使用UCS-E刀片在ISR裝置上配置FirePOWER服務

目錄

簡介 必要條件 需求 <u>採用元件</u> 背景<u>資訊</u> 支援的硬體平台 採用UCS-E刀片的ISR G2裝置 採用UCS-E刀片的ISR 4000裝置 授權 限制 設定 網路圖表 UCS-E上FirePOWER服務的工作流程 配置CIMC 連線到CIMC 配置CIMC 安裝ESXi 安裝vSphere客戶端 下載vSphere客戶端 啟動vSphere客戶端 部署FireSIGHT管理中心和FirePOWER裝置 介面 ESXi上的vSwitch介面 向FireSIGHT管理中心註冊FirePOWER裝置 重新導向和驗證流量 將通訊量從ISR重定向到UCS-E上的感測器 驗證封包重新導向 驗證 疑難排解 相關資訊

簡介

本檔案介紹如何在入侵偵測系統(IDS)模式下在Cisco Unified Computing System E系列(UCS-E)刀 鋒平台上安裝和部署Cisco FirePOWER軟體。本文檔中介紹的配置示例是對官方使用手冊的補充。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- Cisco Integrated Services Routers(ISR)XE image 3.14或更高版本
- •思科整合式管理控制器(CIMC)版本2.3或更新版本
- Cisco FireSIGHT管理中心(FMC)版本5.2或更高版本
- Cisco FirePOWER虛擬裝置(NGIPSv)版本5.2或更高版本
- VMware ESXi版本5.0或更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

附註:在將代碼升級到版本3.14或更高版本之前,請確保系統具有足夠的記憶體、磁碟空間以 及升級許可證。請參閱<u>範例1:將映像複製到flash:從TFTP伺服器部</u>分,從Access Routers軟體 升級過程思科文檔瞭解更多有關代碼升級的資訊。

附註:要升級CIMC、BIOS和其他韌體元件,您可以使用Cisco Host Upgrade Utility(HUU),也可以手動升級韌體元件。要瞭解有關韌體升級的詳細資訊,請參閱Cisco UCS E系列伺服器和Cisco UCS E系列網路計算引擎的主機升級實用程式使用手冊的<u>在Cisco</u> UCS E系列伺服器上升級韌體部分。

背景資訊

本節介紹與本文檔中介紹的元件和過程相關的支援的硬體平台、許可證和限制的相關資訊。

支援的硬體平台

本部分列出了G2和4000系列裝置支援的硬體平台。

採用UCS-E刀片的ISR G2裝置

支援以下具有UCS-E系列刀片的ISR G2系列裝置:

 産品
 平台
 UCS-E型號

 2911
 UCS-E 120/140單寬選件

 Cisco 2900系列ISR
 2921
 UCS-E 120/140/160/180單寬或雙寬選項

 2951
 UCS-E 120/140/160單寬或雙寬選項

 3925
 UCS-E 120/140/160單寬和雙寬選項或180雙寬

 3925E
 UCS-E 120/140/160單寬和雙寬選項或180雙寬

 3945E
 UCS-E 120/140/160單寬和雙寬選項或180雙寬

採用UCS-E刀片的ISR 4000裝置

支援以下具有UCS-E系列刀片的ISR 4000系列裝置:

產品平台 UCS-E型號Cisco 4400系列ISR4451 UCS-E 120/140/160單寬和雙寬選項或180雙寬4431 UCS-E網路介面模組4351 UCS-E 120/140/160/180單寬和雙寬選項或180雙寬Cisco 4300系列ISR4331 UCS-E 120/140單寬選件4321 UCS-E網路介面模組

授權

ISR必須具有安全K9許可證以及appx許可證,才能啟用該服務。

限制

以下為與本檔案所述資訊有關的兩個限制:

- 不支援組播
- •每個系統僅支援4,096個網橋域介面(BDI)
- BDI不支援以下功能:
 - 雙向轉發檢測(BFD)協定
 - Netflow
 - •服務品質(QoS)
 - •網路型應用程式辨識(NBAR)或進階視訊編碼(AVC)
 - 區域型防火牆(ZBF)
 - 加密VPN
 - 多重協定標籤交換 (MPLS)
 - •乙太網路上的點對點通訊協定(PPP)(PPPoE)

附註:對於BDI,最大傳輸單元(MTU)大小可配置為1,500到9,216位元組之間的任何值。

設定

本節介紹如何配置與此部署相關的元件。

網路圖表

本檔案所述的組態使用以下網路拓撲:



FirePOWER Sensor VM (on UCS-E) 172.16.1.6

UCS-E上FirePOWER服務的工作流程

以下是在UCS-E上運行的FirePOWER服務的工作流程:

- 1. 資料平面將流量從BDI/UCS-E介面推出以進行檢查(適用於G2和G3系列裝置)。
- 2. Cisco IOS®-XE CLI啟用資料包重定向進行分析(所有介面或每個介面的選項)。
- 3. 感測器CLI設置啟動指令碼簡化了配置。

配置CIMC

本節介紹如何配置CIMC。

連線到CIMC

連線到CIMC的方法有多種。在本示例中,通過專用管理埠完成與CIMC的連線。確保使用乙太網電 纜將M埠(專用)連線到網路。連線後,在路由器提示符下運行hw-module subslot命令:

ISR-4451#**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 -110 receive_cmd is : rz -vv

提示1:要退出,請運行^a^q。

提示2:預設使用者名稱是admin,密碼為<password>。密碼重置過程如下所述 : <u>https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/e/3-1-</u> <u>1/gs/guide/b_Getting_Started_Guide/b_3_x_Getting_Started_Guide_appendix_01011.html#G</u> UID-73551F9A-4C79-4692-838A-F99C80E20A28

配置CIMC

使用以下資訊完成CIMC的配置:

```
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

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 64.102.6.247

Unknown /cimc/network *# set hostname 4451-UCS-E

Unknown /cimc/network *# commit
```

注意:確保運行commit命令以儲存更改。

附註:使用管理埠時,模式設定為dedicated。

執行show detail命令以驗證詳細資訊設定:

```
4451-UCS-E /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: 64.102.6.247
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
4451-UCS-E /cimc/network #
使用預設使用者名稱和密碼從瀏覽器啟動CIMC的Web介面,如下圖所示。預設使用者名稱和密碼
為:
```

• 使用者名稱:admin

•密碼:<password>

$\bullet \Rightarrow \bullet \bullet$ [] https://	172.16.1.8	
uhuhu cisco	Cisco Integrated Management Controller 4451-UCS-E	Username: <mark>admin</mark>
	Version: 2.1(1.20130726203500)	Password:

安裝ESXi

登入到CIMC的使用者介面後,您可以檢視與下圖所示類似的頁面。按一下Launch KVM Console圖示,按一下add image,然後將ESXi ISO對映為虛擬介質:

← → C & beeps://172.	16.1.8/index.html				☆ =
cisco Cisco Integ	grated Management Co	ntroller		CIMC Hostname: 4451-UCS-E Logged in as: admin@172.16.1.2	Log Out
Overall Server Status Good Server Admin Summary Inventory RAID Sensors System Event Log Remote Presence BIOS Power Policies Fault Summary Host Image Mapping	C C C C C C C C C C C C C C C C C C C	Server Properties Product Name: Serial Number: PID: UUD: BIOS Version: Description: Server Status Power Status: Power Status: Overall Server Status: Processors: Memory: Cisco Integrated Manage Hostname: IP Address: Firmware Version: CPLD Version: Hardware Version:	E1405 FOC17513BQL UCS-E1405-M1/K9 FOF75512-08F5-0000-3EDE-3FB206D80100 UCSE5.1.5.0.2 (Build Date: 05/15/2013)		
				Save Changes Rese	t Values

按一下Virtual Media頁籤,然後按一下Add Image以對映虛擬媒體,如圖所示。

] 172.16.1.8 - KVM Console					
File Help					
KVM Virtual Med	lia				
Client View					
Mapped Rei	ad Only Drive		Fxit		
	🖾 🔗 E: - CD/DVD				
	D: - Removable	Disk	Create Image		
			Add Image		
		🔊 Open	Remove Image		
		Look In: 14451 💌 🐼 🛱 🗂 🐯 🗁	Dotails +		
			Details		
		0.56-100-2.1.1.150			
•					
Details					
Target Drive	Mapped To	File Name: ESXI-5 1.0-799733-custom-Cisco-2.1.0.3 iso			
Virtual CD/DVD	Not mapped	Files of Type: Disk image file (* iso * ima)	USB Reset		
Removable Disk	Not mapped				
Floppy	Not mapped	Open Cancel			

對映虛擬介質後,從CIMC首頁點選**Power Cycle Server**以重新啟動UCS-E。ESXi安裝程式從虛擬 介質啟動。完成ESXi安裝。

附註:記錄ESXi IP地址、使用者名稱和密碼以供將來參考。

安裝vSphere客戶端

本節介紹如何安裝vSphere客戶端。

下載vSphere客戶端

啟動ESXi並使用Download VSphere Client連結下載vSphere客戶端。將其安裝在電腦上。

VMware ESXi 5.1 Welcome

Getting Started

If you need to access this host remotely, use the following program to install vSphere Client software. After running the installer, start the client and log in to this host.

+

Download vSphere Client

To streamline your IT operations with vSphere, use the following program to install vCenter. vCenter will help you consolidate and optimize workload distribution across ESX hosts, reduce new system deployment time from weeks to seconds, monitor your virtual computing environment around the clock, avoid service disruptions due to planned hardware maintenance or unexpected failure, centralize access control, and automate system administration tasks.

Download VMware vCenter

If you need more help, please refer to our documentation library:

vSphere Documentation

啟動vSphere客戶端

For Administrators

vSphere Remote Command Line

The Remote Command Line allows you to use command line tools to manage vSphere from a client machine. These tools can be used in shell scripts to automate day-to-day operations.

- Download the Virtual Appliance
- Download the Windows Installer (exe)
- Download the Linux Installer (tar.gz)

Web-Based Datastore Browser

Use your web browser to find and download files (for example, virtual machine and virtual disk files).

 Browse datastores in this host's inventory

For Developers

vSphere Web Services SDK

Learn about our latest SDKs, Toolkits, and APIs for managing VMware ESX, ESXi, and VMware vCenter. Get sample code, reference documentation, participate in our Forum Discussions, and view our latest Sessions and Webinars.

Learn more about the Web Services SDK

從電腦啟動vSphere客戶端。使用您在安裝期間建立的使用者名稱和密碼登入,如下圖所示:

🖉 VMware vSphere Client	
vmware VMware vSphere ^{**} Client	
In vSphere 5.5, all n through the vSphere will continue to opera vSphere 5.0, but no vSphere 5.5. The vSphere Client is Manager (VUM) and (e.g. Site Recovery I To directly manage a singl To manage multiple hosts, vCenter Server.	ew vSphere features are available only Web Client. The traditional vSphere Client ate, supporting the same feature set as t exposing any of the new features in s still used for the vSphere Update Host Client, along with a few solutions Manager). e host, enter the IP address or host name. enter the IP address or name of a
IP address / Name: User name: Password:	172.16.1.10 root ******* Use Windows session credentials Login Close Help

部署FireSIGHT管理中心和FirePOWER裝置

完成<u>在VMware ESXi思科上部署FireSIGHT管理中心</u>文檔中所述的步驟,以便在ESXi上部署 FireSIGHT管理中心。

附註:用於部署FirePOWER NGIPSv裝置的過程與用於部署管理中心的過程類似。

介面

在雙寬UCS-E上,有四個介面:

- •最大MAC地址介面是前面板上的Gi3
- 第二高MAC地址介面是前面板上的Gi2
- 顯示的最後兩個是內部介面

在單寬UCS-E上,有三個介面:

- •最大的MAC地址介面是前面板上的Gi2
- 顯示的最後兩個是內部介面

ISR4K上的兩個UCS-E介面都是中繼埠。

UCS-E 120S和140S有三個網路介面卡和管理埠:

- vmnic0對映到路由器背板上的UCSEx/0/0
- vmnic1對映到路由器背板上的UCSEx/0/1
- vmnic2對映到UCS-E前平面GE2介面
- •前面板管理(M)埠只能用於CIMC。

UCS-E 140D、160D和180D具有四個網路介面卡:

- vmnic0對映到路由器背板上的UCSEx/0/0。
- vmnic1對映到路由器背板上的UCSEx/0/1。
- vmnic2對映到UCS-E前平面GE2介面。
- vminc3對映到UCS-E前平面GE3介面。
- 前面板管理(M)埠只能用於CIMC。

ESXi上的vSwitch介面

ESXi上的vSwitch0是ESXi、FireSIGHT管理中心和FirePOWER NGIPSv裝置通過網路通訊的管理 介面。按一下vSwitch1(SF-Inside)和vSwitch2(SF-Outside)的**Properties**以進行更改。

lardware	View: vSphere Standard Switch	
Health Status	Networking	
Processors		
Memory	Standard Switch vSwitch0	Remove Properties)
Storage	- Virtual Machine Port Group	- Physical Adapters
Networking	🖓 VM Network	😡 💊 🖕 📾 vmnic2 1000 Full 📮
Storage Adapters	3 virtual machine(s)	
Network Adapters	4451-VMware vCenter Server Appl	
Advanced Settings	SFS	
Power Management	DC	
oftware	-VMkernel Port	
Licensed Features	vmk0 : 172.16.1.10	
Time Configuration	fe80::e22f:6dff:fee0:f888	
DNS and Pouting		
Authentication Services		
Virtual Machine Startun/Shutdown	Standard Switch: vSwitch1	Remove Properties
Virtual Machine Swapfile Location	Virtual Machine Port Group	Adapters
Sequrity Profile	SF-Inside	vmnic0 1000 Full
Host Cache Configuration	I virtual machine(s)	
System Resource Allocation	SFS C +	
Agent VM Settings		
Advanced Settings	Standard Switch vSwitch2	Remove Properties)
Advanced Setungs	Virtual Machine Port Group Physica	Adapters
	SF-Outside	vmnic1 1000 Full 🖓
	1 virtual machine(s) VLAN ID: 20	Constant of the Constant of th
	ere Pa	

此圖顯示vSwitch1的屬性(您必須為vSwitch2完成相同的步驟):

附註:確保將NGIPSv的VLAN ID配置為4095,根據NGIPSv文檔,這是必需的

: <u>http://www.cisco.com/c/en/us/td/docs/security/firepower/60/quick_start/ngips_virtual/NGIP</u> <u>Sv-quick/install-ngipsv.html</u>

vSwitch1 Properties torts Network Adapters Port Group Properties Network Label: SF-Inside VLAN ID: None (0) Effective Policies Security Promiscuous Mode: Accept ACCept Forged Transmits: Accept Traffic Shaping Average Bandwidth: Peak Bandwidth:							
Nrbs Network Adapters Port Group Properties Network Label: SF-Inside VLAN ID: None (0) Effective Policies Security Promiscuous Mode: Accept Accept Proged Transmits: Accept Forged Transmits: Peak Bandwidth: Peak Bandwidth		General Security Traffic Shaping NIC Teaming					witch1 Properties
Configuration Summary		Policy Exceptions				's	Network Adapters
Security Promiscuous Mode: Accept MAC Address Changes: Accept MAC Address Changes: Accept Forged Transmits: Accept Traffic Shaping	• •	Promiscuous Mode: Recept MAC Address Changes: Accept Forged Transmits: Accept		side (0)	Port Group Properties Network Label: SF- VLAN ID: Nor Effective Policies	Summary 120 Ports Virtual Machine	onfiguration vSwitch SF-Inside
Standby Adapters: None			E	Accept Accept Port ID Link status only Yes Yes	Security Promiscuous Mode: MAC Address Changes: Forged Transmits: Traffic Shaping Average Bandwidth: Peak Bandwidth: Burst Size: Failover and Load Balancing Load Balancing: Network Failure Detection: Notify Switches: Failback: Catile Advectors:		
Add Edit Remove Unused Adapters: None			•	None None	Standby Adapters: Unused Adapters:	Edit Remove	Add (
Close Help			Help				

- 1. 導航到FirePOWER裝置的虛擬機器。
- 2. 按一下Edit virtual machine settings。
- 3. 檢驗所有三個網路介面卡。
- 4. 確保正確選擇它們, 如下圖所示:

	SFS - Virtual Machine Properties	
SEC	Hardware Options Resources	Virtual Machine Version: 7
Getting Started Summary Resource Allocation	Show All Devices Add Remo	ove Device Status
 What is a Virtual Machine? A virtual machine is a software computer the physical computer, runs an operating system installed machine is called a guest operating system installed machine is called a guest operating system. Because every virtual machine is an isolate environment, you can use virtual machines workstation environments, as testing environsolidate server applications. Virtual machines run on hosts. The same is many virtual machines. Basic Tasks Power Off the virtual machine Suspend the virtual machine Edit virtual machine settings 	Hardware Summary Memory 4096 MB CPUs 4 Video card Video card VMCI device Restricted SCSI controller 0 LSI Logic Parallel Hard disk 1 Virtual Disk Network adapter 1 VM Network Network adapter 2 SF-Inside Network adapter 3 SF-Outside	✓ Connect at power on Adapter Type Current adapter: E 1000 MAC Address 00:0c:29:19:df:3a ⓒ Automatic Manual DirectPath I/O Status: Not supported ③ Network label: SF-Inside SF-Inside SF-Joutside VM Network
	Help	OK Cancel

向FireSIGHT管理中心註冊FirePOWER裝置

完成思科文檔中所述的程式,以便向FireSIGHT管理中心註冊FirePOWER裝置。

重新導向和驗證流量

使用本節內容,確認您的組態是否正常運作。

本節介紹如何重新導向流量以及如何驗證封包。

將通訊量從ISR重定向到UCS-E上的感測器

使用以下資訊重新導向流量:

interface GigabitEthernet0/0/1
ip address dhcp
negotiation auto
!
interface ucse2/0/0
no ip address
no negotiation auto

```
switchport mode trunk
no mop enabled
no mop sysid
service instance 1 ethernet
encapsulation untagged
bridge-domain 1
!
interface BDI1
ip unnumbered GigabitEthernet0/0/1
end
!
utd
mode ids-global
ids redirect interface BDI1
```

附註:如果當前運行的是3.16.1版或更高版本,請運行**utd engine advanced**命令,而不是 **utd**命令。

驗證封包重新導向

在ISR控制檯中運行此命令,以驗證資料包計數器是否增加:

cisco-ISR4451 # show plat hardware qfp active feature utd stats

```
Drop Statistics:
Stats were all zero
General Statistics:
Pkts Entered Policy 6
Pkts Entered Divert 6
Pkts Entered Recycle Path 6
Pkts already diverted 6
Pkts replicated 6
Pkt already inspected, policy check skipped 6
Pkt set up for diversion 6
```

```
驗證
```

您可以執行以下show命令以驗證您的組態是否正常運作:

- show platt software utd global
- · show platt software utd interfaces
- · show platt software utd rp active global
- · show platt software utd fp active global
- · show platt hardware qfp active feature utd stats
- · show platform hardware qfp active feature utd

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

您可以運行以下debug命令對組態進行疑難排解:

- debug platform condition feature utd controlplane
- · debug platform condition feature utd dataplane submode

相關資訊

- Cisco UCS E系列伺服器和Cisco UCS E系列網路計算引擎入門指南2.x版
- Cisco UCS E系列伺服器和Cisco UCS E系列網路計算引擎故障排除指南
- Cisco UCS E系列伺服器和Cisco UCS E系列網路計算引擎入門指南2.x版 升級韌體
- Cisco ASR 1000系列聚合服務路由器軟體配置指南 配置網橋域介面
- <u>Cisco UCS E系列伺服器和Cisco UCS E系列網路計算引擎的主機升級實用程式使用手冊 升</u> 級Cisco UCS E系列伺服器上的韌體
- 技術支援與文件 Cisco Systems