在 Firepower 设备上安装和升级 FTD

目录
<u>简介</u>
先决条件
使用的组件
<u>背景信息</u>
<u>网络图</u>
<u>任务1.FTD软件下载</u>
任务2.验证FXOS-FTD兼容性
任务3.将FTD映像上传到Firepower设备
任务4.配置FTD管理和数据接口
任务5.创建和配置新的逻辑设备
任务6.将FTD注册到Firepower管理中心(FMC)
<u>任务7.升级FTD</u>
<u>解决方案</u>
<u>确认</u>
Firepower 2100
<u>在FP2100上安装FTD</u>
FP2100上的FTD升级
<u>故障排除</u>
相关信息

简介

本文档介绍如何在Firepower设备上安装、升级和注册Firepower威胁防御(FTD)软件。

先决条件

要求

本文档没有任何特定的要求。

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FXOS 2.0(1.37)的Cisco Firepower 4140安全设备

• 运行6.1.0.330的Firepower管理中心

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。

背景信息

FTD是可在以下平台上安装的统一软件映像:

- ASA5506-X、ASA5506W-X、ASA5506H-X、ASA5508-X、ASA5516-X
- ASA5512-X、ASA5515-X、ASA5525-X、ASA5545-X、ASA5555-X
- Firepower设备(FPR2100、FPR4100、FPR9300)
- VMware (ESXi)
- Amazon Web Services (AWS)
- 基于内核的虚拟机(KVM)
- 集成多业务路由器(ISR)模块



网络图



任务1.FTD软件下载

导航到下一代防火墙(NGFW) > FirePOWER 4100系列> FirePOWER 4140安全设备,然后选择 Firepower威胁防御软件(如图所示)。 Download Software

10 Ite Download Cart (0 ite

Downloads Home > Products > Security > Firewalls > Next-Generation Firewalls (NGFW) > Firepower 4100 Series > Firepower 4140 Security Appliance

Select a Software Type:

Adaptive Security Appliance (ASA) Device Manager Adaptive Security Appliance (ASA) Software Adaptive Security Appliance REST API Plugin Firepower Extensible Operating System Firepower Threat Defense Software

任务2.验证FXOS-FTD兼容性

任务要求

验证机箱上运行的FXOS版本是否与要在安全模块中安装的FTD版本兼容。

解决方案

步骤1:检查FXOS-FTD兼容性。

在将FTD映像安装到模块/刀片之前,请确保Firepower机箱运行兼容的FXOS软件。在《FXOS兼容 性指南》中,检查逻辑设备兼容性表。运行FTD 6.1.x所需的最低FXOS版本为1.1(4.95),如表2所 示:

Table 2 Logical Device Compatibility

FXOS	ASA OS	Firepower Threat Defense
1.1(1.147)	9.4(1)	not supported
1.1(1.160)	9.4(1)	
1.1(4.95)	9.6(1)	6.0.1.x
	9.6(2)	6.1

如果FXOS映像与目标FTD映像不兼容,请先升级FXOS软件。

验证FXOS映像

方法 1.从Firepower机箱管理器(FCM) UI概述页面,如图所示:



方法 2. 导航到FCM System > Update页,如图所示:

Overview Interfaces	Logical Devices Security Engine Platform Settings						System	Tools	нөр	admin
					Configuration	Licensing	Updates	User	Manag	ement
Available Updates						C Refresh	Upload Image			×
Image Name		Туре	Version	Status	Bu	ild Date				
fxos-k9.2.0.1.23.SPA		platform-bundle	2.0(1.23)	Not-Installed	05	/18/2016		5	8	
fxos-k9.2.0.1.37.SPA		platform-bundle	2.0(1.37)	Installed	05	/11/2016			8	
fxos-k9.2.0.1.4.SPA		platform-bundle	2.0(1.4)	Not-Installed	04	/06/2016		5	8	

方法 3.从FXOS CLI:

<#root>

FPR4100#

show fabric-interconnect firmware

```
Fabric Interconnect A:
Running-Kern-Vers: 5.0(3)N2(4.01.35)
Running-Sys-Vers: 5.0(3)N2(4.01.35)
```

Package-Vers: 2.0(1.37)

Startup-Kern-Vers: 5.0(3)N2(4.01.35)
Startup-Sys-Vers: 5.0(3)N2(4.01.35)
Act-Kern-Status: Ready
Act-Sys-Status: Ready
Bootloader-Vers:

任务3.将FTD映像上传到Firepower设备

任务要求

将FTD映像上传到FPR4100机箱。

解决方案

方法1-从FCM UI上传FTD映像。

登录FPR4100机箱管理器并导航到System > Updates选项卡。选择Upload Image上传文件,如图 所示。

Overview Interfaces	Logical Devices Security Engine Platform Settings						System	Tools	Help	admin
					Configuration	Licensing	Updates	User	Manag	jement
Available Updates						C Refresh	Upicad Image			×
Image Name		Туре	Version	Status	Bui	ld Date				
fxos-k9.2.0.1.23.SPA		platform-bundle	2.0(1.23)	Not-Installed	05/	18/2016		5	8	
fxos-k9.2.0.1.37.SPA		platform-bundle	2.0(1.37)	Installed	06/	11/2016			8	
fxos-k9.2.0.1.4.SPA		platform-bundle	2.0(1.4)	Not-Installed	04/	06/2016		5	8	

浏览并选择FTD映像文件,然后单击Upload,如图所示:

Upload Image	?×
Select File : Browse cisco-ftd.6.1.0.330.SPA.csp	
Upload	Cancel

接受最终用户许可协议(EULA)。

验证如图所示。

Overview	Interfaces	Logical Devices	Security Engine	Platfor	m Settings				System	Tools	Help	admin
							Configuration	Licensing	Updates	User	Manaç	gement
Available	Updates							C Refresh	Upioad Image	Filter.		×
Image Name			Туре		Version	Status		Build Date				
fxos-k9.2.0.1.8	6.SPA		platfor	m-bundle	2.0(1.86)	Installed		10/15/2016			8	
fxos-k9.2.0.1.4	.SPA		platfor	m-bundle	2.0(1.4)	Not-Installed		04/06/2016			% 8	
cisco-ftd.6.1.0	.330.csp		ftd		6.1.0.330	Not-Installed		08/26/2016			8	

方法2 -从FXOS CLI上传FTD映像

您可以从FTP、Secure Copy (SCP)、Secure FTP (SFTP)或TFTP服务器上传FTD映像。

在映像传输开始之前,验证机箱管理接口和远程服务器之间的连接:

<#root>

FPR4100#

connect local-mgmt

FPR4100(local-mgmt)#

ping 10.229.24.22

PING 10.229.24.22 (10.229.24.22) from 10.62.148.88 eth0: 56(84) bytes of data. 64 bytes from 10.229.24.22: icmp_seq=1 ttl=124 time=0.385 ms 64 bytes from 10.229.24.22: icmp_seq=2 ttl=124 time=0.577 ms 64 bytes from 10.229.24.22: icmp_seq=3 ttl=124 time=0.347 ms

要下载FTD镜像,请导航到此范围并使用download image命令:

<#root>

FPR4100#

scope ssa

FPR4100 /ssa #

scope app-software

FPR4100 /ssa/app-software #

download image ftp://ftp_username@10.229.24.22/cisco-ftd.6.1.0.330.SPA.csp

Password:

要监控映像上传进度,请执行以下操作:

<#root>

FPR4100 /ssa/app-software #

show download-task detail

Downloads for Application Software:

File Name: cisco-ftd.6.1.0.330.SPA.csp

Protocol: Ftp Server: 10.229.24.22 Port: 0 Userid: ftp Path: Downloaded Image Size (KB): 95040 Time stamp: 2016-12-11T20:27:47.856

State: Downloading

Transfer Rate (KB/s): 47520.000000

Current Task: downloading image cisco-ftd.6.1.0.330.SPA.csp from 10.229.24.22(FSM-STAGE:sam:dme:App

使用以下命令验证下载是否成功:

<#root>

FPR4100 /ssa/app-software #

show download-task

Dowr	loads for	Application Software	:				
	File Name		Protocol	Server	Port	Userid	State
	cisco-ftd.	.6.1.0.330.SPA.csp	Ftp	10.229.24.22	0	ftp	

Downloaded

有关其他详细信息:

<#root>

```
KSEC-FPR4100 /ssa/app-software #
```

```
show download-task fsm status expand
```

```
File Name: cisco-ftd.6.1.0.330.SPA.csp
```

FSM Status:

Affected Object: sys/app-catalogue/dnld-cisco-ftd.6.1.0.330.SPA.csp/fsm

Current FSM: Download

Status: Success

Completion Time: 2016-12-11T20:28:12.889 Progress (%): 100

FSM Stage:

Order	Stage Name	Status	Try
1	DownloadLocal		

Success

1

2 DownloadUnpackLocal

Success

1 File Name: Cisco_FTD_SSP_Upgrade-6.1.0-330.sh

该图像显示在机箱存储库中:

<#root>

KSEC-FPR4100 /ssa/app-software # exit
KSEC-FPR4100 /ssa #

show app

Application: Name Version Description Author Deploy Type CSP Type Is Default App

asa 9.6.2.3 N/A cisco Native Application	ı No
--	------

ftd 6.1.0.330

N/A cisco Native Application No

任务4.配置FTD管理和数据接口

任务要求

在Firepower设备上为FTD配置并启用管理和数据接口。

解决方案

要创建新接口,请登录FCM并导航到Interfaces 选项卡。查看当前接口。要创建新的端口信道接口 ,请选择Add Port Channel按钮,如图所示:

Overview Interfaces Logical Devices Security Engine Platform Settings	System	Tools	Help	admin
Network Module 1Network Module 2 1 3 5 1 3 5 1 3 5 1 3 5 1 3 5 1 3 5 2 4 6 8 1 2 2 4 6				
All Interfaces Hardware Bypass				
		0	Add Port	Channel

步骤1:创建端口通道数据接口。

创建新的端口通道接口,如图所示:

端口通道ID	10
类型	数据
enable	Yes
成员ID	Ethernet1/1、Ethernet 1/2

端口通道ID为1到47之间的值。

💊 注意:PortChannel 48用于集群。

Add Port Ch	annel						? ×
Port Channel ID:	10		Enable				
Type:	Data	¥		1			
Admin Speed:	10gbps	v]				
Interfaces							
Ava	ailable Interface				Member ID		
	Search	2			Ethernet1/1	6	
	Ethernet1/1				Ethernet1/2	6	
	Ethernet1/2						
	Ethernet1/6		2				
	Ethernet1/7		5				
	Ethernet1/8		Add				
	Ethernet2/1		Interface				
	Ethernet2/2						

验证如图所示。

Overview Interfaces	Logical Device	es Security Engir	ne Platform Settings	i.		
CONSOLE MGMT	Networ USB 2	k Module 1 3 5 7 4 6 8	Network Module 2 1 3 5 2 4 6		Network Module 3	4
All Interfaces Hardware B	ypass					
Interface	Туре	Admin Speed	Operational Speed	Application	Operation State	Admin State
мдмт	Management					Enabled
Port-channel10	data	10gbps	10gbps		up	Enabled
Ethernet1/1					up	
Ethernet1/2					up	

第二步:创建管理接口。

在Interfaces 选项卡上,选择接口,选择Edit,然后配置管理接口,如图所示:

Edit Interface - Ethernet1/3								
Name:	Ethernet1/3 Zenable							
Type:	mgmt	•						
Admin Speed:	10gbps							
	OK Cancel)						

任务5.创建和配置新的逻辑设备

任务要求

创建FTD作为独立逻辑设备并进行部署。

解决方案

步骤1:添加逻辑设备。

导航到逻辑设备选项卡并选择添加设备按钮以创建新的逻辑设备,如图所示:

Overview	Interfaces	Logical Devices	Security Engine	Platform Settings	System	Tools	Help	admin
					C Refre	sh	Add D	evice
No logical devi	ces available. Cl	ick on Add Device to add	a new logical device.					

使用图中所示的设置配置FTD设备:

设备名	FTD
模板	Cisco Firepower威胁防御

映像版本

6.1.0.330

Add Device			?×
Device Name:	FTD		
Template:	Cisco Firepower Threat Defense	~	
Image Version:	6.1.0.330	~	
Device Mode:	Standalone		
	ОК		Cancel

第二步:引导逻辑设备。

创建逻辑设备后,将显示Provisioning - device_name窗口。选择设备图标开始配置,如图所示:

¢	Overview	Interfaces	Logi	cal Devices	Security Engine	Platform Setting	IS	System	Tools	Help	admin
s	P <mark>rovisionin</mark> tandalone	g - FTD Cisco Firep	ower 1	Threat Defense	e 6.1.0.330			Sav	/e	Cance	el
1	Data Ports										
	Ethernet1/4										
	Ethernet1/5							Click	her	6	
	Ethernet1/6							CHCK	nei	<u> </u>	4.1
	Ethernet1/7										
	Ethernet1/8										
	Ethernet2/1										
	Ethernet2/2										
	Ethernet2/3										
	Ethernet2/4					FTD - 6.1.0.3	30				
	Ethernet2/5					Click to configu	re				
	Ethernet2/6										
	Ethernet2/7										
	Ethernet2/8										
	Ethernet3/1										
	Ethernet3/2										
	Ethernet3/3										
	Ethernet3/4										
	Port-channel	10									
	Applicati	on Vers	ion	Management I	P Gateway	Management Port	Status				
Ξ	FTD	6.1.0	.330								

配置FTD常规信息选项卡,如图所示:

管理接口	Ethernet1/3
地址类型	仅IPv4
管理IP	10.62.148.84
网络掩码	255.255.255.128
网络网关	10.62.148.1

Cisco Firepower Threat Defense - Configuration										
General Information Settings Agreement										
Interface Information										
Management Interface:	Ethernet1/3									
Management										
Address Type:	IPv4 only									
IPv4										
Management IP:	10.62.148.84									
Network Mask:	255.255.255.128									
Network Gateway:	10.62.148.1									

配置FTD Settings选项卡,如图所示:

注册密钥	思科
密码	Pa\$\$w0rd
Firepower管理中心IP	10.62.148.50
搜索域	cisco.com
防火墙模式	路由
DNS Servers	192.168.0.1
完全限定的主机名	FTD4100.cisco.com
事件接口	-

Cisco Firepower Threat Defense - Configuration General Information Settings Agreement							
Registration Key:	•••••						
Password:	•••••						
Firepower Management Center IP:	10.62.148.50						
Search domains:	cisco.com						
Firewall Mode:	Routed	~					
DNS Servers:	192.168.0.1						
Fully Qualified Hostname:	FTD4100.cisco.com						
Eventing Interface:		~					

确保接受协议,然后选择确定。

第三步:分配数据接口。

展开数据端口(Data Ports)区域并选择要分配给FTD的每个接口。在此场景中,分配了一个接口 (Port-channel10),如图所示:

Ov	erview	Interfaces	Log	ical Device	Security Engine	e Platforr	n Settings		System	Tools	Help	admin
Pro Sta	o <mark>visionin</mark> Indalone	g - FTD Cisco Firep	ower	Threat Defei	nse 6.1.0.330				Sa	ve	Cance	2
Dat	a Ports											
Eti	hernet1/4											
Et	hemet1/5											
Et	hernet1/6											
Et	hernet1/7											
Et	hernet1/8											
Et	hemet2/1											
Et	hemet2/2											
Et	hemet2/3						2					
Et	hernet2/4			Port- channel10	Port-			FTD - 6.1.0.330				
Et	hernet2/5			6			(Ethernet1/3 Click to configure				
Et	hernet2/6							,				
Et	hernet2/7											
Et	hernet2/8											
Et	hernet3/1											
Eti	hernet3/2											
Eti	hernet3/3											
Et	hernet3/4	_										
Po	rt-channel	10										
	Applicati	on	Ve	ersion	Management IP	Gateway	Manager	nent Port	Statu	IS		
•	FTD		6.	1.0.330	10.62.148.84	10.62.148.1	Ethernet1	/3				
	Ports:											
	Data	Interfaces:	Por	t-channel10								

选择Save完成配置。

第四步:监控安装过程。

从FCM UI监控时,FTD安装过程如下(如图所示):

c	verview	Interfaces	Logical Devices	Security Engir	e Platform	Settings			System	Tools	Help	admin
									C Refi	resh) Add (Device
6	FTD	1	Standalone	Status: ok							8	/
	Applica	ition	Version	Mana	igement IP	Gateway	Management Port	Status				
6	FTD		6.1.0.330	10.62	.148.84	10.62.148.1	Ethernet1/3	📌 installing	Disabl	a) 🕅		
	Port	s:							•			
	Da	ta Interfaces:	Port-channel10									

Ov	erview Interfaces	Logical Device	es Secur	ity Engine Pl	atform Sett	tings		System T	ools Help	admin
								C Refresh	Add De	evice
	FTD	Standalone	Status: ok						P* 0	9 8
	Application	Version		Management IP	Gateway	Management Port	Status			
-	FTD	6.1.0.330	:	10.62.148.84	10.62.148.1	Ethernet1/3	offline	Enabled		
	Ports:	Port-channel10								
	Dudi Interfaces.	For chameric								
Ov	erview Interfaces	Logical Device	es Secur	ity Engine Pl	atform Sett	tings		System T	ools Help	admin
								C Refresh	Add De	evice
	FTD	Standalone	Status: ok						P+	
	Application	Version		Management IP	Gateway	Management Port	Status			
-	FTD	6.1.0.330	:	10.62.148.84	10.62.148.1	Ethernet1/3	🎇 starting	Enabled		
	Ports: Data Interfaces:	Port-channel10								
ov	erview Interfaces	Logical Devic	es Secur	ity Engine Pl	atform Sett	tings		System T	ools Help	admin
								C Refresh	Add De	evice
	FTD	Standalone	Status: ok						P+	
	Application	Version		Management IP	Gateway	Management Port	Status			
-	FTD	6.1.0.330	1	10.62.148.84	10.62.148.1	Ethernet1/3	💮 started	Enabled 🌒 💏		
	Ports:							-		
	Data Interfaces:	Port-channel10								

从Firepower CLI监控安装过程:

<#root>
FPR4100#
connect module 1 console
Telnet escape character is '~'. Trying 127.5.1.1 Connected to 127.5.1.1. Escape character is '~'.
CISCO Serial Over LAN: Close Network Connection to Exit
Cisco FTD: CMD=-start, CSP-ID=cisco-ftd.6.1.0.330ftd_001_JAD19500F7YHCNL7715, FLAG=''
Cisco FTD starting
Registering to process manager VNICs requested: 9,22 Cisco FTD started successfully. Cisco FTD initializing Firepower-module1>Setting up VNICs

Found Firepower management vnic 18. No Firepower eventing vnic configured. Updating /ngfw/etc/sf/arc.conf ... Deleting previous CGroup Configuration ... Initializing Threat Defense ... [OK] Starting system log daemon... Г ОК 1 Stopping mysql... Dec 12 17:12:17 Firepower-module1 SF-IMS[14629]: [14629] pmtool:pmtool [ERROR] Unable to connect to UNI Starting mysql... Dec 12 17:12:17 Firepower-module1 SF-IMS[14641]: [14641] pmtool:pmtool [ERROR] Unable to connect to UNI Flushing all current IPv4 rules and user defined chains: ...success Clearing all current IPv4 rules and user defined chains: ...success Applying iptables firewall rules: Flushing chain `PREROUTING' Flushing chain `INPUT' Flushing chain `FORWARD' Flushing chain `OUTPUT' Flushing chain `POSTROUTING' Flushing chain `INPUT' Flushing chain `FORWARD' Flushing chain `OUTPUT' Applying rules successed Flushing all current IPv6 rules and user defined chains: ...success Clearing all current IPv6 rules and user defined chains: ...success Applying ip6tables firewall rules: Flushing chain `PREROUTING' Flushing chain `INPUT' Flushing chain `FORWARD' Flushing chain `OUTPUT' Flushing chain `POSTROUTING' Flushing chain `INPUT' Flushing chain `FORWARD' Flushing chain `OUTPUT' Applying rules successed Starting nscd... mkdir: created directory '/var/run/nscd' Г ОК 1 Starting , please wait.....complete. Firstboot detected, executing scripts OK Executing S01virtual-machine-reconfigure Г ٦ ОК Executing S02aws-pull-cfg Ε ٦ Executing S02configure_onbox Ε OK] Executing SO4fix-httpd.sh Ε 0K] Executing SO6addusers Ε ОК ٦ Executing S07uuid-init OK Ε] Executing SO8configure_mysql Ε OK] ********** Attention ******** Initializing the configuration database. Depending on available system resources (CPU, memory, and disk), this may take 30 minutes or more to complete. ********** Attention ******** Executing S09database-init Ε OK] Executing S11database-populate Ε OK ٦ Executing S12install_infodb Г OK ٦ Executing S15set-locale.sh Ε OK ٦ Executing S16update-sensor.pl Ε OK] Executing S19cert-tun-init Ε OK] Executing S20cert-init Г OK 1

Executing S21disable_estreamer	Ε	OK]		
Executing S25create_default_des.pl	Γ	OK]		
Executing S30init_lights_out_mgmt.pl	Γ	OK]		
Executing S40install_default_filters.pl	Ε	ОК]		
Executing S42install_default_dashboards.pl	Ε	ОК]		
Executing S43install_default_report_templates.pl	Ε	ОК]		
Executing S44install_default_app_filters.pl	Ε	OK]		
Executing S45install_default_realms.pl	Ε	ОК]		
Executing S47install_default_sandbox_E0.pl	Ε	ОК]		
Executing S50install-remediation-modules	Ε	ОК]		
Executing S51install_health_policy.pl	Ε	OK]		
Executing S52install_system_policy.pl	Ε	OK]		
Executing S53change_reconciliation_baseline.pl	Ε	OK]		
Executing S70remove_casuser.pl	Ε	OK]		
Executing S70update_sensor_objects.sh	Γ	OK]		
Executing S85patch_history-init	Ε	OK]		
Executing S90banner-init	Γ	OK]		
Executing S96grow_var.sh	Γ	OK]		
Executing S96install_vmware_tools.pl	Γ	OK	נ		
***** Attention ********					
Initializing the system's localization settings. Depending on av	aila	ble			
system resources (CPU, memory, and disk), this may take 10 minute	S	~			
or more to complete.					
********* Attention *********					
Executing S96localize-templates	Ε	OK]		
Executing S96ovf-data.pl	Ε	OK]		
Executing S97compress-client-resources	Ε	OK]		
Executing S97create_platinum_forms.pl	Ε	OK]		
Executing S97install_cas	Ε	OK]		
Executing S97install_cloud_support.pl	Ε	OK]		
Executing S97install_geolocation.pl	Ε	ОК]		
Executing S97install_ssl_inspection.pl	Ε	ОК]		
Executing S97update_modprobe.pl	Ε	ОК]		
Executing S98check-db-integrity.sh	Ε	ОК]		
Executing S98htaccess-init	Ε	ОК]		
Executing S98is-sru-finished.sh	Ε	ОК]		
Executing S99correct_ipmi.pl	Ε	ОК]		
Executing S99start-system	Ε	ОК]		
Executing S99z_db_restore	Ε	ОК]		
Executing S99_z_cc-integrity.sh	Ľ	OK]		
Firstboot scripts finished.	_		_		
Configuring NTP]	OK]		
insmod: ERROR: could not insert module /lib/modules/kernel/drivers/u	10/1	gb_u	10.	ko: File exists	
rw console=ttyS0,38400 loglevel=2 auto kstack=128 reboot=force panic	=1 i	de_g	ene	ric.probe_mask=0x1 i	del=
Fru Size : 512 bytes					
Done					
VNIC command successful					
VNIC command successful					
fatattr: FAI_10CIL_GEI_AITRIBUTES: Inappropriate foct for device					
Tatattr: can't open '/mnt/disk0/.private2': No such file or director	У				
<pre>tatattr: can't open /mnt/diskU/.ngtw': No such file or directory</pre>					
Model reconfigure detected, executing scripts					
Pinging mysql					
Found mysql is running	-	011	-		
Executing 45update-sensor.pl	L	UK	Ţ		
Executing Sprecalculate_arc.pl	L	UK	L		
Mon Dec 12 17:16:15 UIC 2016					
Starting MySQL					
ringing mysql					

Pinging mysql, try 1 Found mysql is running Detecting expanded storage... Running initializeObjects... Stopping MySQL... Killing mysqld with pid 32651 Wait for mysqld to exit\c done Mon Dec 12 17:16:21 UTC 2016 Starting sfifd... [OK] Starting Cisco Firepower 4140 Threat Defense, please wait...No PM running! ...started. Cisco FTD initialization finished successfully. ... output omitted ... Reading from flash... Cryptochecksum (changed): blabfa7e 63faee14 affdddb0 9bc9d8cd INFO: Power-On Self-Test in process. INFO: Power-On Self-Test complete. INFO: Starting HW-DRBG health test (DRBG 0)... INFO: HW-DRBG health test (DRBG 0) passed. INFO: Starting HW-DRBG health test (DRBG 1)... INFO: HW-DRBG health test (DRBG 1) passed. INFO: Starting SW-DRBG health test... INFO: SW-DRBG health test passed. Firepower-module1> Firepower-module1> show services status Services currently running: Feature | Instance ID | State | Up Since _____ ftd | 001_JAD19500F7YHCNL7715 | RUNNING | :00:08:07

任务6.将FTD注册到Firepower管理中心(FMC)

任务要求

在FMC中注册FTD。

解决方案

步骤1:检验FTD和FMC之间的基本连接。

在向FMC注册FTD之前,请验证FTD和FMC之间的基本连接:

<#root>

Firepower-module1>

connect ftd

Connecting to ftd console... enter exit to return to bootCLI

>

ping system 10.62.148.50

PING 10.62.148.50 (10.62.148.50) 56(84) bytes of data. 64 bytes from 10.62.148.50: icmp_seq=1 ttl=64 time=0.133 ms 64 bytes from 10.62.148.50: icmp_seq=2 ttl=64 time=0.132 ms 64 bytes from 10.62.148.50: icmp_seq=3 ttl=64 time=0.123 ms

由于引导程序配置,FTD已配置管理器FMC:

<#root>

>

show managers

Host Registration Key Registration	::	10.62.148.50 ****
pending		
RPC Status	:	

第二步:将FTD添加到FMC。

在FMC上,导航到设备>设备管理选项卡,然后导航到添加…… > 添加设备,如图所示:

Overview Analysis	Policies	Devices	Object	s AMI	P	Deploy	Sy	rstem He	elp 🔻	admin 🔻
Device Management	NAT	VPN Q	oS Pla	tform Sett	ings					
						By Group		~) 4	۸dd
Name			Group	Model	License Type	Access Control Policy		Add D	evice	
4 🣁 Ungrouped (6)								Add H	ligh Ava	ailability

配置FTD设备设置,如图所示:

Add Device		?	×				
Host:	10.62.148.84						
Display Name:	FTD4100						
Registration Key:	cisco		1				
Group:	None	Y					
Access Control Policy:	FTD4100	Y					
Smart Licensing Malware:	 Image: A start of the start of						
Threat:							
URL Filtering:							
 Advanced On version 5.4 devices or earlier, the licensing options will need to be specified from <u>licensing page</u>. 							
	Register Cance	el					

选择Register按钮。

在FMC上,检查Tasks(任务)以查看注册进度。除了注册之外,FMC还:

- 发现FTD设备(检索当前接口配置)。
- 部署初始策略。

成功注册如图所示:

Overview Analysis Policies	Devices	Objects	АМР				Deploy	🛛 S	ystem	Help 🔻	admi	n v
Device Management NAT	VPN Qos	S Platfor	m Settings									
							By Group		*	0	Add	•
Name				Group	Model	License Type	Access Con	trol Polic	y			
 Ungrouped (7)		Cisco Fir	Base, Threat, Ma	FTD4100		6	9					

✤注意:在版本6.1中,引入了Firepower设备管理器(FDM)以提供机上管理。Firepower设备上 安装的FTD不能由FDM管理。

任务7.升级FTD

任务要求

将FTD从6.1.0.330升级到6.1.0.1。

解决方案

步骤1:验证兼容性。

检查FXOS发行版本注释以确保目标FTD版本与FXOS软件兼容。如果需要,请先升级FXOS软件。

第二步:升级FTD。

FTD软件由FMC而不是FCM管理。要升级FTD模块,请连接到FMC,导航到System > Updatespage,然后选择Upload Update,如图所示。

Overview	Analysis	Policies	Devices	Objects	AMP						Deploy		System
						Configuration	Users	Domains	Integration	Updates	Licenses 🔻	Health	v Mo
Product (Updates	Rule Up	dates (Geolocation	Updates								
				Currentl	y running software	version: 6.	1.0						
				Updat	es								
				Upload	software up	dates and patches	here.						
				Packag	2	Choose File Cis Upload Ca	co_FTD_SS	1.0.1-53.sh					

在FTD模块上安装更新,如图所示:

Overview	Analysis	Policies	Devices	Objects	AMP						Deploy	🔹 🛇 System
						Configuration	Users	Domains	Integration	Updates	Licenses 🔻	Health v M
Product U	Ipdates	Rule Up	dates	Geolocation	Update	s						
												🔾 Upload Update
Currently runni	Currently running software version: 6.1.0											
Updates												
Туре						Version	Date			Release Note	es <u>Reboot</u>	
Sourcefire Vu	Inerability Ar	d Fingerprin	t Database	Updates		275	Wed	Nov 16 16:50	:43 UTC 2016		No	i
Cisco FTD SS	P Patch					6.1.0.1-53	Fri De	ec 2 17:37:52	UTC 2016		Yes	🐞 🗒

或者,您可以启动就绪性检查:

Product Updates Rule Updates		Geolocation Updates			
				Currently running software ve	ersion: 6.1.0
Selected Upd	late				
Type Version Date Release Notes Reboot	Cisco FTD SSP Patch 6.1.0.1-53 Fri Dec 2 17:37:52 UTC 2016 e Notes t Yes				By Group ▼
Ungrouped	(1 tota	al)			
FTD4100 10.62.148.84	- Cisco I	Firepower 4140 Threat (Defense v6.1.0	Health Policy Initial Health Policy 2 12:21:09	016-11-21 🥥 📀
				Launch Readiness Check	Install Cancel

成功的就绪性检查如图所示:

Readiness Check Status									
Current Version: 6.1									
Update Version: 6.1.0.1-53									
Readiness Check Complete									
Total 1 devices Selected									
FTD4100 10.62.148.84 - Cisco Firepower 4140 Threat Defensev6.1.0									
Status Log:Readiness Check To 10.62.148.84 Success									

要启动升级过程,请单击Install,如图所示:

Product Upd	ates Rule Updates	Geolocation Updates	
		Currently running	software version: 6.1.0
Selected Up	date		
Type Version Date Release Notes Reboot	Cisco FTD SSP Patch 6.1.0.1-53 Fri Dec 2 17:37:52 UTC 2 Yes	16	By Group •
V Tungroupe	d (1 total)		
✓ FTD4100 10.62.148.84	- Cisco Firepower 4140 Thr	at Defense v6.1.0	Health Policy Initial Health Policy 2016-11-21 🥥 📀 12:21:09
			Launch Readiness Check Install Cancel

升级需要FTD重新启动,如图所示:

10.62.148.50 says:		×				
Update installation will reboot the system(s). Are you sure you want to continue?						
	ОК	Cancel				

与FTD安装类似,可以从FMC UI (Tasks)监控FTD升级过程。可以从FTD CLI(CLISH模式)跟踪 升级进度。

升级完成后,将策略部署到FTD,如图所示:

				Depk	oy 📀	System	Help 🔻	adm	in v
De	eployments	Health	Tasks					٥	?
2	0+ total	0 waiting	0 running	0 retrying	20+ su	ccess 0 f	ailures		
~	Remote Instal						12m 3	55s X	-
	Apply to 1 Please rea	0.62.148.8 pply polici	4. es to your	managed de	vices.				

确认

从FMC UI中,如图所示:

Overview	Analysis	Policies	Dev	ices 0	bjects	AMP	
Device Mar	agement	NAT	VPN	QoS	Platform	Settings	
Name							Group
Ungroe Street Ungroe	uped (7) 94100 52.148.84 - Ci	sco Firepow	er 4140	Threat Def	ense v6.1.	0.1 route	

从FCM UI中,如图所示:

Overview	Interfaces	Logical Devices	Security Engine	Platform Settings
FTD		Standalone	Status: ok	
Applica	tion	Version	м	anagement IP
FTD		6.1.0.1.53	10	0.62.148.84
从机箱CLI:				
<#root>				
FPR4100#				
scope ssa				
FPR4100 /ssa #	ŧ			
show app-insta	ance			
Application Na	ame Slot ID	Admin State O	perational State Rur	ning Version Startup Vers

ftd 1 Enabled Online 6.1.0.1.53

6.1.0.330 Not Applicable

从FTD CLI:

<#root>

```
FPR4100#
```

connect module 1 console Telnet escape character is '~'. Trying 127.5.1.1... Connected to 127.5.1.1. Escape character is '~'. CISCO Serial Over LAN: Close Network Connection to Exit > show version -----[FTD4100.cisco.com]------: Cisco Firepower 4140 Threat Defense (76) Model Version 6.1.0.1 (Build 53) : 22c66994-c08e-11e6-a210-931f3c6bbbea UUID Rules update version : 2016-03-28-001-vrt VDB version : 275 _____ -------

>

Firepower 2100

Firepower 2100上的FTD使用包含FXOS和FTD映像的单个捆绑包。因此,安装和升级过程与 FP4100/FP9300上的有所不同。

FP2100上的FTD安装

有4种不同的过程,具体取决于具体情况:

- 案例1:清除配置并使用相同的FTD映像重新启动系统。
- 案例2:使用新的应用软件版本重新映像系统。
- 案例3:将系统重新映像为其出厂默认设置。
- 案例4:将系统重新映像为其出厂默认设置(管理员密码恢复)。

有关每个案例及其程序的详细信息,请查看:

<u>重新映像过程</u>

案例2适用于大多数FTD安装案例,而案例3(格式化和从ROMMON引导)可用于特定案例(例如 ,系统不稳定或处于引导环路等)。

FP2100上的FTD升级

由于没有单独的FXOS套件,要升级FP2100上的FTD,请执行以下列出的步骤:

步骤1:验证兼容性。

如果FTD由FMC管理(机下管理),请检查软件目标FTD发行版本注释中的兼容性部分。

第二步:如有需要,请先升级FMC。始终运行等于或高于FTD目标软件版本的FMC软件版本。

第三步:升级FTD。

使用与FP4100/9300中记录的过程相同的过程。在FTD升级之前要阅读的重要文档:

- FTD发行版本注释(例如,如果要升级到版本6.3.0.2,请检查6.3.0.2发行版本注释以验证升级 路径和所有相关详细信息。)<u>版本说明</u>
- FMC升级指南(章节:升级Firepower威胁防御:其他设备)<u>Cisco Firepower管理中心升级指</u> <u>南,版本6.0-7.0</u>

验证

当前没有可用于此配置的验证过程。

故障排除

当前没有故障排除此配置的特定可用资料。

相关信息

- FXOS兼容性指南
- <u>Cisco Firepower NGFW文档</u>
- <u>技术支持和文档 Cisco Systems</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)。