronization task on primary Defense Center.
- The presence of an access policy with the same name on both the DCs create two Access control Policies of the same name. One policy is configured locally and the other is synchronized from the peer DC.

  Note: You cannot add a target or apply this policy because it throws up an error, which states that there is already a policy with the same name.

- Licenses are not synchronized between DC peers, therefore, they are required to be added separately to the DCs.
- All managed devices are added only to one DC. The configuration is synchronized between the peer DCs.
- Managed devices send logs to both the DCs.
- DCs synchronize latest actions. For example, if you delete a user from DC-1, the other peer DC-2 does not synchronize user configuration to DC-1. It synchronizes the **delete action** and the user is lost from both DC-1 & DC-2.

Configuration shared bidirectionally between peers

HA DCs synchronizes policies bi-directionally. These configurations are synced bidirectionally between peers. You can also view most of these configurations with the path defined right next to it:

Identities and Authentication

- External LDAP configuration- Navigate to **System > Local > User Management > External Authentication**
- Users (Internal and External)**System > Local> User Management> Users**
- Custom User roles**System > Local > User Management > User Roles**

Reports

- Report templates**Overview > Reporting > Report Templates**

Configurable Policies (Under Policies Section)

- Access Control Policies,Intrusion Policies, File Policies, SSL Policies, Network access policies,Correlation Policies and rules, Compliance whitelist and traffic profiles.
- Intrusion Rules (Local and SRU)**Policies > Intrusion> Rule Editor > Local Rules.**
- Network Discovery,Host attributes, Network discovery user feedback, including notes and host criticality, the deletion of hosts, applications, and networks from the network map and the deactivation or modification of vulnerabilities.
- Custom Application Detectors
- LDAP Connections in User policies- Navigate to**Policies > Users**
- Alerts **Policies> Actions > Alerts** (Under Responses)

Device Information

- NAT Rules- Navigate to**Devices> NAT**
- VPN Rules**Devices > VPN**
- All device information including the name and its group is synced bidirectionally. Location for log storage for each device is also synced between peers **Devices > Device Management**
- Custom Intrusion Rule classifications
- Activated custom fingerprints
- System policy and Health Policy
- Custom dashboards,Custom workflows and custom tables
- Change Reconciliation, snapshots and report settings
- Sourcefire Rule Updates (SRU),Geolocation database (GeoDB), and vulnerability database (VDB) updates

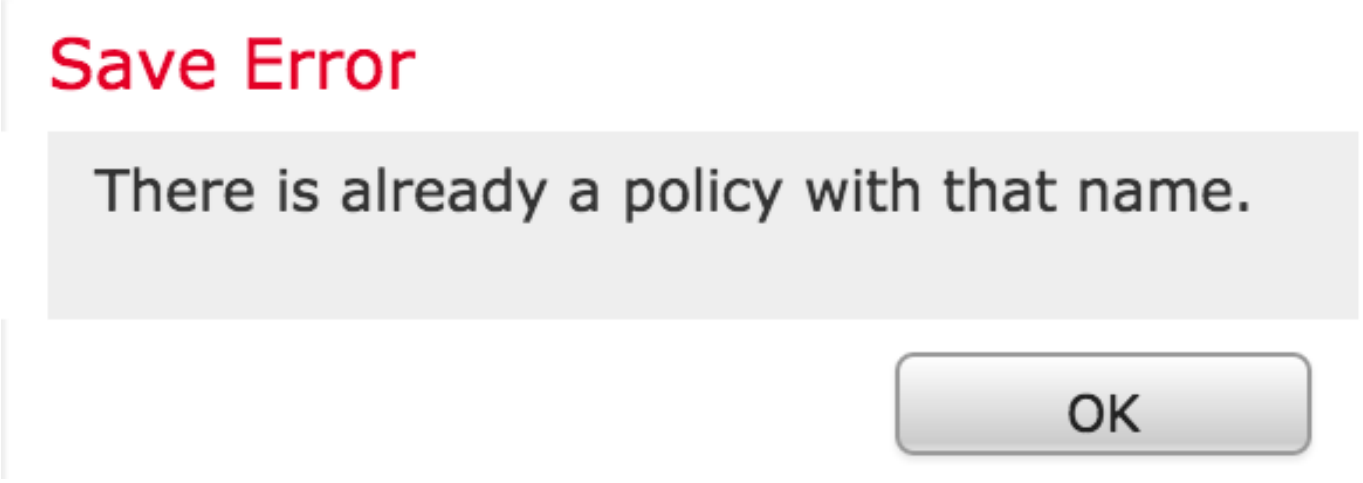
Configuration not synced between DCs

- User Agent information in User policy
- NMAP Scans
- Response Groups
- Remediation Modules
- Remediation Instances
- Estreamer and Host Input Client
- Backup profiles
- Schedules
- Licenses
- Updates
- Health Alerts

Configure

Pre-requisites to configure High Availability

- The devices must be of same software and hardware version.
- The devices must have the same VDB installed.
- The devices must have the same SRU.
- Ensure both Defense Centers have a user account named admin with Administrator privileges. These accounts must use the same password.
- Ensure that other than the admin account, the two Defense Centers do not have user accounts with identical usernames. Remove or rename one of the duplicate users account before you establish high availability.
- Ensure both the devices do not have any Access Control policies with the same name. If there are two Access Control policies with the same name they both coexist on the DCs. However, they cannot get associated with any device.Once you save this policy after adding a target device , this configuration is rejected with an error as shown in the image:



- Both the Defense Centers must have access to the internet.

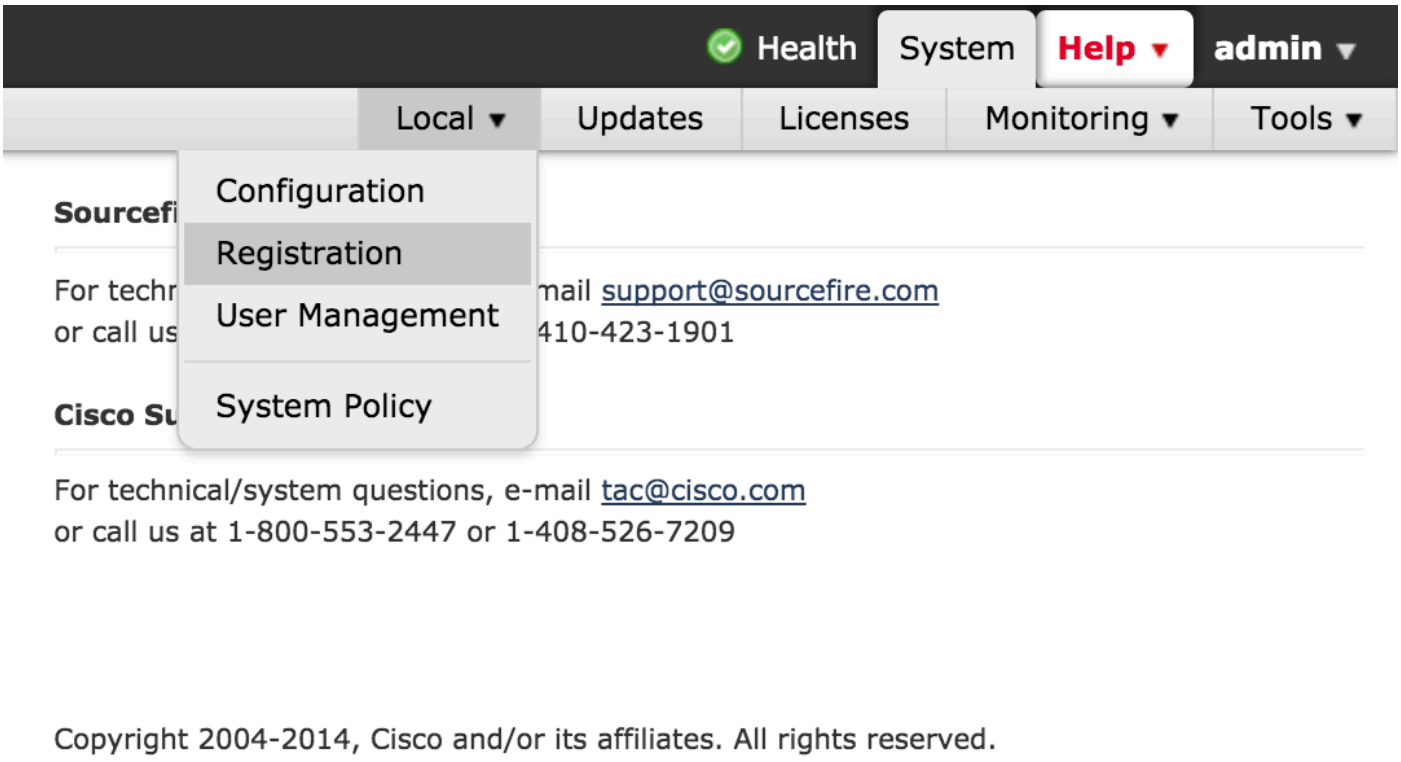
Configure High Availability

These are the 8 steps to configure High Availability.

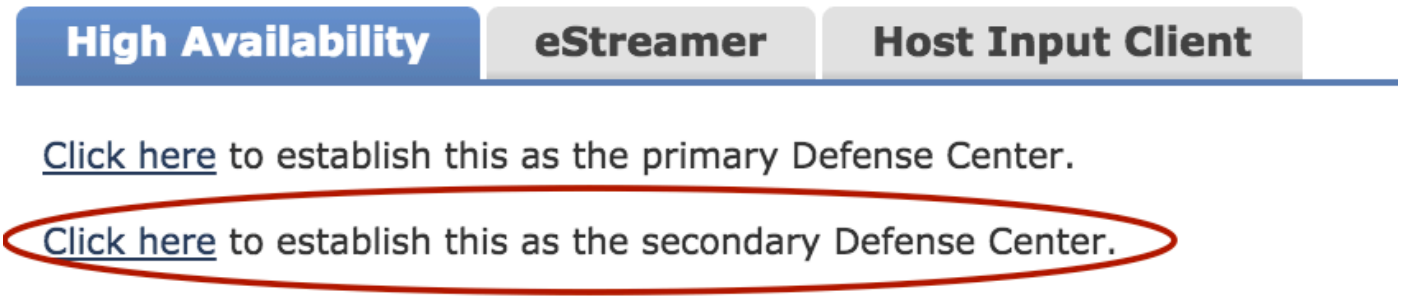
Step 1. Confirm that the software and hardware version along with the VDB version and the rule update version are the same.

Model	Defense Center 1500
Serial Number	BZDW14300158
Software Version	5.4.1.2 (build 38)
OS	Sourcefire Linux OS 5.4.0 (build126)
Snort Version	2.9.7 GRE (Build 262)
Rule Update Version	2015-11-16-001-vrt
Rulepack Version	1606
Module Pack Version	1837
Geolocation Update Version	None
VDB Version	build 258 (2015-11-10 22:58:57)

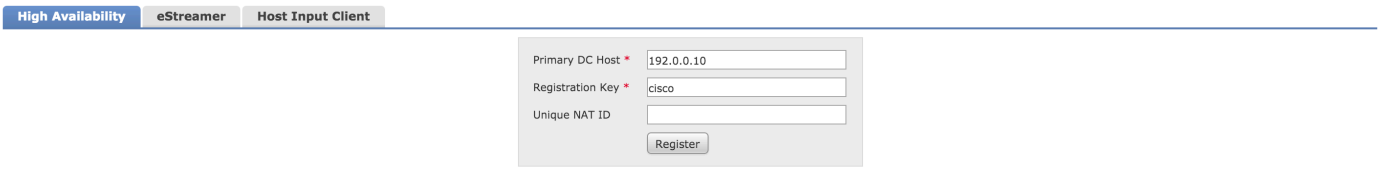
Step 2. In order to make your device secondary, navigate to **System > Local > Registration**, as shown in the image. Ensure that you have no configuration on this DC.



Step 3. Under the **High Availability** tab Click on **Click here to establish this as a secondary defense Center**, as shown in the image:



Step 4. As you complete Step 3, a page is displayed as shown in the image. Add the IP of the primary DC and the pass key. Ensure that you add a unique NAT ID for devices, which are behind a Network Address Translation.

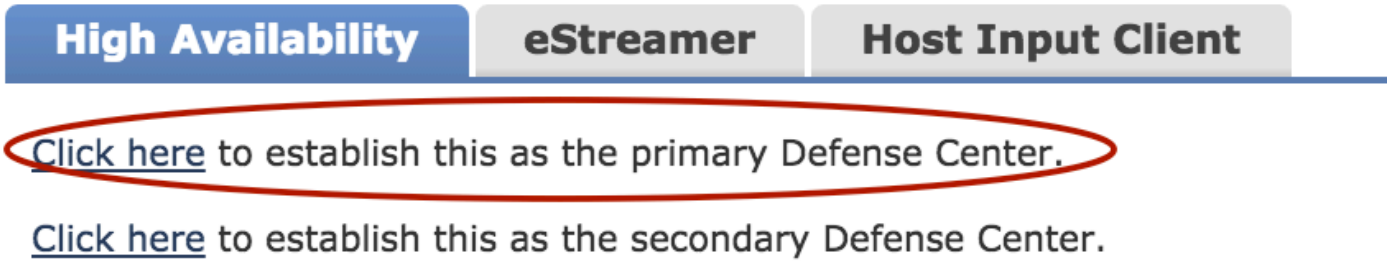


Step 5. After the IP address is verified, if correct click on **Register**. You see a page as shown in the image:

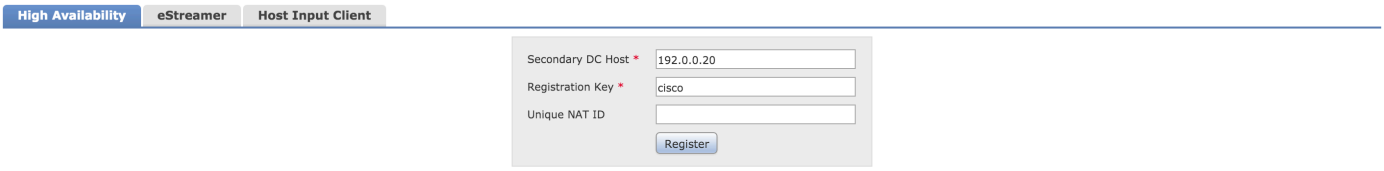
This means that HA is configured on the Secondary DC and you need to configure it on the Primary DC.

Step 6. Log in to the device you wish to configure as the primary DC. Navigate to **System > Local > Registration.**

Under the **High Availability** tab Click on **Click here to add as the primary Defense Center**, as shown in the image:

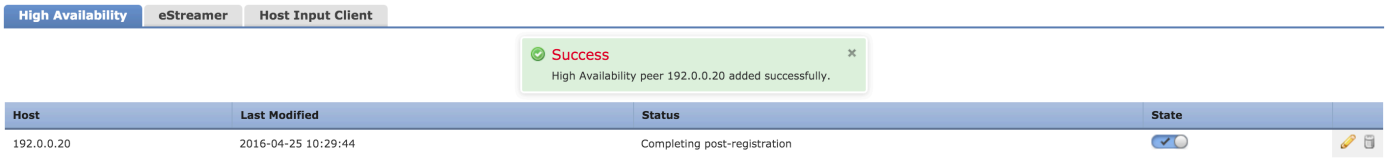


Step 7. After you complete Step 6, a page is displayed as shown in the image:



Add the Secondary DC IP. Provide the same registration key and NAT id which was provided while you configured the secondary DC.

Step 8. After the details of the IP are verified click on **Register.** Once the registration is complete, Sucess page is seen as shown in the image:



After 5-10 minutes HA's configuration and synchronization are completed.

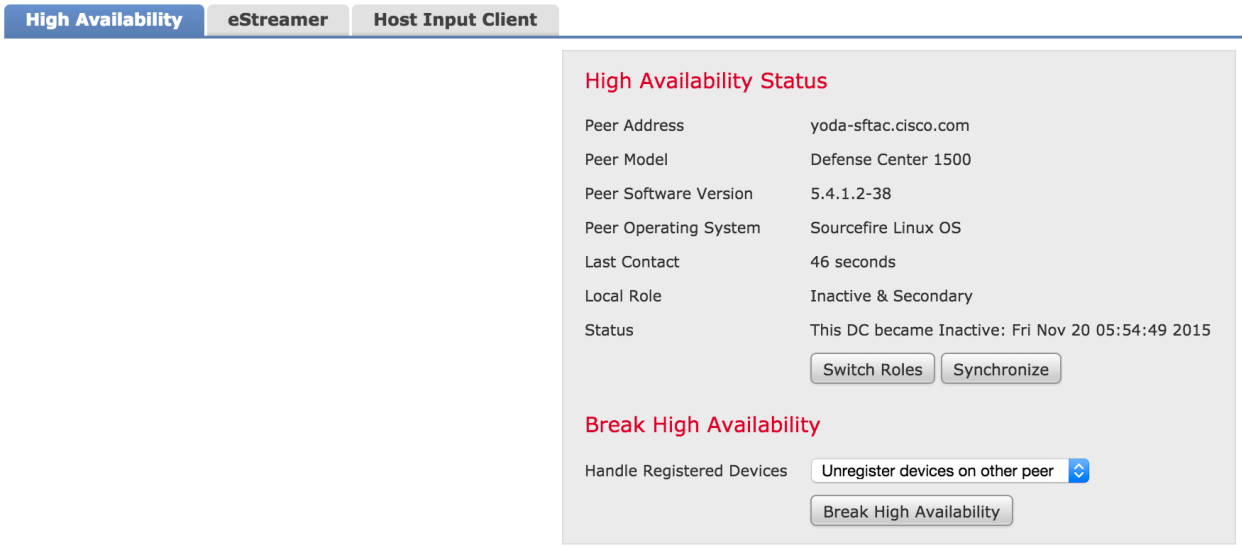
It takes almost 5-10 minutes in order to complete

Verify

Step by Step configuration to verify that your DC's are configured correctly for high availability.

Step 1. Navigate to **System >Local >Registration** on the primary device as shown in the image:

Step 2. **System >Local >Registration** on the secondary device as shown in the image:



Troubleshoot

This section provides basic troubleshooting steps for high availability.

- Ensure both the DC's are listening on TCP port 8305, since HA uses this port to synchronize information and heartbeats..
- Ensure TCP port 8305 is not blocked in the network or by any intermediate devices.
- HA creation fails if there is a stale entry of a previous peer device which is removed or replaced. The EM_Peers table provides more information on such peer devices.

Related Information

- **Configuration of Stack on the Cisco Firepower 8000 Series Devices**
- **Firesight System User Guide 5.4.1**
- **Technical Support & Documentation - Cisco Systems**