Cisco FirePOWER Threat Defense IPS Mode

Cisco FirePOWER Threat Defense is Cisco's premier network security option. It provides a comprehensive suite of security features such as firewall capabilities, monitoring, alerts, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).

Deploy the FirePOWER Sensor on a Cisco Unified Computing System (UCS) E-Series Blade in IPS mode to configure IPS inspection. IPS inspects the traffic, and if configured, will drop the traffic block that it determines as network intrusions.

This module describes how to configure and deploy IPS on Cisco Integrated Services Routers (ISR).

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for FirePOWER Threat Defense IPS Mode

The following prerequisites apply to the Intrusion Prevention System (IPS) inline mode configuration:

- For Cisco IOS XE Release 3.14S and later releases and Cisco IOS Release 15.5(1)T and later releases, use Cisco Integrated Management Controller (CIMC) version 2.3 or later.
- Connect the CIMC dedicated port (M) to the network using an Ethernet cable.

Restriction for Cisco FirePOWER Threat Defense IPS Mode

- Multicast traffic is not inspected.
- Zone-based firewalls, Flexible NetFlow, CENT, Embedded Packet Capture (EPC), and Encapsulated Remote Switched Port Analyzer (ERSPAN) are not supported on bridge-domain interfaces (BDI). Only quality of service (QoS) queuing is supported.

Information About Cisco FirePOWER Threat Defense IPS Mode

IPS Inline Mode in Cisco FirePOWER Threat Defense

Intrusion Prevention Systems (IPS) inspects the traffic, and if configured, will drop the traffic block that it determines as network intrusions. Deploy the FirePOWER Sensor on a Cisco Unified Computing System (UCS) E-Series Blade in IPS mode.

The UCS E-Series Blade in a Cisco Integrated Services Routers (ISR) Generation 2 or ISR 4000 Series Integrated Services Routers hosts the FirePOWEr Sensor, and the sensor communicates back to the Cisco FireSIGHT to get policies and export events.

To enable IPS functionality, the traffic must be routed to the UCS E-Series Blade backplane interface, and this traffic will come out to the external network through the GigabitEthernet front panel port. You can chose a GigabitEthernet interface on a router to enable IPS functionality, and substitute the UCS E-Series Blade front panel port for that interface. Because the front panel of the UCS E-Series Blade is used for traffic flows, the cable connecting to the network must be directly connected to the front panel port.

To enable the FirePOWER Threat Defense IPS mode, no configuration changes are required on the router. However, on the router, you must configure the UCS E-Series backplane interface with relevant physical interface parameters, such as IP address and Dot1Q subinterfaces, security access control lists (ACLs) and so on.

If IPS inline mode is configured on a router that is connected to the Internet, we recommend that you run IPS on the LAN side. Internet-facing ports are configured with Network Address Translation (NAT) and the zone-based firewall, and it is also expected to host a large amount of spurious traffic. If you deploy the IPS solution on this interface, the IPS traffic is exposed to the Internet before NAT/firewall inspects the traffic, leading to spurious intrusions being detected. If you deploy IPS on LAN-facing interfaces, the traffic that IPS inspects is *trusted* traffic in the LAN-to-WAN direction or *cleaned* traffic in the WAN-to-LAN direction.

How to Configure Cisco FirePOWER Threat Defense IPS Mode

LAN-to-WAN traffic that needs inspection arrives on the front panel port of the UCS-E Series Blade. After FirePOWER Sensor inspection, allowed packets egress through the backplane out of the WAN interface.

WAN-to-LAN traffic ingress on the WAN interface of the router; this traffic is forwarded to the backplane, inspected by FirePOWER Sensor, and egress through the front panel port on the UCS E-Series Blade.

Perform the following task to configure Intrusion Prevention System (IPS) inline mode on UCS-E Series Blade:

- Configure CIMC.
- Set up ESXi and install VSphere client.
- Set up FirePOWER Sensor and FireSIGHT virtual machines (VMs).
- Obtain Cisco FirePOWER Threat Defense license.

Configuring Cisco Integrated Management Controller

The following prerequisites apply to CIMC configuration:

- Use Cisco IOS Release 15.5(1)T or later image on Integrated Services Routers (ISR) Generation 2 (G2).
- Use Cisco IOS XE Release 3.14S or later image on ISR 4000 Series Integrated Services Routers.
- Connect the dedicated port (M) to the network using an Ethernet cable.
- Use CIMC Version 2.3 or later, when using Cisco IOS XE Release 3.14 and later images.

This section describes how to configure CIMC for Cisco FirePOWER Threat Defense:

1 Connect to the dedicated management port and configure the **hw-module subslot** command.

Note For more information on the different methods to configure CIMC, see the http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/e/2-0/gs/guide/b_2_0_Getting_Started_Guide/b_2_0_Getting_Started_Guide_chapter_0101.html#d8160e1725a1635.

2 Provide the authentication credentials when prompted. The default username is admin and password is password.
The following example shows how to connect to the dedicated management port:

```
Router# hw-module subslot 2/0 session imc

IMC ACK: UCSE session successful for IMC
Establishing session connect to subslot 2/0
To exit, type ^a^q

picocom v1.4

port is        : /dev/ttyDASH1
flowcontrol    : none
baudrate is    : 9600
parity is      : none
databits are   : 8
escape is      : C-a
noinit is      : no
noreset is     : no
nolock is      : yes
send_cmd is    : ascii_xfr -s -v -l10
receive_cmd is : rz -vv

Terminal ready
```

3 Perform this task to configure CIMC:

```
Device# ucse subslot 1/0 session imc
Unknown# scope cimc
Unknown /cimc # scope network
Unknown /cimc/network # set dhcp-enabled no
Unknown /cimc/network *# set dns-use-dhcp no
Unknown /cimc/network *# set mode dedicated ! mode dedicated when management port is used

Unknown /cimc/network *# set v4-addr 172.16.1.8
Unknown /cimc/network *# set v4-netmask 255.255.255.0
Unknown /cimc/network *# set v4-gateway 172.16.1.1
Unknown /cimc/network *# set preferred-dns-server 10.102.6.247
Unknown /cimc/network *# set hostname device-2951-UCS-E
Unknown /cimc/network *# commit ! make sure to commit to save the changes
```

The following sample output from the **show detail** command is used to verify the CIMC configuration. Use ^a^q to quit or exit the console.

```
Router /cimc/network # show detail

Network Setting:
  IPv4 Address: 172.16.1.8
  IPv4 Netmask: 255.255.255.0
  IPv4 Gateway: 172.16.1.1
  DHCP Enabled: no Obtain
  DNS Server by DHCP: no
  Preferred DNS: 10.102.6.247
  Alternate DNS: 0.0.0.0
  VLAN Enabled: no
  VLAN ID: 1
  VLAN Priority: 0
  Hostname: 4451-UCS-E
  MAC Address: E0:2F:6D:E0:F8:8A
  NIC Mode: dedicated NIC
  Redundancy: none
  NIC Interface: console

Router /cimc/network #
```

To upgrade CIMC to the latest firmware, see the Upgrading Firmware module of the *Getting Started Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine*.

Setting Up ESXi and Installing VSphere Client

Perform the following tasks to set up ESXi and install VSphere client.

Setting Up ESXi

1 Install ESXi by logging into the Cisco Integrated Management Controller (CIMC) GUI.
2 Click on the KVM console and click Add Image, to map the ESXi ISO as the virtual media. For more information, see the VMware vSphere ESXi Installation module of the *Cisco UCS C-Series Servers VMware Installation Guide*.
3 Power cycle UCS-E Series Blade from the CIMC home page by clicking the Power Cycle Server button.
4 ESXi setup launches from the virtual media. Complete the ESXi installation.
5 During the installation, you need to provide the IP address of the ESXi and the user ID and password to connect to it. This information is required during VSphere client installation. In our example, we are using 172.6.1.10 as the ESXi IP address, root as the user ID and cisco123 as the password.: cisco123

The dual-wide UCS E-Series Blade has four interfaces. The interface with the highest MAC address is Gigabit 3 on the front panel, the second highest interface is Gigabit 2 on the front panel, and the last two are internal

interfaces. The single-wide UCS E-Series Blade has three interfaces. The interface with the highest MAC address is Gigabit 2 on the front panel and the last two are internal interfaces.

Installing VSphere Client

1. Launch ESXi, and use the Download VSphere Client link to download VSphere set up and install it on your laptop.
2. After installation, launch the VSphere Client and login using the user ID and password that was generated during the EXSi installation. For example, here the user ID is root and password is cisco 123.

Setting up FirePOWER Sensor and FireSIGHT Virtual Machine

Perform the following task to set up FirePOWER Sensor and FireSIGHT virtual machine:

1. On the VSphere client console click on File > Deploy OVF Template.
2. Browse and choose the FirePOWER Sensor OVF for ESXi and complete the deployment.
3. Power on the Virtual Machine (VM) and configure an IP address, and so on for the FirePOWER Sensor.
4. Log into the FirePOWER Sensor console using authentication credentials. The default user ID is admin and password is Sourcefire. The password is case sensitive.
5. Configure the FirePOWER Sensor. Accept the End User License Agreement (EULA) and provide information about the IP address, mask, gateway, IP address of the DNS and so on.
6. Configure VSwitch interfaces on the ESXi and verify the three network adapters on the FirePOWER Sensor VM.
7. Spin the FireSIGHT VM and configure FireSIGHT. Ensure that FireSIGHT and the FirePOWER Sensor can communicate with each other on the TCP port 8305.
   The FireSIGHT VM can manage up to 25 physical or virtual 3D sensors.

   Login as admin and password as Sourcefire. The password is case sensitive. Once logged in, type "sudo su" to the "#" prompt. Switch to the /usr/local/sf/bin folder and run the configure-network script.

```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Tue May 27 23:59:46 2014

Copyright 2001-2013, Sourcefire, Inc. All rights reserved.
Sourcefire is a registered trademark of Sourcefire, Inc.
All other trademarks are property of their respective owners.

Sourcefire Linux OS v5.3.0 (build 52)
Sourcefire Virtual Defense Center 64bit v5.3.0 (build 571)

admin@Sourcefire3D:~$ sudo su
Password:

root@Sourcefire3D:/var/home/admin# cd /usr/local/sf/bin
root@Sourcefire3D:/usr/local/sf/bin# ./configure-network

Do you wish to configure IPv4? (y or n) y
Management IP address? 172.16.1.9
Management netmask? 255.255.255.0
Management default gateway? 172.16.1.1

Are these settings correct? (y or n) y

Do you wish to configure IPv6? (y or n) n
Updated network configuration.
Updated comms. channel configuration.
Please go to https://172.16.1.9/ or https://[]/ to finish installation.
```

8 Add FireSIGHT to the FirePOWER Sensor.
Decide on a registration key to communicate between the Sensor and FireSIGHT. The registration key used here is cisco123. On the Sensor console, configure the following command:

```
configure manager add 172.16.1.9 cisco123
```

9 Add the FirePOWER Sensor to FireSIGHT.
Log into FireSIGHT via the browser https://172.16.1.9 and add the IP address of the Sensor under devices. Use the same registration key cisco123 that was used in Step 8.

Adding License to FireSIGHT

1 Use the **ifconfig** command at the FireSIGHT console to get the MAC address of FireSIGHT.

```
root@Sourcefire3D:/usr/local/sf/bin# ifconfig

eth0      Link encap:Ethernet HWaddr 00:0C:29:15:2A:AB
          inet addr:172.16.1.9 Bcast:172.16.1.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feb8:980/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:992678 errors:0 dropped:0 overruns:0 frame:0
          TX packets:261784 errors:0 dropped:0 overruns:0 carrier:0 collisions:0
          txqueuelen:1000 RX bytes:541215916 (516.1 Mb) TX bytes:64866840 (61.8 Mb)
```

2 Get the license key from Cisco FirePOWER Threat Defense.
3 In the FireSIGHT GUI, go to System >> Licenses and click on add new license. Copy and paste the entire license key from Begin Product License File to End Product License File. Repeat this procedure for all features that you require.

Additional References for Cisco FirePOWER Threat Defense IPS Mode

Related Documents

Related Topic	Document Title
IOS commands	Cisco IOS Master Command List, All Releases
Security commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z

Related Topic	Document Title
UCS E-Series Servers	http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/e/2-0/gs/guide/b_2_0_Getting_Started_Guide.html

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Cisco FirePOWER Threat Defense IPS Mode

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Cisco FirePOWER Threat Defense IPS Mode

Feature Name	Releases	Feature Information
Cisco FirePOWER Threat Defense IPS Mode	Cisco IOS Release 15.5(1)T	Cisco FirePOWER Threat Defense is Cisco's premier network security option. It provides a comprehensive suite of security features such as firewall capabilities, monitoring, alerts, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). Deploy the FirePOWER Sensor on a Cisco Unified Computing System (UCS) E-Series Blade in IPS mode to configure IPS inspection. IPS inspects the traffic, and if configured, will drop the traffic block that it determines as network intrusions.