通过FDM或CLISH在FTD上配置SSH和HTTPS的管理访问

目录

简介

先决条件

- 要求
- 使用的组件

配置

- FDM步骤
- CLISH步骤

验证

参考

简介

本文档介绍在本地或远程管理的FTD上配置和验证SSH和HTTPS的管理访问列表的过程。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

- 运行由FDM管理的7.4.1版本的思科安全防火墙威胁防御。

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。

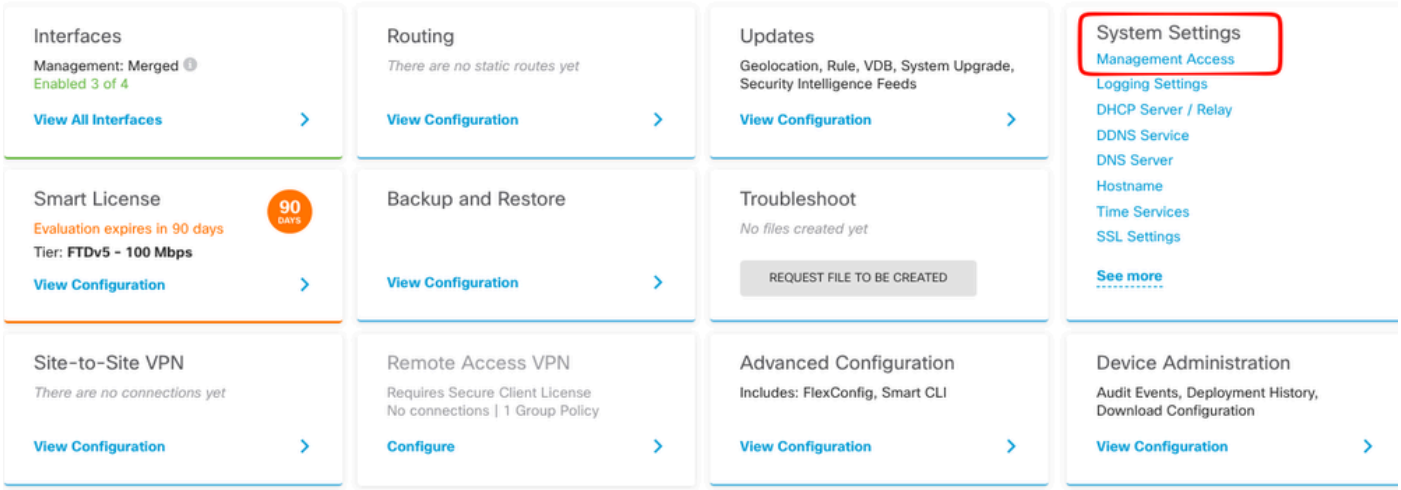
配置

FTD可以使用FDM本地管理，也可以通过FMC管理。本文档的主要重点是通过FDM和CLI进行管理访问。使用CLI，您可以对FDM和FMC进行更改。

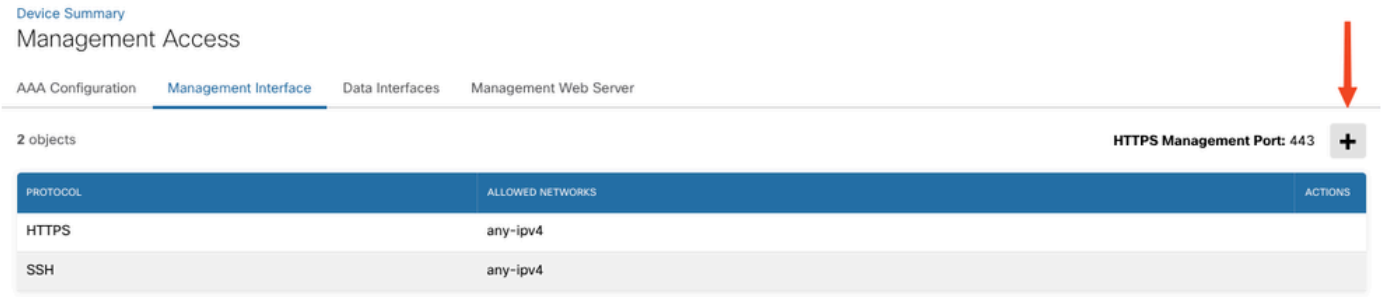
⚠ 警告：配置SSH或HTTPS访问列表，一次配置一个，以避免会话锁定。首先，更新并部署一个协议，验证访问，然后继续执行另一个协议。

FDM步骤

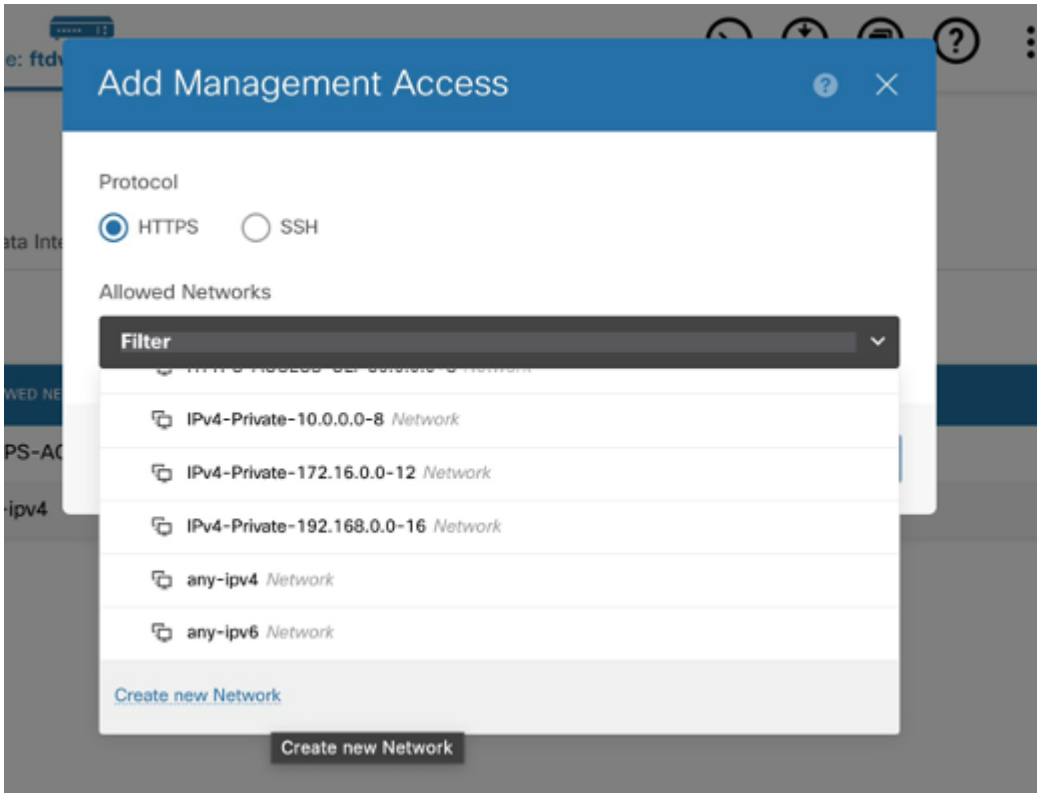
1.登录到Firepower设备管理器(FDM)，然后导航到系统设置>管理访问>管理接口。



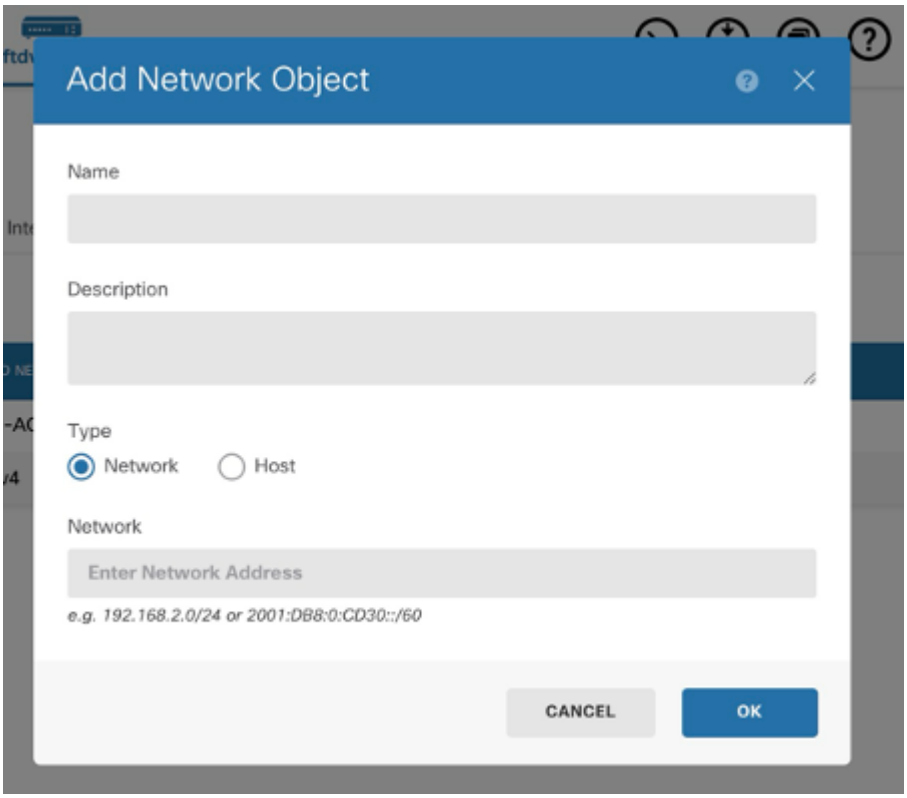
2.单击+图标打开添加网络的窗口。



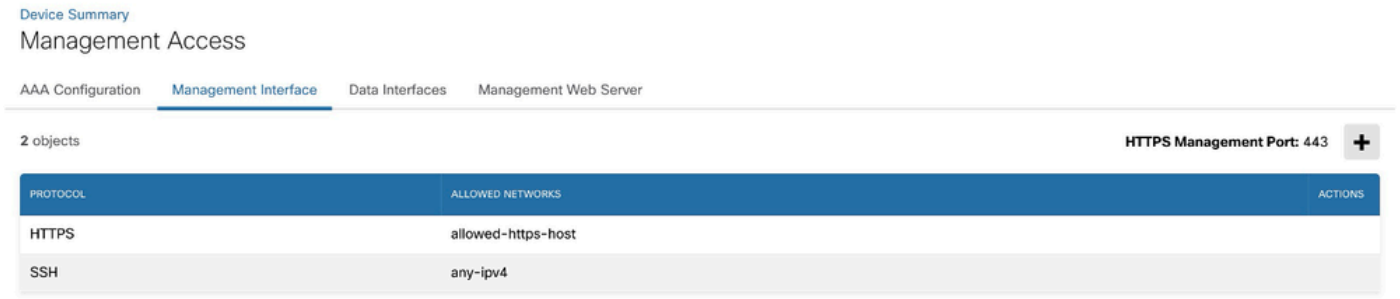
3.添加网络对象以访问SSH或HTTPS。如果必须创建新网络，请选择Create New Network选项。您可以在管理访问部分为网络或主机添加多个条目。



4.可选:选择Create a New Network选项将打开Add Network Object窗口。

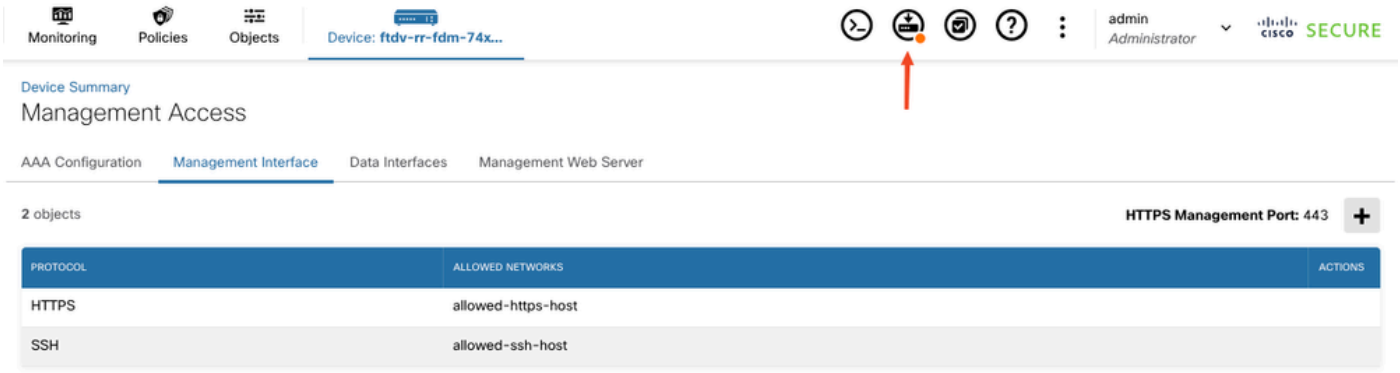


5.验证所做的更改并进行部署。

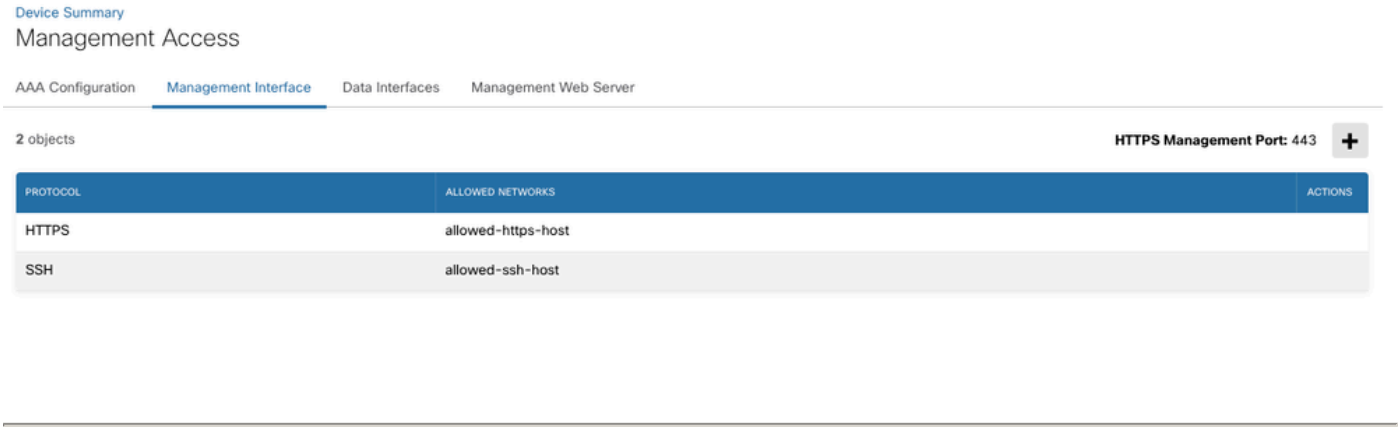


---

6. 可选：验证之前对HTTPS所做的更改后，对SSH重复相同的操作。



7.部署更改并验证从允许的网络和主机对FTD的访问。



CLISH步骤

如果同时管理FDM或FMC，则可以使用CLI步骤。要将设备配置为接受来自指定IP地址或网络的HTTPS或SSH连接，请运行configure https-access-list或configure ssh-access-list命令。

- 必须在单个命令中包含所有受支持的主机或网络。此命令中指定的地址会覆盖各个访问列表的当前内容。
- 如果设备是本地管理的高可用性组中的设备，则您的更改会在下一次主用设备部署配置更新时覆盖。如果这是主用设备，则更改会在部署期间传播到对等设备。

```
> configure https-access-list x.x.x.x/x,y.y.y.y/y

The https access list was changed successfully.

> show https-access-list
ACCEPT     tcp  --  x.x.x.x/x            anywhere             state NEW tcp dpt:https
ACCEPT     tcp  --  y.y.y.y/y            anywhere             state NEW tcp dpt:https
```

注意：x.x.x.x/x和y.y.y.y/y表示使用CIDR表示法的IPv4地址。要指定所有IPv4主机，请输入0.0.0.0/0。要指定所有IPv6主机，请指定：:/0。

对于SSH连接，请运行configure ssh-access-list命令。

```
> configure ssh-access-list x.x.x.x/x

The ssh access list was changed successfully.

> show ssh-access-list
ACCEPT     tcp  --  x.x.x.x/x            anywhere             state NEW tcp dpt:ssh
```

注意：您可以运行命令configure disable-https-access或configure disable-ssh-access，以分别禁用HTTPS或SSH访问。确保您了解这些更改，因为这会使您无法参与会话。

您也可以在单个命令中为ipaddress/CIDR的值配置多个条目，这些条目之间用逗号分隔。

验证

要从CLISH进行验证，可以运行命令：

```
> show ssh-access-list
ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:ssh

> show https-access-list
ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:https
```

示例输出显示了f2b-ssh条目。在连续10次失败的SSH尝试后，系统自动添加f2b-sshd条目以运行show ssh-access-list命令输出。

```
> show ssh-access-list
f2b-sshd   tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:ssh
Chain f2b-sshd (1 references)
```

请参阅“参考”一节中的f2b。

参考

- 思科安全防火墙威胁防御命令参考
- 适用于Firepower设备管理器的思科Firepower威胁防御配置指南

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）。