# 更改由FMC管理的FTD上的管理接口IP地址

### 目录

<u>先决条件</u>		
<u>要求</u>		
使用的组件		
<u>配置</u>		
<u>配置</u>		
<u>验证</u>		
<u>故障排除</u>		
<u>相关信息</u>		

## 简介

本文档介绍如何更改由安全防火墙管理中心管理的防火墙威胁防御设备的管理IP。

# 先决条件

#### 要求

Cisco 建议您了解以下主题:

- 思科安全防火墙管理中心(FMC)
- 思科安全防火墙威胁防御(FTD)

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 运行版本7.2.5(1)的安全防火墙管理中心虚拟
- 运行版本7.2.4的思科安全防火墙威胁防御虚拟

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

### 配置

#### 配置

步骤1:导航到FMC GUI,然后转到Device > Device Management。

第二步:选择设备,然后找到管理部分。

Frepower					
Cisco Firepower Threat Defense for VMware					
Device Routing Interfaces Inli	ine Sets DHCP VTEP				
General	/±=	License	/	System	0 G
Name:	Frepower	Performance Tier :	FTDv50 - Tiered (Core 12 / 24 GB)	Model:	Cisco Firepower Threat Defense for VMware
Transfer Packets:	Yes	Base:	Yes	Serial:	9A0HJUS0J27
Mode:	Routed	Export-Controlled Features:	No	Time:	2024-04-12 00:57:32
Compliance Mode:	None	Malware:	Yes	Time Zone:	UTC (UTC+0:00)
TLS Crypto Acceleration:	Disabled	Threat	Yes	Version:	7.2.4
		URL Filtering:	Yes	Time Zone setting for Time based Rules:	UTC (UTC+0:00)
Device Configuration:	Import Export Download	AnyConnect Apex:	No		
		AnyConnect Plus:	No		
		AnyConnect VPN Only:	No		
Inspection Engine		Health		Management	/ 🔍
Inspection Engine:	Snort 3	Status:	0	Host:	192.168.10.42
Revert to Snort 2		Policy:	Initial_Health_Policy 2024-04-08 17:12:48	Status:	•
		Excluded:	None	Manager Access Interface:	Management Interface
1		A CONTRACTOR OF			
Inventory Details	c	Applied Policies	/	Advanced Settings	/
CPU Type:	CPU Xeon 4100/6100/8100 series 2700 MHz	Access Control Policy:	Default 🕹	Application Bypass:	No
CPU Cores:	1 CPU (4 cores)	Prefilter Policy:	Default Prefilter Policy	Bypass Threshold:	3000 ms
Memory:	8192 MB RAM	SSL Policy:		Object Group Search:	Enabled
Storage:	N/A	DNS Policy:	Default DNS Policy	Interface Object Optimization:	Disabled
Chassis URL:	N/A	Identity Policy:			
Chassis Serial Number:	N/A	NAT Policy:			
Chassis Module Number:	N/A	Platform Settings Policy:			
Chassis Module Serial Number:	NA	QoS Policy:			
		the second second second second second			

#### 第三步:单击滑块关闭管理,然后选择是确认操作。

Device   Roufing   Intersider   PLT     General   PLT     Name:   Frepower     Transfer Packets:   Yes     Mode:   Roufed     Compliance Mode:   None     TLS Crypto Acceleration:   Device Configuration:     Device Configuration:   Intersider Packets:     Device Configuration:   Intersider Packets:     Mode:   Compliance Mode:     Device Configuration:   Intersider Packets:     Mode:   Compliance Mode:     Mode:   None     Maxware:   Yes     AnyConnect Paus:   None     AnyConnect Paus:   None     AnyConnect Paus:   None     Health   Massagement this device with not be providered for this based Rules:     Massagement this device with not be providered for this based Rules:   Massagement to be providered for this based Rules:     Massagement this device with not be providered for this based Rules:   Massagement to be providered for this based Rules:     Massagement to be providered for this device with not be providered for	
General   Image: System   System   Market     Name:   Frepower   Performance Tier:   FTDy50 - Tiered (Core 12 / 24 0B)   Model:   Cisco Firepower Threat Defense for Whw     Transfer Packets:   Ves   Base:   Ves   Serial:   3404UB0.     Mode:   Routed   Export-Controlled Features:   No   Time:   2024-04-12 01:14     Compliance Mode:   None   Mawre:   Ves   Time:   2024-04-12 01:14     Compliance Mode:   Disabled   Mawre:   Ves   Time:   2024-04-12 01:14     Device Configuration:   Disabled   Timest:   Ves   Time Zone:   UTC (UTc+o)     AnyConnect VPN of AnyConnect VPN of AnyConnect VPN of AnyConnect VPN of Disable Management   No   No   Time Zone setting for Time based Rules:   UTC (UTc+o)     Inspection Engine   Health   Masaging this device will not be provide tif if Management to be provide tif if Management to be provide to be provid	
General   Icense   System   System   System     Name:   Frequeers   Frequeers   Frequeers   Frequeers   Frequeers   Model:   Claco Frequeers for View     Transfer Packets:   Yes   Base:   Yes   Serial:   Seria:   Seria:   Seria:   Seria	
Name:   Frequence   Performance Tier:   FTDv50 - Tiered (Core 12 / 24 GB)   Model:   Claco Firepower Threat Defense for View     Transfer Packets:   Ves   Base:   Ves   Serial:   3A04LUS0.     Mode:   Routed   Export-Controlled Features:   No   Time:   2024-04-12 01:14     Compliance Mode:   None   Mawre:   Ves   Time:   2024-04-12 01:14     Compliance Mode:   None   Mawre:   Ves   Time:   2024-04-12 01:14     Compliance Mode:   None   Mawre:   Ves   Time:   2024-04-12 01:14     Device Configuration:   Disabled   Threet:   Ves   Version:   7     URL Filtering:   Ves   AnyConnect Apex:   No   Time Zone setting for Time based Rules:   UTC (UTc+outer)     Device Configuration:   Impedition Engine   Disable Management   No   No   AnyConnect View   No     Inspection Engine   Health   Masaging this device will not be exponent of big   No   Management big   Management big	0G
Tandfer Packets: Yes Serial: GAOH.USD.   Mode: Routed Export-Controlled Features: No Time: 2024-04-12 0.14   Compliance Mode: None Malware: Yes Time: 2024-04-12 0.14   Compliance Mode: None Malware: Yes Time: 2024-04-12 0.14   Compliance Mode: None Malware: Yes Time: 2024-04-12 0.14   TLS Crypto Acceleration: Disable Time: Yes Yes Time Zone: UTC (UTC+0)   Device Configuration: Impert features: No AnyConnect Apex: No Time Zone setting for Time based Rules: UTC (UTC+0)   Inspection Engine Health Masaging this device will not be exponent to be No No Management	vare
Mode: Routed Export-controlled Features: No Time: 2024-04-12 01:14   Compliance Mode: None Maiware: Ves Time Zone: UTC (UTC 40)   TLS Crypto Acceleration: Disabled Time: Ves Version: 7   Device Configuration: Image: Count of the Count	J27
Compliance Mode: None Makware: Yes Time Zone: UTC (UTC+0)   TLS Crypto Acceleration: Disabled Timet: Yes Version: 7   Device Configuration: meet Tool Tool Tool Tool Tool Tool Tool Too	4:15
TLS Crypto Acceleration: Disabled Threat: Yes Version: 7   Device Configuration: Image: Loop Township (Life Internation Connect Apex: AnyConnect Apex: No No AnyConnect Apex: No AnyConnect Apex: No   Inspection Engine Health Management Pia No Management Pia	:00)
Device Configuration: West Stoor Vest AnyConnect Apex: No   AnyConnect VPN O Disable Management No   Inspection Engine Health Management Pis	.2.4
Device Configuration: Import Example AnyConnect Apex: No   AnyConnect VPN 0 Disable Management No   Inspection Engine Health Management Pis	:00)
AnyConnect Plus: No AnyConnect VPN O Disable Management No Inspection Engine Health Management Plus Management Plus	
AmyConnect VPN O     Disable Management     No       Inspection Engine     Health     Management P is consults fit is device will not be consults fit is dev	
Inspection Engine Health Managing this device will not be cossible if it's Management P is Management P is	
Inspection Engine Health Managing this device will not be Management	
Inspection Engine: Short 3 Status: disabled. Do you want to proceed? You Plat: 192.168.10	0.42
Reserve to toor 2 Policy: 124-04-08 17:12	0
Excluded: None Manager Access Interface: Management Interf	face
Inventory Details c Applied Policies / Advanced Settings	/
CPU Xeon 4100/6100/8100 series 2700 Access Control Policy: Detail: Access Control Policy: Det	No
CPU Type: MHz Prefirer Policy: Default Prefirer Policy: Default Prefirer Policy: 0 2000	0 ms
CPU Cores: 1 CPU (4 cores) SSL Palloy: CPU	bled
Memory: 8192 MB RAM DRS Policy: Default DMS Policy: DM	bied
Storage: N/A Storage Distance of the storage Distance	



注意:关闭管理会中断管理中心和设备之间的连接,但将设备保留在管理中心内。

第四步:禁用管理后,选择编辑以编辑管理连接。

第五步:在管理对话框中,更改远程主机地址字段的IP地址,然后选择保存。



第六步:连接到FTD控制台以修改管理IP地址。



警告:如果通过管理IP地址建立会话,则更改管理IP地址可能导致设备的SSH连接丢失。因此,建议按照思科的建议,通过控制台访问执行此更改。

步骤 7.在Clish模式下,使用以下命令修改管理IP地址:

> configure network ipv4 manual 192.168.10.49 255.255.0.0 192.168.255.254



注意:默认情况下,此配置应用于管理接口。

步骤 8返回到FMC GUI,并通过将滑块切换到On位置来重新激活Management。

Management	/ 🔍
Host:	192.168.10.49
Status:	9
Manager Access Interface:	Management Interface

步骤 9请注意,重新建立管理连接可能需要一些时间;成功重新连接如下图所示:

Management	/ 🔍
Host:	192.168.10.49
Status:	0
Manager Access Interface:	Management Interface

### 验证

使用本部分可确认配置能否正常运行。

您可以通过FTD CLI验证管理连接。这通过连接到CLI并在Clish模式下运行以下命令来实现:

> sftunnel-status

Check routes: No peers to check

### 故障排除

本部分提供了可用于对配置进行故障排除的信息。

 要验证FTD CLI中的管理连接状态,请运行命令show sftunnel status brief。观察已关闭连接的 输出,该连接由未连接到对等体通道详细信息和缺少心跳信息指示。

> sftunnel-status-brief

PEER:192.168.10.40 Registration: Completed. Connection to peer '192.168.10.40' Attempted at Fri Apr 19 21:14:23 2024 UTC Last disconnect time : Fri Apr 19 21:14:23 2024 UTC Last disconnect reason : Both control and event channel connections with peer went down 当FTD CLI上的sftunnel-status-brief命令生成包括连接到信息和心跳数据的对等体信道的输出时,将 确认设备之间的正常连接。

> sftunnel-status-brief

PEER:192.168.10.40 Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '192.168.10.40' via '192.168 Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '192.168.10.40' via '192.168.1 Registration: Completed. IPv4 Connection to peer '192.168.10.40' Start Time: Fri Apr 19 21:12:59 2024 UTC Heartbeat Send Time: Fri Apr 19 21:13:00 2024 UTC Heartbeat Received Time: Fri Apr 19 21:13:23 2024 UTC Last disconnect time : Fri Apr 19 21:12:57 2024 UTC Last disconnect reason : Process shutdown due to stop request from PM

• 要检查网络连接,从管理接口ping管理中心,并在FTD CLI中输入ping system fmc\_ip。

# 相关信息

- 设备管理基础知识
- <u>思科技术支持和下载</u>

#### 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。