

使用 Firepower 管理中心管理 Firepower Threat Defense Virtual

本章介绍如何部署使用 FMC 管理的独立式 FTDv 设备。

注释 本文档涵盖最新的 FTDv 版本功能;有关功能更改的详细信息,请参阅使用 Firepower Management 管理 Firepower Threat Defense Virtual 的历史,第15页。如果您使用的是旧版本的软件,请参考您的版本的《FMC 配置指南》中的步骤。

- 关于使用 Firepower 管理中心管理的 Firepower Threat Defense Virtual,第1页
- 登录到 Firepower 管理中心,第2页
- •向 Firepower 管理中心注册设备,第2页
- •配置基本安全策略,第4页
- 访问 Firepower 威胁防御 CLI,第15页
- 使用 Firepower Management 管理 Firepower Threat Defense Virtual 的历史 , 第 15 页

关于使用 Firepower 管理中心管理的 Firepower Threat Defense Virtual

Firepower Threat Defense Virtual (FTDv) 是思科 NGFW 解决方案的虚拟化组件。FTDv 提供各种下一 代防火墙服务,包括状态防火墙、路由、下一代入侵防御系统(NGIPS)、应用可视性与可控性(AVC)、 URL 过滤,以及高级恶意软件防护(AMP)。

您可以使用 Firepower 管理中心 (FMC) 管理 FTDv,这是一个功能齐全的多设备管理器,位于单独的服务器上。有关安装 FMC 的详细信息,请参阅 FMC 入门指南。

FTDv 向您分配给 FTDv 虚拟机的管理接口上的 FMC 注册并与之通信。

要进行故障排除,您可以使用管理接口上的 SSH 访问 FTD CLI,也可以从 Firepower CLI 连接到 FTD。

登录到 Firepower 管理中心

使用 FMC配置并监控 FTD。

开始之前

有关受支持浏览器的信息,请参阅您所用版本的发行说明(参阅https://www.cisco.com/go/firepower-notes)。

过程

步骤1 使用支持的浏览器输入以下 URL。

https://fmc_ip_address

• fmc_ip_address - 标识 FMC 的 IP 地址或主机名。

步骤2 输入您的用户名和密码。

步骤3 单击 Log In。

向 Firepower 管理中心注册设备

开始之前

确保 FTDv 虚拟机已部署成功、已接通电源并且已首次完成其启动程序。

过程

步骤1选择设备>设备管理.

步骤2 从添加下拉列表选择添加设备,然后输入以下参数。

Add Device	3
Host:+	
ftd-1.cisco.com	
Display Name:	
ftd-1.cisco.com	
Registration Key:*	
••••	
Group:	
None	•
Access Control Policy:*	
inside-outside	•
Smart Licensing	
✓ Malware	
Threat	
✓ URL Filtering	
Advanced	
Unique NAT ID:+	
natid56	
✓ Transfer Packets	
	Cancel Register

- 主机 输入要添加的逻辑设备的 IP 地址。如果您在 FTD 引导程序配置中指定了 FMC IP 地址和 NAT ID,则可以将此字段留空。
- •显示名称 输入要在 FMC 中显示的逻辑设备的名称。
- •注册密钥 输入您在 FTDv 引导程序配置中指定的注册密钥。
- Domain 如果有多域环境,请将设备分配给分叶域。
- Group 如果在使用组,则将其分配给设备组。

 Access Control Policy - 选择初始策略。除非已经拥有您知道自己需要使用的自定义策略,否则 选择 Create new policy,然后选择 Block all traffic。之后您可以更改此设置以允许流量通过; 请参阅配置访问控制,第13页。

Name:	ftd_ac_policy			
Description:				
Select Base Policy:	None		~	
Default Action:	Block all traffic O Intrus	sion Prevention ON	etwork Discovery	

- Smart Licensing 为要部署的功能分配所需的智能许可证: Malware (如果您打算使用 AMP 恶意软件检查)、Threat (如果您打算使用入侵防御)、URL (如果您打算实施基于类别的 URL 过滤)。
- •唯一NAT ID 指定您在 FTDv 启动程序配置中指定的 NAT ID。
- Transfer Packets 可让设备将数据包传输至 FMC。如果在启用此选项时触发了 IPS 或 Snort 等 事件,设备会将事件元数据信息和数据包数据发送到 FMC进行检测。如果禁用此选项,只有事 件信息会发送到 FMC,数据包数据不发送。

步骤3 单击 Register,并确认注册成功。

如果注册成功,设备将添加到列表中。如果注册失败,您会看到一则错误消息。如果 FTDv注册失败,请检查以下项:

• Ping - 访问 FTD CLI (访问 Firepower 威胁防御 CLI,第15页),然后使用以下命令 ping FMC IP 地址:

ping system ip_address

如果 ping 不成功,请使用 show network 命令检查您的网络设置。如果需要更改 FTD IP 地址,请使用 configure network {ipv4 | ipv6} manual 命令。

- NTP 确保 NTP 服务器与以下页面上设置的 FMC 服务器相符: 系统 > 配置 > 时间同步页面。
- 注册密钥、NAT ID 和 FMCIP 地址 确保在两个设备上使用相同的注册密钥和 NAT ID (如有使用)。您可以在 FTDv 上使用 configure manager add 命令设置注册密钥和 NAT ID。也可以使用此命令更改 FMCIP 地址。

配置基本安全策略

本部分介绍如何使用以下设置配置基本安全策略:

- •内部和外部接口 为内部接口分配静态 IP 地址,并将 DHCP 用作外部接口。
- DHCP 服务器 在内部接口上为客户端使用 DHCP 服务器。
- •默认路由-通过外部接口添加默认路由。
- •NAT 在外部接口上使用接口 PAT。
- •访问控制-允许流量从内部传到外部。

过程

步骤1 配置接口,第5页 步骤2 配置 DHCP 服务器,第8页 步骤3 添加默认路由,第9页 步骤4 配置 NAT,第10页 步骤5 配置访问控制,第13页 步骤6 部署配置,第14页

配置接口

启用 FTDv接口,为其分配安全区域并设置 IP 地址。通常,您必须至少配置两个接口才能让系统传递有意义的流量。通常,您将拥有面向上游路由器或互联网的外部接口,以及组织网络的一个或多个内部接口。其中一些接口可能是"隔离区"(DMZ),您可以在其中放置可公开访问的资产,例如Web 服务器。

典型的边缘路由情况是通过 DHCP 从 ISP 获取外部接口地址,同时在内部接口上定义静态地址。

以下示例使用 DHCP 在接口内部配置了一个路由模式(含静态地址),并在接口外部配置了一个路由模式。

过程

步骤1选择设备>设备管理,然后单击该设备的编辑(✓)。

步骤2单击 Interfaces。

Overview Analysis	Policies De	evices Object	ts AMP	Intelligence			Deploy	94 System	Help 🔻	admin 🔻
Device Management	NAT VPN	l▼ QoS	Platform Set	ttings FlexCo	nfig Certificates					
10.89.5.20 Cisco Firepower 9000 Serie	s SM-24 Threat De	efense							Save	🔀 Cancel
Device Routing	Interfaces	Inline Sets	DHCP							
							🔍 Search by name	Sync Device	e 🕜 Add	Interfaces 🕶
Interface	Logical Name	Туре	Se	curity Zones	MAC Address (Activ	e/Standby)	IP Address			
Ethernet1/2		Physical							E <	6
Ethernet1/3.1		SubInterf	ace						Ξ	Ø
Ethernet1/4	diagnostic	Physical							Ξ	Ø
Ethernet1/5		Physical							Ξ	Ø

步骤3单击要用于内部的接口的编辑(//)。

General 选项卡将显示	0
----------------	---

Edit Phys	ical Int	erface							? ×
General	IPv4	IPv6	Advanced	Hardware	Configuration				
Name:			inside				🗹 Enabled	🗌 Manageme	nt Only
Description									
Mode:			None			*			
Security Zor	ne:		inside_zone			~			
Interface ID	1		GigabitEtherne	et0/0					
MTU:			1500		(64 - 9000)				
							0	Cano	el

a) 输入长度最大为 48 个字符的 Name。

例如,将接口命名为 inside。

- b) 选中 Enabled 复选框。
- c) 将 Mode 保留为 None。
- d) 从 Security Zone 下拉列表中选择一个现有的内部安全区域,或者单击 New 添加一个新的安全区域。

例如,添加一个名为inside_zone的区域。必须将每个接口分配给安全区域和/或接口组。每个接口只能属于一个安全区域,但可以同时属于多个接口组。您可以根据区域或组应用安全策略。例如,您可以将内部接口分配到内部区域,而将外部接口分配到外部区域。然后可以配置访问控制策略,允许流量从内部传到外部,但不允许从外部传入内部。大多数策略仅支持安全区域;您可以在 NAT 策略、预过滤器策略和 QoS 策略中使用区域或接口组。

- e) 单击 IPv4 和/或 IPv6 选项卡。
 - IPv4 从下拉列表中选择 Use Static IP, 然后以斜杠表示法输入 IP 地址和子网掩码。 例如, 输入 192.168.1.1/24

Edit Phys	sical Int	erface			
General	IPv4	IPv6	Advanced	Hardware Configuration	
IP Type:			Jse Static IP	v	
IP Address			192.168.1.1/24	eg. 192.0.2.1/255.255.255.12 192.0.2.1/25	8 or

- IPv6 为无状态自动配置选中 Autoconfiguration 复选框。
- f) 单击确定。
- 步骤4 单击要用于外部的接口的编辑 (╱)。

General 选项卡将显示。

Edit Physical Inte	rface						?	×
General IPv4	IPv6	Advanced	Hardware	Configuration	Ĺ			
Name:		outside				🗹 Enabled	🗌 Management O	nly
Description:								
Mode:		None			*			
Security Zone:		outside_zone			~			
Interface ID:		GigabitEtherne	et0/0					
MTU:		1500		(64 - 9000)				
						0	K Cancel	

a) 输入长度最大为 48 个字符的 Name。

例如,将接口命名为 outside。

- b) 选中 Enabled 复选框。
- c) 将 Mode 保留为 None。
- d) 从 Security Zone 下拉列表中选择一个现有的外部安全区域,或者单击 New 添加一个新的安全区域。

例如,添加一个名为 outside_zone 的区域。

- e) 单击 IPv4 和/或 IPv6 选项卡。
 - IPv4 选择 Use DHCP, 然后配置以下选填参数:
 - Obtain default route using DHCP 从 DHCP 服务器获取默认路由。
 - DHCP route metric 分配到所获悉路由的管理距离,介于1和255之间。获悉的路由的默认管理距离为1。

Edit Phys	ical Int	erface			
General	IPv4	IPv6	Advanced	Hardware	e Configuration
IP Type:		ι	Jse DHCP	¥	
Obtain defa DHCP:	ult route	using 🧧	2		
DHCP route	e metric:	1	L		(1 - 255)

- IPv6 为无状态自动配置选中 Autoconfiguration 复选框。
- f) 单击确定。

步骤5 单击保存。

配置 DHCP 服务器

如果希望客户端使用 DHCP 从 FTDv处获取 IP 地址,请启用 DHCP 服务器。

过程

步骤1选择设备>设备管理,然后单击该设备的编辑(✓)。

- 步骤 2 选择 DHCP > DHCP 服务器.
- 步骤3在Server页面上单击Add,然后配置以下选项:

Add Server				? ×
Interface*	inside	~		
Address Pool*	10.9.7.9-10.9.7.25		(2.2.2	2.10-2.2.2.20)
Enable DHCP Server				
			ОК	Cancel

• Interface -- 从下拉列表中选择接口。

- Address Pool DHCP 服务器使用的 IP 地址的范围(从最低到最高)。IP 地址范围必须与选定接口位于相同的子网上,且不能包括接口自身的 IP 地址。
- Enable DHCP Server 在所选接口上启用 DHCP 服务器。

步骤4 单击确定。

步骤5 单击保存。

添加默认路由

默认路由通常指向可从外部接口访问的上游路由器。如果您将 DHCP 用作外部接口,则您的设备可 能已经收到了默认路由。如果需要手动添加路由,则遵照此程序执行。如果从 DHCP 服务器收到默 认路由,它将显示在 IPv4 路由或 IPv6 路由表中,该表位于 设备 > 设备管理 > 路由 > 静态路由页 面。

过程

步骤1选择设备>设备管理,然后单击该设备的编辑(▲)。 步骤2选择路由>静态路由,单击添加路由,然后设置以下参数:

Interface* Available Network Selected Network Selected Network Selected Network Selected Network any-ipv4 IPv4-Benchmark-Tests IPv4-Benchmark-Tests IPv4-Private-10.0.0.0-8 IPv4-Private-172.16.0.0 IPv4-Private-192.168.0. IPv4-Private-192.168.0. IPv4-Private-192.168.0. IPv4-Private-All-RFC191 Gateway* default-gateway Metric: 1 Tunneled: (Used only for default Route) Route Tracking:	?	1			ation IPv6	ite Configur	Add Static Rou
Available Network Selected Network Search any-ipv4 IPv4-Benchmark-Tests Add IPv4-Private-10.0.0.0-8 IPv4-Private-172.16.0.0 IPv4-Private-192.168.0. IPv4-Private-192.168.0. IPv4-Private-192.168.0. IPv4-Private-192.168.0. IPv4-Private-10.1-RFC191 Ivef-to-IPv4-Relay-Anyu Gateway* default-gateway Metric: 1 (Used only for default Route) Route Tracking: Image:				~		outside	Interface*
Search IPv4-Benchmark-Tests IPv4-Link-Local IPv4-Multicast IPv4-Private-10.0.0.0-8 IPv4-Private-172.16.0.0 IPv4-Private-192.168.0. IPv4-Private-All-RFC191 IPv6-to-IPv4-Relay-Anyu			elected Network	5	0	ork C	Available Netw
any-ipv4 IPv4-Benchmark-Tests IPv4-Link-Local IPv4-Private-10.0.0.0-8 IPv4-Private-172.16.0.0 IPv4-Private-192.168.0. IPv4-Private-192.168.0. IPv4-Private-All-RFC191 IPv6-to-IPv4-Relay-Anyi	1	i	any-ipv4				🔍 Search
IPv4-Benchmark-Tests IPv4-Link-Local IPv4-Multicast IPv4-Private-10.0.0.0-8 IPv4-Private-172.16.0.0 IPv4-Private-192.168.0. IPv4-Private-192.168.0. IPv4-Private-192.168.0. IPv4-Private-All-RFC191 IPv6-to-IPv4-Relay-Anyı Gateway* default-gateway © Metric: 1 (Used only for default Route) Route Tracking: Y ©							any-ipv4
IPv4-Link-Local IPv4-Nulticast IPv4-Private-10.0.0.0-8 IPv4-Private-172.16.0.0 IPv4-Private-192.168.0. IPv4-Private-192.168.0. IPv4-Private-All-RFC191						hmark-Tests	💂 IPv4-Bend
Add IPv4-Multicast IPv4-Private-10.0.0.0-8 IPv4-Private-172.16.0.0 IPv4-Private-192.168.0. IPv4-Private-All-RFC191 IPv6-to-IPv4-Relay-Any: Gateway* default-gateway V Sateway* (1 - 254) Tunneled: (Used only for default Route) Route Tracking: V Sateway Sateway Sateway V Sateway Satew					_	Local	📄 IPv4-Link-
IPv4-Private-10.0.0.0-8 IPv4-Private-172.16.0.0 IPv4-Private-192.168.0. IPv4-Private-All-RFC191 IPv6-to-IPv4-Relay-Anyi Gateway* default-gateway Wetric: 1 (1 - 254) Tunneled: (Used only for default Route) Route Tracking:				Add		cast	IPv4-Multi
IPv4-Private-172.16.0.0 IPv4-Private-192.168.0. IPv4-Private-All-RFC191 IPv6-to-IPv4-Relay-Anyi Gateway* default-gateway Wetric: 1 (1 - 254) Tunneled: (Used only for default Route) Route Tracking: \hlineth> \hlineth> \hlineth> \hlineth> \hlineth> \hlineth> \hlineth> \hlineth th> \hlineth \hlineth \hlineth \hlineth \hlineth \hlineth \hlineth \hlineth \hlineth th> th> \hlineth th> th> th> th> \hlineth th> \hlineth \hlineth <td< td=""><td></td><td></td><td></td><td></td><td></td><td>te-10.0.0.0-8</td><td>IPv4-Priva</td></td<>						te-10.0.0.0-8	IPv4-Priva
IPv4-Private-192.168.0. IPv4-Private-All-RFC191 Ivof-to-IPv4-Relay-Anyi Gateway* default-gateway Wetric: 1 (1 - 254) Tunneled: (Used only for default Route) Route Tracking: Image: Im						te-172.16.0.0	IPv4-Priva
Gateway* default-gateway Gateway* default-gateway Gateway* (1917) (1 - 254) Tunneled: (Used only for default Route) Route Tracking: Gateway Gateway						te-192.168.0.	IPv4-Priva
Gateway* default-gateway Image: Constraint of the second					~	v4-Relay-Any	IPv4-Priva
Metric: 1 (1 - 254) Tunneled: (Used only for default Route) Route Tracking:			0	~	iy	default-gatewa	Gateway*
Tunneled: Used only for default Route) Route Tracking:			(1 - 254)			1	Metric:
Route Tracking:				ute)	or defaul	(Used only f	Tunneled:
			0	~			Route Tracking:

- Type 根据要添加静态路由的类型,单击 IPv4 或 IPv6 单选按钮。
- Interface 选择出口接口;通常是外部接口。

- •可用网络 为 IPv4 默认路由选择 any-ipv4,为 IPv6 默认路由选择 any-ipv6。
- Gateway 或 IPv6 Gateway 输入或选择作为此路由的下一个跃点的网关路由器。您可以提供 IP 地址或网络/主机对象。
- Metric 输入到目标网络的跃点数。有效值范围为1到255; 默认值为1。

步骤3单击OK。

路由即已添加至静态路由表。

Overview Analysis F	Policies	Devices Obj	ects AMP Int	elligence		Deploy	04 System	ı Help √ ad
Device Management	NAT	VPN VQoS	Platform Settings	FlexConfig	Certificates			
10.89.5.20 Cisco Firepower 9000 Series S	M-24 Threa	t Defense				You have unsa	aved changes	Save <table-cell></table-cell>
Device Routing I	nterfaces	s Inline Sets	DHCP					
OSPF								O Add Route
OSPFv3		Network	Interface	Gateway	Tunneled	Metric	Tracked	
D 💋 BGP		▼ IPv4 Routes						
Static Route		any-ipv4	outside	10.99.10.1	false	1		P 🗎
Multicast Routing		▼ IPv6 Routes						

步骤4 单击保存。

配置 NAT

典型的 NAT 规则会将内部地址转换为外部接口 IP 地址上的端口。这类 NAT 规则称为接口端口地址 转换 (PAT)。

过程

步骤1选择设备>NAT,然后单击新策略>Threat Defense NAT.

步骤2为策略命名,选择要使用策略的设备,然后单击 Save。

Name:	interface_PAT		
Description:			
Targeted Devices			
Select devices	to which you want to apply this policy		
Available De	vices Selec	ted Devices	
Search by	name or value	192.168.0.16]
192.168	3.0.16		
	Add to Policy		
-			

策略即已添加 FMC。您仍然需要为策略添加规则。

步骤3 单击 Add Rule。

Add NAT Rule 对话框将显示。

步骤4 配置基本规则选项:

Add NAT Rule			
NAT Rule:	Auto NAT Rule	•	
Type:	Dynamic	•	✓ Enable
Interface Objects	Translation	PAT Pool	Advanced

- •NAT Rule 选择 Auto NAT Rule。
- Type 选择 Dynamic。
- **步骤 5** 在 Interface Objects 页面,将 Available Interface Objects 区域中的外部区域添加到 Destination Interface Objects 区域。

NAT Rule: Type: Dynamic Interface Objects Translation PAT Pool Advanced Available Interface Objects Constraintion Search by name Search by name Search by name Source Add to Source Add to Destination Add to Destination	Add NAT Rule						? ×
Interface Objects Translation PAT Pool Advanced Available Interface Objects Image: Comparison of the state of the	NAT Rule: Type:	Auto NAT Rule Dynamic	~	✓ Enable			
Available Interface Objects © Source Interface Objects (0) Destination Interface Objects (1) Image: Search by name any Image: Source Iman	Interface Objects	Translation	PAT Pool	Advanced			
Image: Search by name any Image: Add to Add to Image: Outside_zone Add to Image: Add to Source Image: Add to Add to Image: Destination Add to	Available Interface Ol	ojects 🖒		So	urce Interface Objects (0)	Destination Interface Objects (1)	
	Search by name		Ar Sc 2 Ar Dest	af dd to burce dd to tination	ηγ	3 🛆 outside_zone	

步骤6在Translation页面上配置以下选项:

Add NAT Rule				? ×
NAT Rule:	Auto NAT Rule 💙			
Type:	Dynamic 💌	🗹 Enable		
Interface Objects	Translation PAT Pool	Advanced		
Original Packet			Translated Packet	
Original Source:*	all-ipv4)	Translated Source:	Destination Interface IP
Original Port:	ТСР 💌			
			Translated Port:	

• 原始源 - 单击添加 (十) 为所有 IPv4 流量添加网络对象 (0.0.0.0/0)。

Name	all-ipv4			
Description				
Network	Host	O Range	Network	○ FQDN
	0.0.0.0/0			

- **注释** 您不能使用系统定义的 **any-ipv4** 对象,因为自动 NAT 规则在对象定义过程中添加 NAT,并且您无法编辑系统定义的对象。
- Translated Source 选择 Destination Interface IP。

步骤7 单击 Save 以添加规则。

规则即已保存至 Rules 表。

Ove	erview Ana	lysis Polici	es Devices O	bjects AMP Int	elligence						Deploy 🔒	System Help	• admin •
Dev	ice Manageme	nt NAT	VPN VOS	Platform Settings	FlexConfig C	ertificates							
int Ente	erface_P	AT								You ha	ve unsaved chan	ges 🔚 Save	Cancel
Rule	5											Policy	Assignments (1)
dia Fil	ter by Device											0	Add Rule
						Origi	nal Packet			Translated Packet			
#	Direction	Туре 5	Source Interface Objects	Destination Interface Objects	Original Sources	Origi Dest	nal inations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options	
▼ N#	AT Rules Before	•											
▼ Au	to NAT Rules												
#	+	Dynamic (🥞 any	outside_zone	🚔 all-ipv4				🍓 Interface			🍓 Dns:fals	e 🥜 🛅
▼ N/	AT Rules After												

步骤8 单击 NAT 页面上的 Save 以保存更改。

配置访问控制

如果您在使用 FMC注册 FTDv 时创建了基本的封锁所有流量访问控制策略,则需要向策略添加规则 以允许流量通过设备。以下程序可添加规则以允许从内部区域到外部区域的流量。如有其他区域, 请务必添加允许流量到适当网络的规则。

请参阅 FMC 配置指南以配置更高级的安全设置和规则。

过程

- 步骤1选择策略>访问策略>访问策略,然后单击分配给FTD的访问控制策略对应的编辑(/)。
- 步骤2 单击 Add Rule 并设置以下参数:

Add Rule											?>
Name inside_to_outside				🗹 Enat	led	Insert	into Mandat	tory			~
Action 🖌 Allow			V D 21	1							
Zones Networks V	/LAN Tags	🛆 Users	Applications	Ports	URLs	SGT/ISE Attributes	5		Inspection	Logging	Comments
Available Zones 🖒				Source	Zones (1	.)		Destinat	ion Zones (1)		
🔍 Search by name				👬 🛦 ii	nside_zon	e	6	📩 🛆 ou	utside_zone		6
🚠 📐 inside_zone											
📸 🛆 outside_zone											
			Add to Source								
			Add to Destination								

- Name 为此规则命名,例如 inside_to_outside。
- Source Zones 从 Available Zones 中选择内部区域, 然后单击 Add to Source。
- Destination Zones 从 Available Zones 中选择外部区域,然后单击 Add to Destination。

其他设置保留原样。

步骤 3 单击 Add。

规则即已添加至 Rules 表。

Overview Analysis Policies	Devices Objects	AMP Inte	elligence							Dep	oloy 🕛 S	System Help 🛛	
Access Control + Access Control	Network Discovery	Application	Detectors (Correlation	Actions v								
ftd_ac_policy							Yo	u have unsaved o	changes 🔔 Sh	ow Warnings	Analyze Hit Co	ounts 🔚 Save	Cancel
Prefilter Policy: <u>Default Prefilter Policy</u> Rules Security Intelligence H	TP Responses Log	aing Advance	SSL P	olicy: <u>None</u>			1	Identity Policy:	None	T	Inheritance S	ettings 📕 Policy Ass	ignments (1)
齢 Filter by Device							Show Rule	e Conflicts 😡	Add Categor	y 🚺 🙆 Add Ru	le Search Ru	iles	×
Name Source	Zo Dest Zones	Source Ne	Dest Netw	VLAN Tags	Users	Applications	Source Po	Dest Ports	URLs	ISE/SGT A	Action	V 🗅 🔎 🗇 🗉	•
➡ Mandatory - ftd_ac_policy (1-1)													
1 🛕 inside_to_outside 🛛 🛔 insid	e_zone 🚓 outside_zon	e Any	Any	Any	Any	Any	Any	Any	Any	Any	🖋 Allow	VDADJ	o 🥜 🗒
➡ Default - ftd_ac_policy (-)													
There are no rules in this section. Add F	ule or Add Category												
Default Action									Access Co	ntrol: Block All Tra	affic		× 1

步骤4 单击保存。

部署配置

将配置更改部署到FTDv;在部署之前,您的所有更改都不会在设备上生效。

\	L 1 m
11	「ホー
~	リーエ

步骤1 单击右上方的 Deploy。



步骤2选择 Deploy Policies 对话框中的设备,然后单击 Deploy。

/	Device	Inspect Interruption	Туре	Group	Current Version	
7	= 192.168.0.16	No	FTD		2019-02-28 07:11 AM	

步骤3确保部署成功。单击菜单栏中 Deploy 按钮右侧的图标可以查看部署状态。



访问 Firepower 威胁防御 CLI

您可以使用FTDvCLI更改管理接口参数并进行故障排除。要访问CLI,可以使用管理接口上的SSH,也可以从 VMware 控制台连接。

过程

步骤1 (选项1)通过 SSH 直接连接到 FTDv 管理接口的 IP 地址。

在部署虚拟机时,您需要设置管理IP地址。使用 admin 帐户和初始部署期间设定的密码登录 FTDv。

步骤2 (选项2) 打开 VMware 控制台并使用默认用户名 admin 帐户和初始部署期间设定的密码登录。

使用 Firepower Management 管理 Firepower Threat Defense Virtual 的历史

功能名称	平台版本	功能信息
FMC 管理	6.0	初始支持。

I

使用 Firepower 管理中心管理 Firepower Threat Defense Virtual