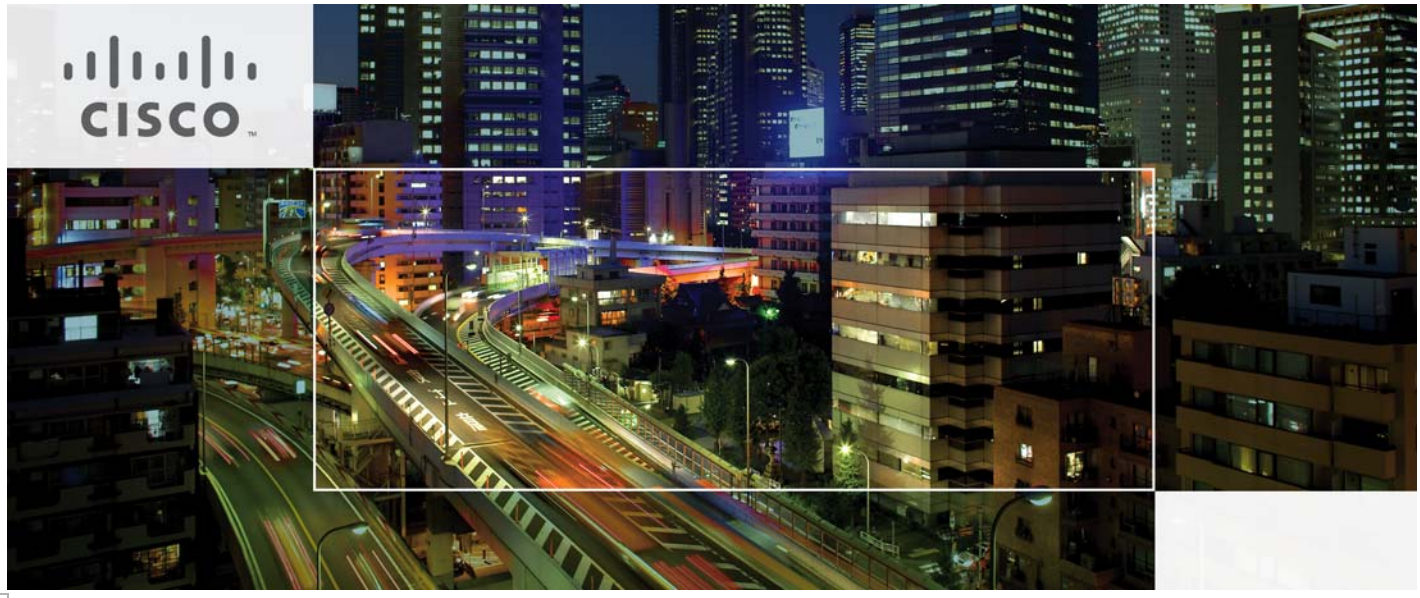


Secure Data Center for Enterprise—Threat Management with Passive Mode NextGen IPS

Implementation Guide—Last Updated: September 16, 2014

Building Architectures to Solve Business Problems

About the Authors

Tom Hogue

Tom Hogue, Security Solutions Manager, Security Business Group, Cisco

Tom is the Data Center Security Solutions Manager at Cisco with over 30 years in developing integrated solutions with Cisco and previous roles in the industry. Tom led the development of the industry leading data center solutions such as the FlexPods, Vblocks, and Secure Multi-tenancy.

Bart McGlothin

Bart McGlothin, Security Systems Architect, Security Business Group, Cisco

Bart is a Security Solutions Architect at Cisco with over 16 years of solutions experience. Bart leads Cisco's involvement with the National Retail Federation's Association for Retail Technology Standards Committee (ARTS) as a member of the ARTS board and Executive Committee. Prior to Cisco, Bart worked as the Network Architect at Safeway, Inc.

Matt Kaneko

Matt Kaneko, Security Systems Architect, Security Business Group, Cisco

Matt Kaneko is the solution technical lead for the Secure Data Center Solution team. In this role, Matt and his team work closely with product marketing teams of various business groups along with customer’s feedback to create solution architecture. Prior to this role, Matt has worked as a Technical Marketing Manager for various Cisco Security Product lines including Cisco ASA Next Generation Firewall, Cisco Intrusion Protection System, Cisco AnyConnect, and associated Management products line.

Mike Storm

Mike Storm, Sr. Technical Engineering Leader, Security Business Group, Cisco CCIE Security #13847

Mike leads the global security community at Cisco Systems for competitive architectures and insight. One of his primary disciplines is Security in the Data Center, developing architectures focused on tightly integrating Next-Generation Security Services with Data Center and Virtualization technologies for enterprise organizations. Storm has over 20 years in the networking and cyber security industry as an Enterprise Consultant and Technical Writer, as well as a Professional Speaker on such topics. Storm is the author of several relevant papers, including the Secure Data Center Design Field Guide and co-author of the Single Site Clustering with TrustSec Cisco Validated Design Guide.

CONTENTS

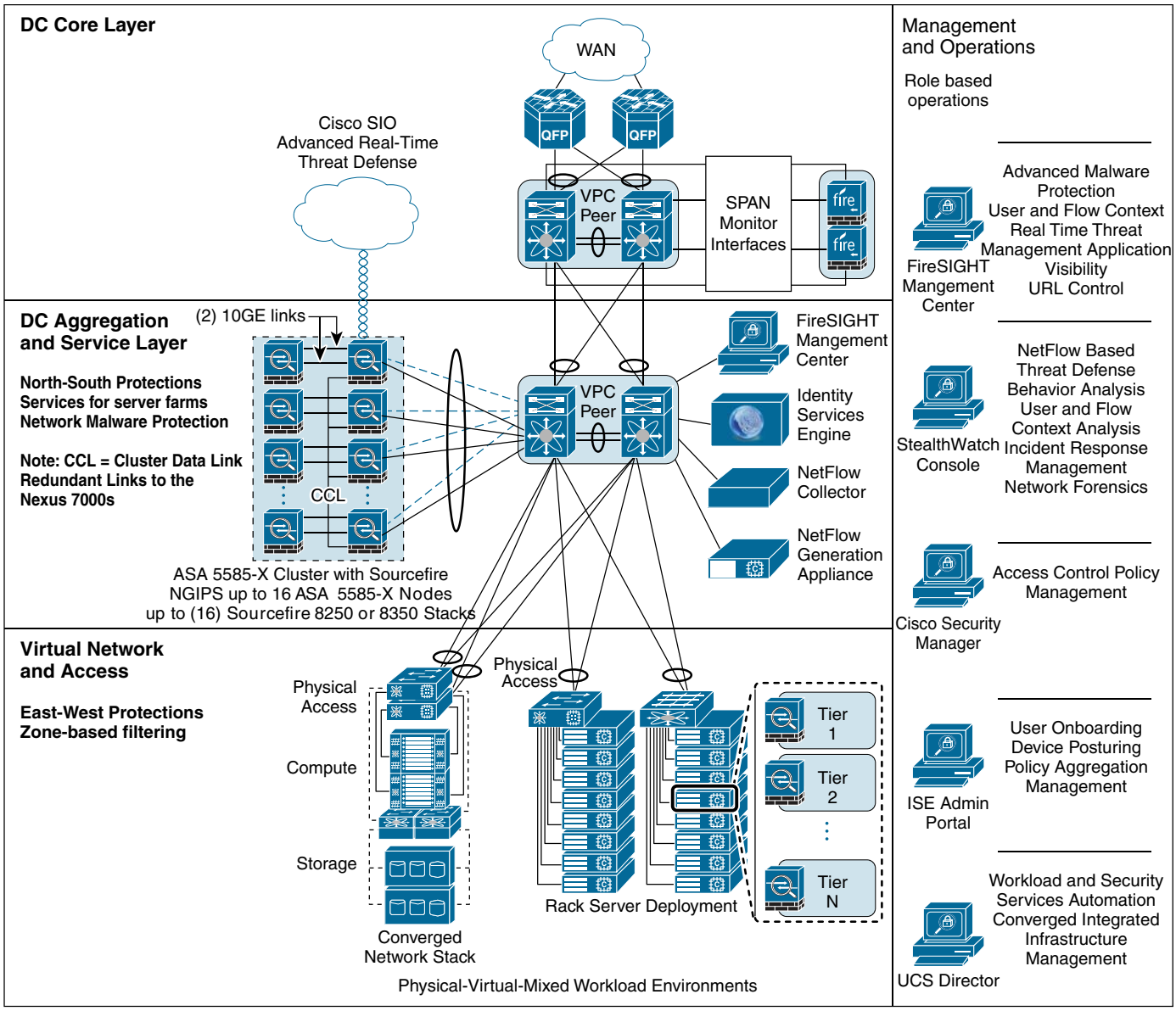
Introduction

Goal of this Document

The Cisco Threat Management with Passive NextGen IPS Solution provides guidance for enterprises that are challenged with the exponential growth of data center resources and associated security policy complexity. Enterprises that want to protect against advanced data security threats can deploy a comprehensive set of security capabilities to address these needs. Figure 1 shows the architectural framework of the Cisco Secure Data Center Portfolio of products and capabilities as expanded to include Threat Management with NextGen IPS.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Figure 1 Threat Management with NextGen IPS

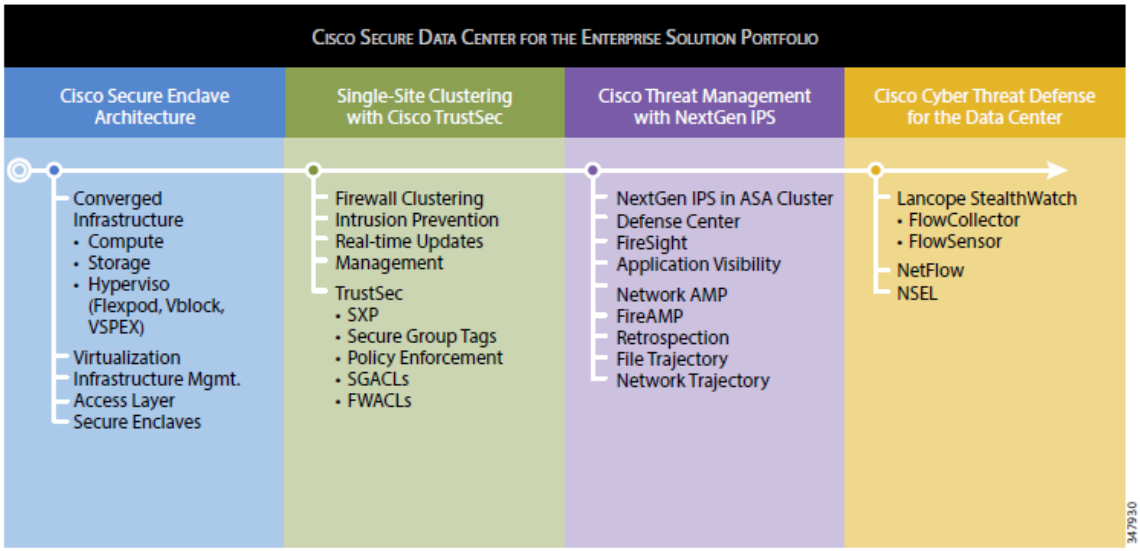


This document is specifically focused on providing implementation guidance for the Threat Management with Passive NextGen IPS solution. It is part of the Cisco Secure Data Center for the Enterprise portfolio of solutions, which provide the best protection available to address today's advanced data security threats. The solutions contain design and implementation guidance for enterprises that want to deploy secure physical and virtualized workloads in their data centers. This solution builds on top of the Secure Data Center Single Site Clustering with TrustSec as a foundation, which should be treated as a pre-requisite for this implementation guide.

The solution portfolio also contains two other solutions: Secure Enclaves Architecture and Cyber Threat Defense for the Data Center. Figure 2 illustrates the relationship among these solutions.

For additional content that lies outside the scope of this document, see the following URL: http://www.cisco.com/go/designzone.

Figure 2 Cisco Secure Data Center for the Enterprise Solution Portfolio



Intended Audience

This document is intended for, but not limited to, security architects, system architects, network design engineers, system engineers, field consultants, advanced services specialists, and customers who want to understand how to deploy a robust security architecture. This document details how specific use cases of the designs were implemented for validation. This implementation guide assumes that the reader is familiar with the basic concepts of IP protocols, quality of service (QoS), high availability (HA), and security technologies. This guide also assumes that the reader is aware of general system requirements and has knowledge of enterprise network and data center architectures.

Validated Components

Table 1 lists the validated components for the solution.

Table 1 Validated Components

Component	Role	Hardware	Release
Cisco NextGen IPS Appliance (FirePOWER)	Application inspection engines	Cisco FirePOWER 3D8250 Cisco Defense Center 3500	Sourcefire 3D 5.3.1
Cisco Nexus 7000	Core switch	Cisco Nexus 7004	NX-OS version 6.1(2)

Solution Component Implementation

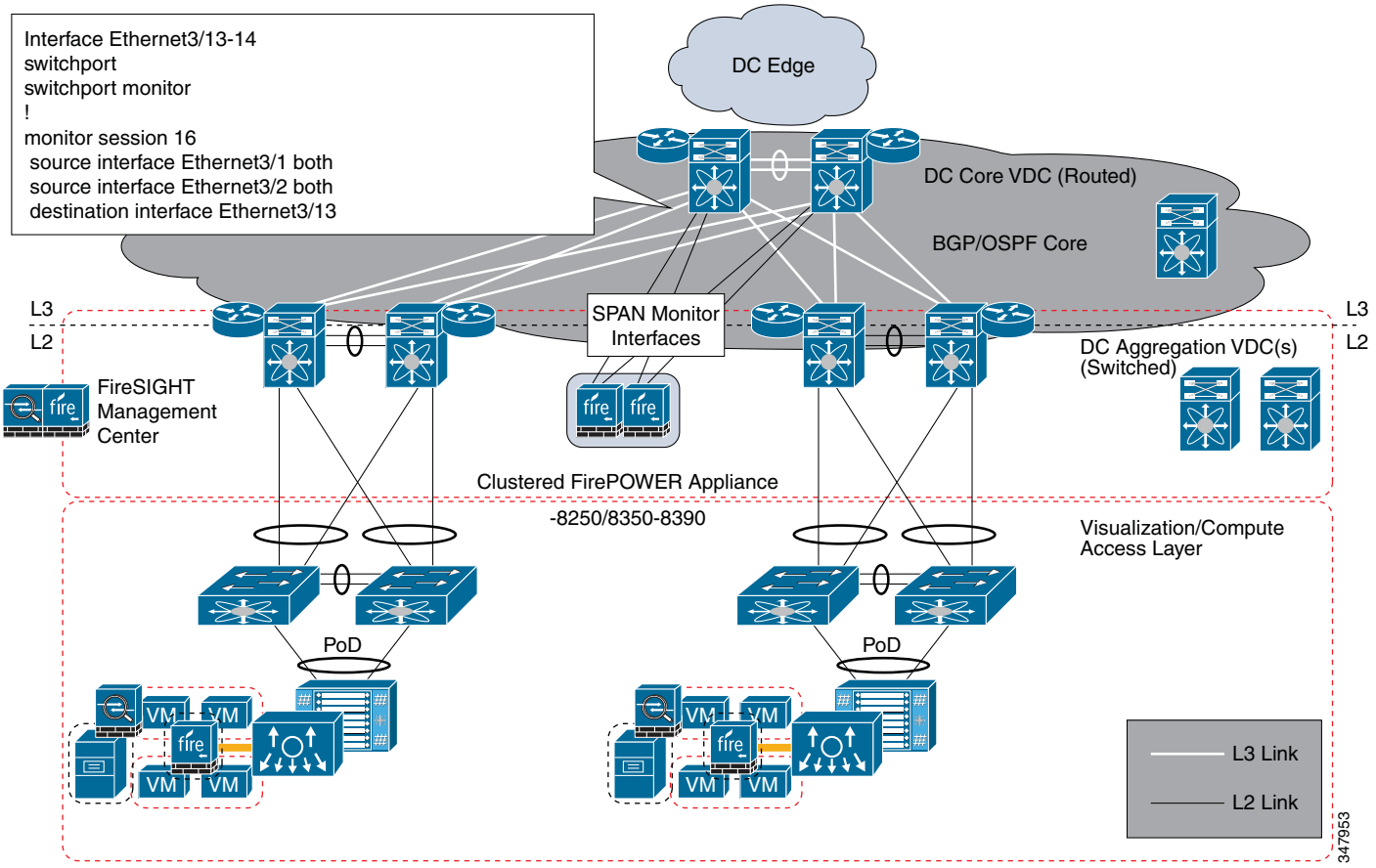
With the introduction of inline Intrusion Prevention Systems (IPS), many companies have shifted their designs from passive intrusion detection systems to inline ones. Although inline mode provides many benefits, the most important being that the system blocks network attacks, there are also benefits to implementing passive intrusion protection within the data center environment.

The most notorious challenges when implementing IPS are false positive alerts. Additionally, enterprises often experience service outages when improperly configured IPS systems block these services, which results in an interruption of the business. Passive intrusion protection is widely used to determine what may cause false positive alerts, and also for administrators to understand the behavior of the IPS protection mechanism without service interruption.

Service interruption is a critical issue for the data center. Although the decision of availability over security may be debatable based on perceived risk, enterprises may prefer deploying intrusion detection in passive mode to prevent service interruption in the data center network.

Figure 3 shows an overview of the lab deployment used for validation. The following sections describe how each product was configured to match specific use cases desired in the validation.

Figure 3 Lab Overview



NextGen IPS Protection

The Threat Management with NextGen IPS Solution leverages the Cisco FirePOWER Next Generation IPS appliances to deliver the protection capabilities of the solution. As discussed in the design guide, there are two identical FirePOWER IPS appliances positioned.

This design uses a passive mode deployment. A redundant pair of FirePOWER appliances is implemented in an clustered configuration. A SPAN monitor session is created on each of the core Cisco Nexus 7000 switches. This configuration provides visibility into all traffic that crosses through the core to and from any aggregation layer.

FirePOWER Installation and Configuration

Initial configuration of the FirePOWER appliances and Defense Center appliance was performed via the console command line where the management address and gateway were assigned following the steps in the *Quick Start Guide*. After each of the appliances were configured and accessible across the network, the remaining configuration was completed using the web GUI. For additional information on configuration options, see the Sourcefire 3D System User, Installation, and Quick Start Guides for version 5.3 at the following URL: https://support.sourcefire.com/sections/10.

Install Defense Center Appliance

The Defense Center appliance was set up as follows.

Procedure

Step 1 At the console, log into the appliance. Use *admin* as the username and *Sourcefire* as the password.

Step 2 At the admin prompt, run the following script:

```
sudo /usr/local/sf/bin/configure-network
```

Step 3 Follow the script's prompts.

a. Configure IPv4 management settings.

b. Enter IPv4 addresses, including the netmask, in dotted decimal form.

```
10.11.236.21 255.255.255.0
```

Step 4 Confirm that your settings are correct.

If you entered settings incorrectly, type *n* at the prompt and press **Enter**. You can then enter the correct information. The console may display messages as your settings are implemented.

Step 5 Log out of the appliance.

For all Defense Centers, you must complete the setup process by logging into the Defense Center's web interface and specifying initial configuration options on a setup page. You must change the administrator password, specify network settings if you have not already, and accept the EULA.

The setup process also allows you to register and license devices. Before you can register a device, you must complete the setup process on the device itself, as well as add the Defense Center as a remote manager, or the registration will fail.

Complete the Initial Setup on a Defense Center using its Web Interface—ACCESS: Admin

Procedure

Step 1 Direct your browser to *https://10.11.230.142/*, the IP address of the Defense Center's management interface.

The login page appears.

Step 2 Log in using *admin* as the username and *Sourcefire* as the password.

The setup page appears. The following sections are needed to complete the setup:

a. Change password

b. Network settings

c. Time settings

d. Recurring rule update imports

e. Recurring geolocation updates

f. Automatic backups

g. License settings

h. Device registration

i. End user license agreement

For more specific steps, see the following URL:
http://www.cisco.com/c/dam/en/us/td/docs/security/sourcefire/3d-system/53/Sourcefire_3D_System_Installation_Guide_v53.pdf

Add Licenses to Defense Center

You can license a variety of features to create an optimal Sourcefire 3D System deployment for your organization. A FireSIGHT license on the Defense Center is required to perform host, application, and user discovery. Additional model-specific licenses allow your managed devices to perform a variety of functions. Because of architecture and resource limitations, not all licenses can be applied to all managed devices. Cisco recommends that you use the initial setup page to add the licenses your organization has purchased. If you do not add licenses now, any devices you register during initial setup are added to the Defense Center as unlicensed; you must license each of them individually after the initial setup process is over. If you have not already obtained your licenses, click the link to navigate to *https://keyserver.sourcefire.com/* and follow the on-screen instructions. You need your license key (listed on the initial setup page), as well as the activation key previously emailed to the contact associated with your support contract.

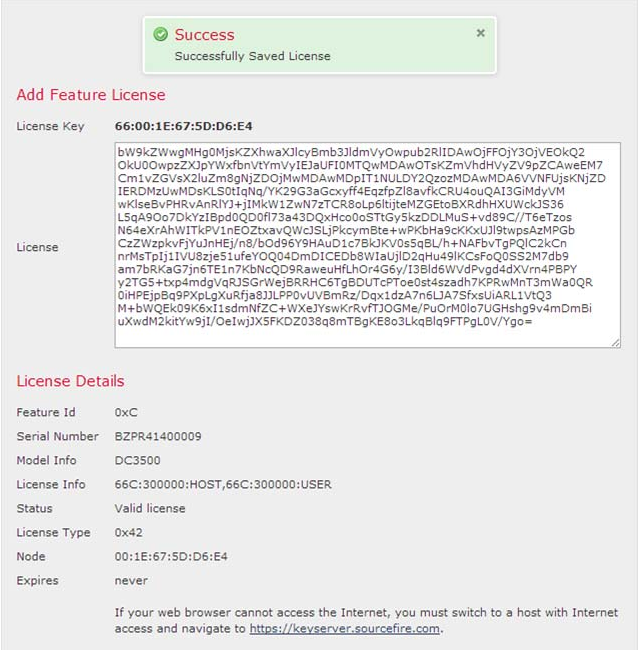
To submit feature license for the device into Defense Center, you need:

- License key from Defense Center that starts with 66:00:00:00:00:00:00 (00 being its MAC address)
- Activation key that was given to the specific device upon your order through the mail

With the above information, you can request the feature license key for the specific device.

Figure 4 shows the successful installation of the feature license into the Defense Center.

Figure 4 Feature License Successfully Installed into the Defense Center



Add FirePOWER Appliances to Defense Center

You can add most pre-registered devices to the Defense Center during the initial setup process (see Figure 5). However, if a device and the Defense Center are separated by a Network Address Translation (NAT) device, you must add it after the setup process completes.

You need the following:

- Host name or IP address of the device
- Registration key (the unique key string assigned during the initial setup for the device)
- Access control policy

Figure 5 Devices

Add a Device to a Defense Center—ACCESS: Admin/Network Admin

To configure the device to be managed by the Defense Center, complete the following steps.

Procedure

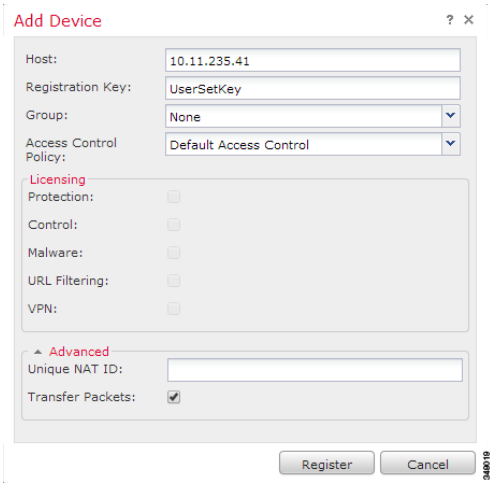
Step 1 Select **Devices > Device Management**.

The Device Management page appears.

Step 2 From the Add drop-down menu, select **Add Device**.

The Add Device pop-up window appears (see Figure 6.

Figure 6 Add Device Pop-Up Window



Step 3 In the Host field, type the IP address or the hostname of the device you want to add.

The hostname of the device is the fully qualified domain name or the name that resolves through the local DNS to a valid IP address.

Step 4 In the Registration Key field, type the same registration key that you used when you configured the device to be managed by the Defense Center.

Step 5 Optionally, add the device to a device group by selecting the group from the Group drop-down list.

Step 6 From the Access Control Policy drop-down list, select an initial policy to apply to the device.

The Default Access Control policy blocks all traffic from entering your network.

Step 7 Select licenses to apply to the device.

Step 8 To allow the device to transfer packets to the Defense Center, select the **Transfer Packets** check box.

This option is enabled by default. If you disable it, you completely prohibit packet transfer to the Defense Center.

Step 9 Click **Register**.

The device is added to the Defense Center. Note that it may take up to two minutes for the Defense Center to verify the device's heartbeat and establish communication.

Configuring HA Clustering on FirePOWER Appliances

Before you establish a device cluster, you must meet the following prerequisites:

- Configure interfaces on each device.

- Each device primary member that you include in the cluster must be the same model and have identical copper or fiber interfaces.
- Both devices must have normal health status, run the same software, and have the same licenses. In particular, the devices cannot have hardware failures that would cause them to enter maintenance mode and trigger a failover.
- You cannot mismatch devices in a cluster. You must cluster single devices with single devices that have identical hardware configurations, except for the presence of a malware storage pack.

After you establish a clustered pair, the system treats the peer devices or stacks as a single device on the Device Management page. Device clusters display the cluster icon in the appliance list. Any configuration changes you make are synchronized between the clustered devices. The Device Management page displays which device or stack in the cluster is active, which changes after manual or automatic failover.

Set Up Clustering—ACCESS Device/Device Management

Procedure

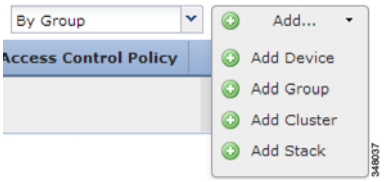
Step 1 Select **Devices > Device Management**.

The Device Management page appears.

Step 2 From the Add drop-down menu, select **Add Cluster**.

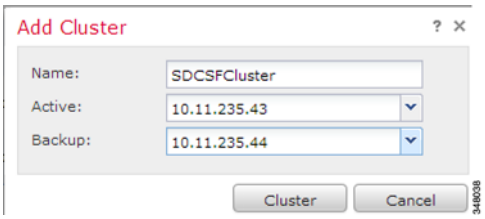
The Add Cluster pop-up window appears. (See Figure 7.)

Figure 7 Add Cluster Pop-Up Window



Step 3 Enter the cluster name, and select the active device and backup device. (See Figure 8.)

Figure 8 Add Cluster Fields



a. In the Name field, type the name of the cluster. You may enter alphanumeric characters and special characters, with the exception of the following characters, which are invalid: +, (,), {, }, #, &, \, <, >, ?, ‘, and “.

b. Select the Active device or stack for the cluster.

c. Select the Backup device or stack for the cluster.

Step 4 Click **Cluster**.

The device cluster is added. This process takes a few minutes as the process synchronizes system data.

Configuring Interfaces for Passive Mode

The following steps explain how you can create or add interfaces for passive mode on Sourcefire 3D system devices.

Procedure

Step 1 Select **Devices > Device Management**.

The Device Management page appears. (See Figure 9.)

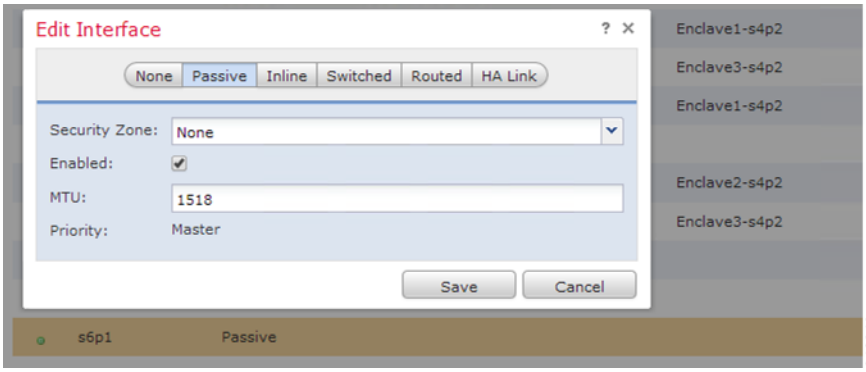
Figure 9 Device Management Page

Step 2 Next to the device where you want to configure the passive interface, click the edit icon.

Step 3 Next to the interface you want to configure as a passive interface, click the edit icon.

The Edit Interface pop-up window appears.(See Figure 10.)

Figure 10 Edit Interface Pop-Up Window



Step 4 Click **Passive** to display the passive interface options.

Step 5 Optionally, from the Security Zone drop-down list, select an existing security zone or select **New** to add a new security zone.

Step 6 Select the **Enabled** check box to allow the passive interface to monitor traffic.

If you clear the check box, the interface becomes disabled so that users cannot access it for security purposes.

Step 7 Click **Save**.

The passive interface is configured. Note that your changes do not take effect until you apply the device configuration.

Monitor Interface Configuration on Cisco Nexus 7000 switches

SPAN for Ethernet ports monitors all traffic for the source port, which sends a copy of the traffic to a destination port. The FirePOWER Appliance, which is attached with the destination port, analyzes the traffic that passes through the source port.

The source port can be a single port, multiple ports, or a VLAN, which is also called a monitored port. You can monitor all the packets for the source port that are received (ingress), transmitted (egress), or bidirectional (both). A replication of the packets is sent to the destination port for analysis.

1. Step 1 shows how to configure the Nexus 7000 interface for Switched Port Analyzer (SPAN):

```
Destination port configuration
switch7000-1#configure terminal
switch7000-1(config)#interface ethernet 3/48


!--- Configures the switchport parameters for a port.

switch7000-1(config-if)#switchport


!--- Configures the switchport interface as a SPAN destination.

switch7000-1(config-if)#switchport monitor
switch7000-1(config-if)#no shut
switch7000-1(config-if)#exit
```

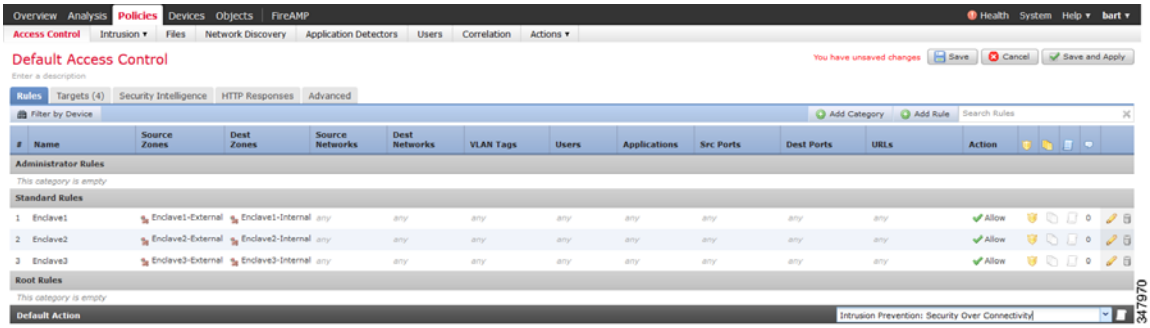
2. Step 2 defines the source and the destination traffic by the interfaces.

```
SPAN session configuration
switch7000-1(config)#monitor session 1


!---Configure the source port with traffic direction.

switch7000-1(config-monitor)#source interface ethernet 3/11 both


!--- Configure the destination port.

switch7000-1(config-monitor)#destination interface ethernet 3/48


!--- To enable the SPAN session, by default session in shutdown state.

switch7000-1(config-monitor)#no shut
switch7000-1(config-monitor)#exit


!--- To save the configurations in the device.

switch7000-1(config)#copy running-config startup-config
```

Security Policies

You can create multiple security policies and apply them to the appliance as a whole using the Default action. (See Figure 11.)

Figure 11 Security Policies



More information on configuring intrusion policies can be found in the *Sourcefire 3D System User Guide*, Chapter 19, page 711.

Validation Testing

Summary of Tests Performed

These test are designed to validate the integration of and general functionality of the Secure Data Center design. The common structure of the architecture is based on Cisco's integrated reference architectures.

Table 2 outlines the various tests conducted to validate the deployment.

Table 2 Test Scenarios

Test	Methodology
Sourcefire high availability recovery and Defense Center connectivity	In this failure scenario, we manually swaps the active unit of the clustered Sourcefire appliance to failover. Upon its recovery, it is checked to confirm that Defense Center regains connectivity.
Intra-enclave communication	Flows within each enclave model will be verified point-to-point within the infrastructure. Uniform traffic patterns and then security policy is critical to Secure Enclave Architecture (SEA) for each enclave. Steps include: • Baseline traffic established • Connections mapped through the enclave
Management traffic flows	Ensure centralized management access for HA-configured Sourcefire devices
Validate integrity of Sourcefire-serviced flows	Validate the integrity of flow and ability to enforce policy

Summary of Results

Table 3 Summary of Results

Test Description	Components	Result
Sourcefire high availability recovery and Defense Center connectivity	Sourcefire 8250, Defense Center	Upon activating standby Sourcefire unit, it successfully failed over and kept the connectivity with Defense Center.
Sourcefire impact to the TrustSec environment	ASA 5585 (9.2(1)), ISE, 7K, Sourcefire, Defense Center	No impact to tagged traffic
Validate integrity of Sourcefire serviced flows	Sourcefire 8250, Defense Center	Cisco has verified that passive mode setup on the Sourcefire 8250 with the high availability feature can be fully integrated and functional with the Secure Data Center Cisco Validated Solution environment.

Conclusion

The Secure Data Center the Enterprise: Passive Mode NextGen IPS solution is a Cisco Validated Design that enables customers to confidently integrate Cisco's security portfolio to respond to the increasing sophisticated attacks being targeted at the data center. This solution is made even stronger when customers also leverage the Secure Enclaves Architecture for securing the workloads, and leverage the Cyber Threat Defense for Data Center solution for enabling behavioral analysis, which provides zero day mitigation protections in the data center.

References

- Data Center Security Design Guide (Mike Storm)— http://www.cisco.com/en/US/netsol/ns750/networking_solutions_sub_program_home.html