Cisco Secure Firewall 3100/4200 的多实例模式

您可以将 Cisco Secure Firewall 3100/4200 作为单个设备（设备模式）或多个容器实例（多实例模式）进行部署。本章介绍如何在多实例模式下部署设备。

关于多实例模式

在多实例模式下，您可以在单个机箱上部署多个容器实例充当完全独立设备。

多实例模式与应用模式

您可以在多实例模式或设备模式下运行设备。

设备模式

设备模式为默认模式。设备运行本地 映像并充当单个设备。唯一可用的机箱级配置（在 **机箱管理器** 页面上）用于网络模块管理（分支端口或启用/禁用网络模块）。

多实例模式

如果更改为多实例模式，则设备在机箱上运行 Cisco Secure Firewall eXtensible 操作系统 (FXOS)，而每个实例运行单独的 映像。您可以使用 FXOS CLI 配置模式。

由于多个实例在同一机箱上运行，因此您需要对以下项执行机箱级管理：

- 使用资源配置文件的 CPU 和内存资源。
- 接口配置和分配。

- 部署和监控实例。

对于多实例设备，将 机箱 添加到 防火墙管理中心 并在 **机箱管理器** 页面上配置机箱级别设置。

机箱管理接口

机箱管理

机箱使用设备上的专用管理接口。多实例模式不支持将数据接口用于机箱管理，也不支持将 DHCP 寻址用于管理接口。

您只能在 CLI（初始设置时）或 FXOS CLI（转换为多实例模式后）中配置机箱管理接口。请参阅在 FXOS CLI 中更改机箱管理设置，第 60 页以更改多实例模式下的管理接口设置。

注释 默认情况下，除非您启用 SSH 服务器和 SSH 访问列表，否则在多实例模式下不允许 SSH 访问此接口。这种差异意味着您可以使用 SSH 连接到应用模式威胁防御管理接口，但在转换为多实例模式后，默认情况下无法再使用 SSH 进行连接。请参阅配置 SSH 和 SSH 访问列表，第 42 页。

实例管理

所有实例共享机箱管理接口，并且每个实例在管理网络上都有自己的 IP 地址。添加实例并指定 IP 地址后，您可以在 CLI 中更改网络设置。

默认情况下，实例管理 IP 地址允许 SSH。

实例事件接口

Cisco Secure Firewall 4200 包括可用于事件的第二个专用接口管理 1/2。您可以在每个实例的 CLI 中配置此接口。为每个实例分配同一网络上的 IP 地址。请参阅配置事件接口。

实例接口

要确保灵活使用实例的物理接口，可以在机箱上创建 VLAN 子接口，还可以在多个实例之间共享接口（VLAN 或物理接口）。请参阅共享接口可扩展性，第 5 页和配置子接口，第 28 页。

注释 本章仅讨论机箱 VLAN 子接口。您还可以在实例内单独创建子接口。有关详细信息，请参阅机箱接口与实例接口，第 3 页。

接口类型

物理接口、VLAN 子接口和 EtherChannel 接口可以是下列类型之一：

- 数据 - 用于常规数据或故障切换链路。数据接口无法在实例之间共享，并且实例无法通过背板与其他实例通信。对于数据接口上的流量，所有流量必须在一个接口上退出机箱，并在另一个接口上返回以到达另一个实例。您可以将 VLAN 子接口添加到数据接口，以便为每个高可用性对提供单独的故障切换链路。
- 数据共享 - 用于常规数据。这些数据接口可以由一个或多个实例共享。每个实例都可通过背板与共享此接口的所有其他实例通信。共享的接口可能会影响您可以部署实例的数量。共享接口不支持用于网桥组成员接口（在透明模式或路由模式下）、内联集、被动接口、或故障转移链路。

机箱接口与实例接口

在机箱层面，管理物理接口、实例的 VLAN 子接口和 EtherChannel 接口的基本以太网设置。在实例中，您可以配置更高级别的设置。例如，您只能在机箱中创建 EtherChannel；但是，您可以为实例中的 EtherChannel 分配 IP 地址。

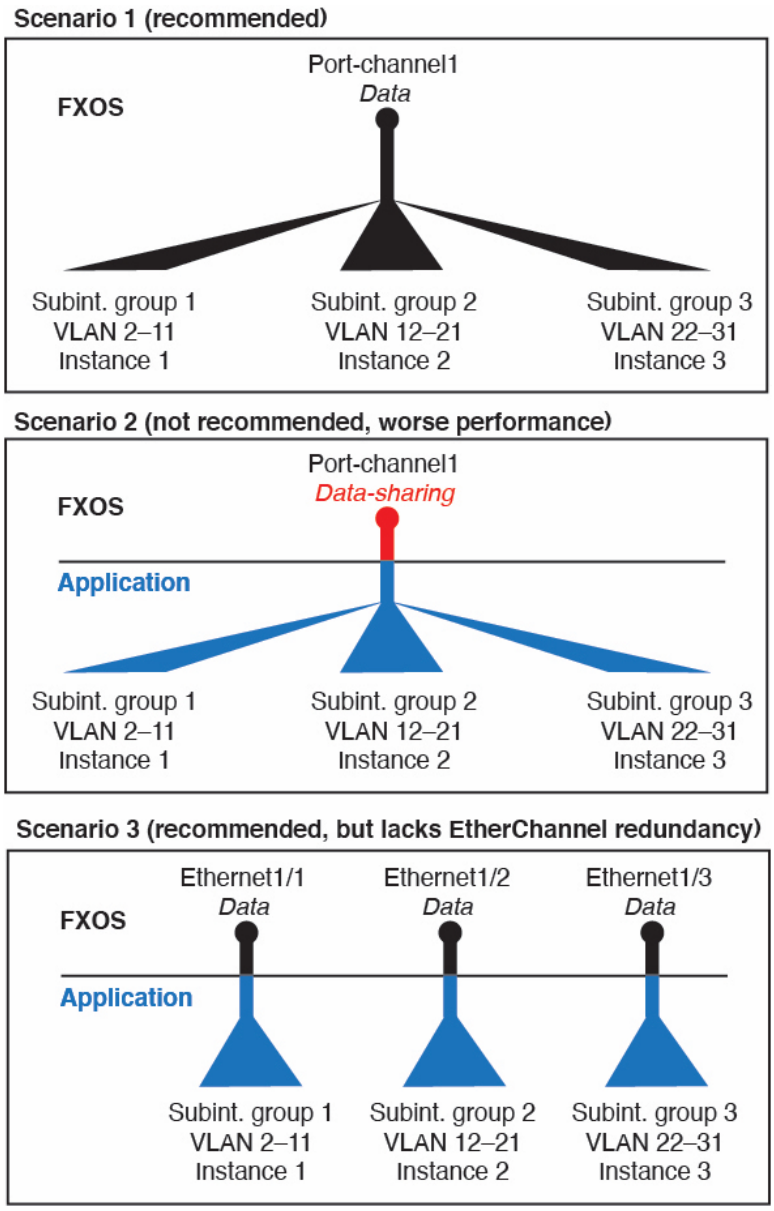
下文将介绍机箱接口与实例接口之间的交互。

VLAN 子接口

您可以在实例中创建 VLAN 子接口，就像创建任何设备一样。

您 还 可以在机箱中创建 VLAN 子接口。实例定义的子接口不受机箱限值的约束。选择在哪个位置创建子接口取决于网络部署和个人偏好。例如，要共享子接口，必须在机箱创建子接口。偏好机箱子接口的另一种场景包含将单个接口上的单独子接口组分配至多个实例。例如，您想要结合使用端口通道 1 与实例 A 上的 VLAN 2-11、实例 B 上的 VLAN 12-21 和实例 C 上的 VLAN 22-31。如果您在实例内创建这些子接口，则必须在机箱中共享父接口，但这可能并不合适。有关可以用于实现这种场景的三种方法，请参阅下图：

图 *1:* 机箱中的 ***VLAN*** 与实例



机箱和实例中的独立接口状态

您可以从管理上启用和禁用机箱和机箱中的接口。必须在两个位置中都启用能够正常运行的接口。由于接口状态可独立控制，因此机箱与实例之间可能出现不匹配的情况。

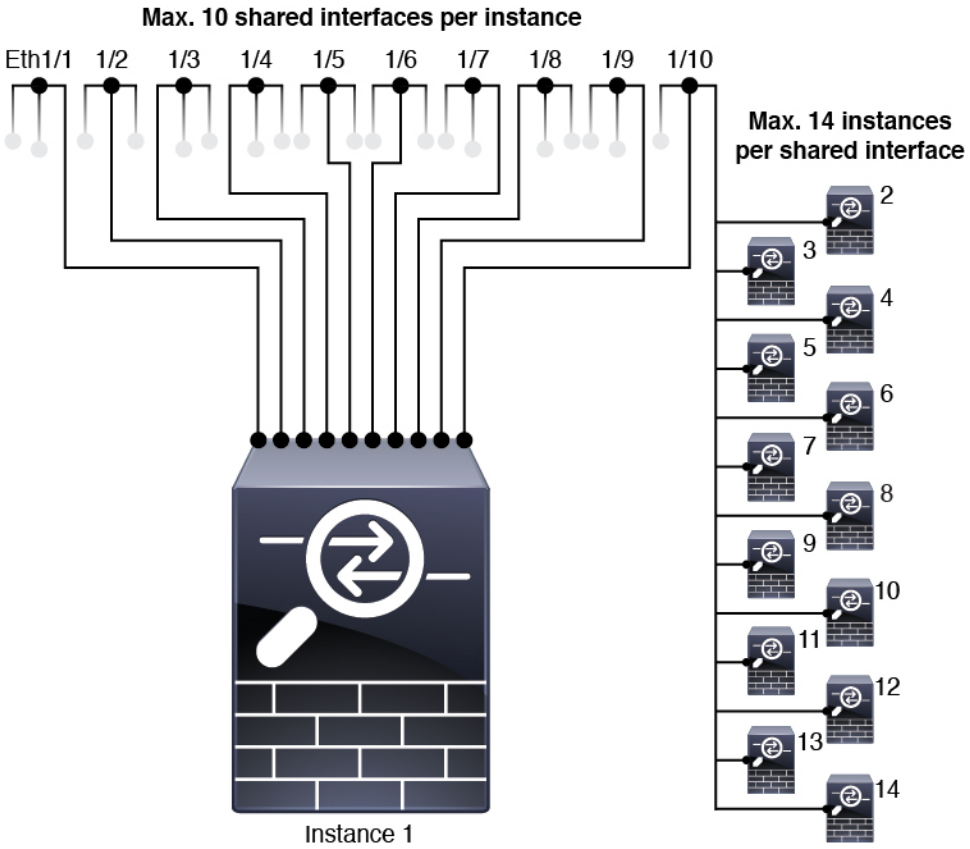
实例内接口的默认状态取决于接口类型。例如，在实例内，默认禁用物理接口或 EtherChannel，但默认启用子接口。

共享接口可扩展性

实例可以共享数据共享型接口。此功能允许您保存物理接口的使用情况，以及支持灵活的网络部署。当您共享接口时，机箱会使用唯一 MAC 地址将流量转发至适当实例。然而，由于需要在机箱内实现全网状拓扑，因此共享接口将导致转发表规模扩大（每个实例都必须能够与共享同一接口的所有其他实例进行通信）。因此，您可以共享的接口存在数量限制。

除转发表外，机箱还维护用于 VLAN 子接口转发的 VLAN 组表。 您最多可以创建 500 个 VLAN 子接口。

请参阅共享接口分配的以下限制：



共享接口最佳实践

为确保转发表的最佳可扩展性，请共享尽可能少的接口。相反，您可以在一个或多个物理接口上创建最多 500 个 VLAN 子接口，然后在容器实例之间划分 VLAN。

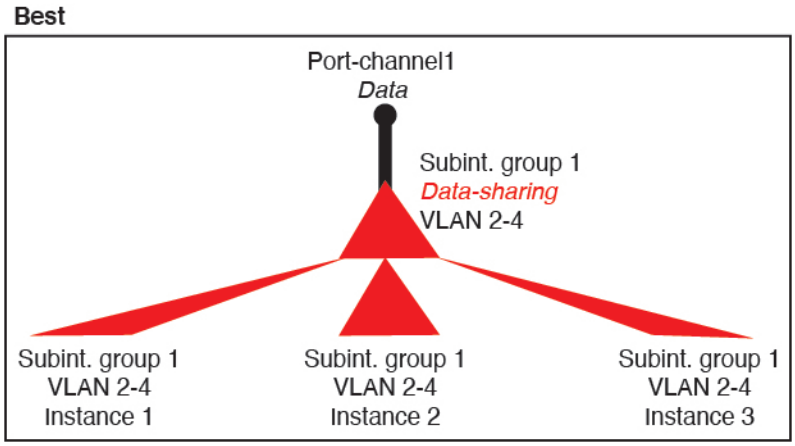
共享接口时，请按照可扩展性从高到低的顺序遵循这些最佳实践：

1. 最佳 - 共享单父项下的子接口，并结合使用相同集合的子接口和同组实例。

   例如，创建一个大型 EtherChannel 以将所有类似接口捆绑在一起，然后共享该 EtherChannel 的子接口：Port-Channel1.2, 3 和 4 而不是 Port-Channel2、Port-Channel3 和 Port-Channel4。与跨父项共

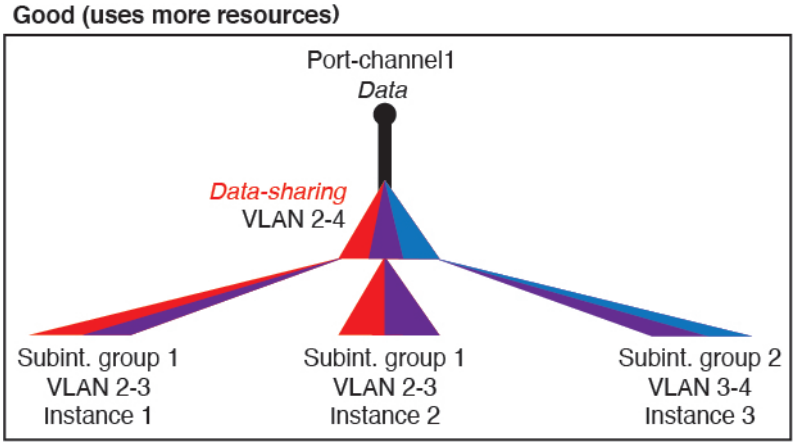
享物理/EtherChannel 接口或子接口相比，当您共享单父项子接口时，VLAN 组表提供更高的转发表可扩展性。

图 *2:* 最佳：一个父项上的共享子接口组



如果未与一组实例共享相同集合的子接口，则配置会提高资源使用率（更多 VLAN 组）。例如，与实例 1、2 和 3（一个 VLAN 组）共享 Port-Channel1.2, 3 和 4 而不是与实例 1 和 2 分享 Port-Channel1.2 和 3，同时与实例 3（两个 VLAN 组）共享 Port-Channel1.3 和 4。

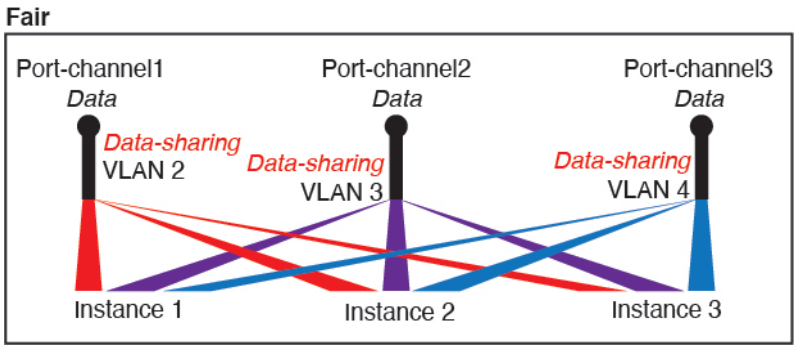
图 *3:* 良好：一个父项上共享多个子接口组



2. 一般 - 跨父项共享子接口。

   例如，共享 Port-Channel1.2、Port-Channel2.3 和 Port-Channel3.4 而不是 Port-Channel2、Port-Channel4 和 Port-Channel4。虽然这种使用方法的效率低于仅共享同一父项上的子接口，但仍可利用 VLAN 组。

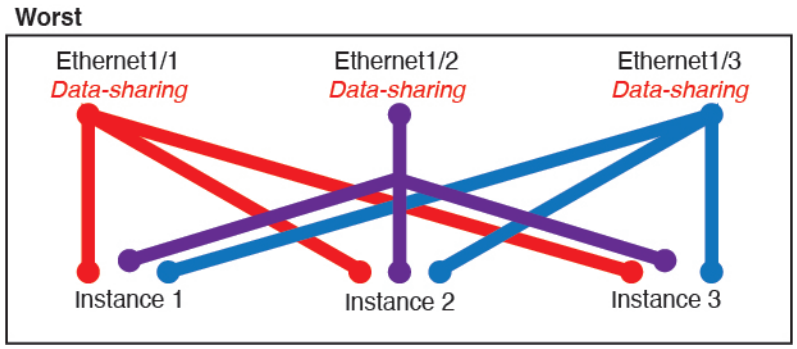
图 *4:* 一般：独立父项上的共享子接口



3. 最差 - 共享单个父接口（物理或 EtherChannel）。

   此方法使用的转发表条目最多。

图 *5:* 最差：共享父接口



机箱如何将数据包分类

必须对进入机箱的每个数据包进行分类，以便机箱能够确定将数据包发送到哪个实例。

- 唯一接口 - 如果仅有一个实例与传入接口相关联，则机箱会将数据包分类至该实例。对于桥接组成员接口（在透明模式或路由模式下）、内联集或被动接口，此方法用于始终与数据包进行分类。
- 唯一 MAC 地址 - 机箱将自动生成包括共享接口在内的所有接口的唯一 MAC 地址。如果多个实例共享一个接口，则分类器在每个实例中使用分配给该接口的唯一 MAC 地址。上游路由器无法直接路由至不具有唯一MAC地址的实例。在应用内配置每个接口时，您也可以手动设置MAC地址。

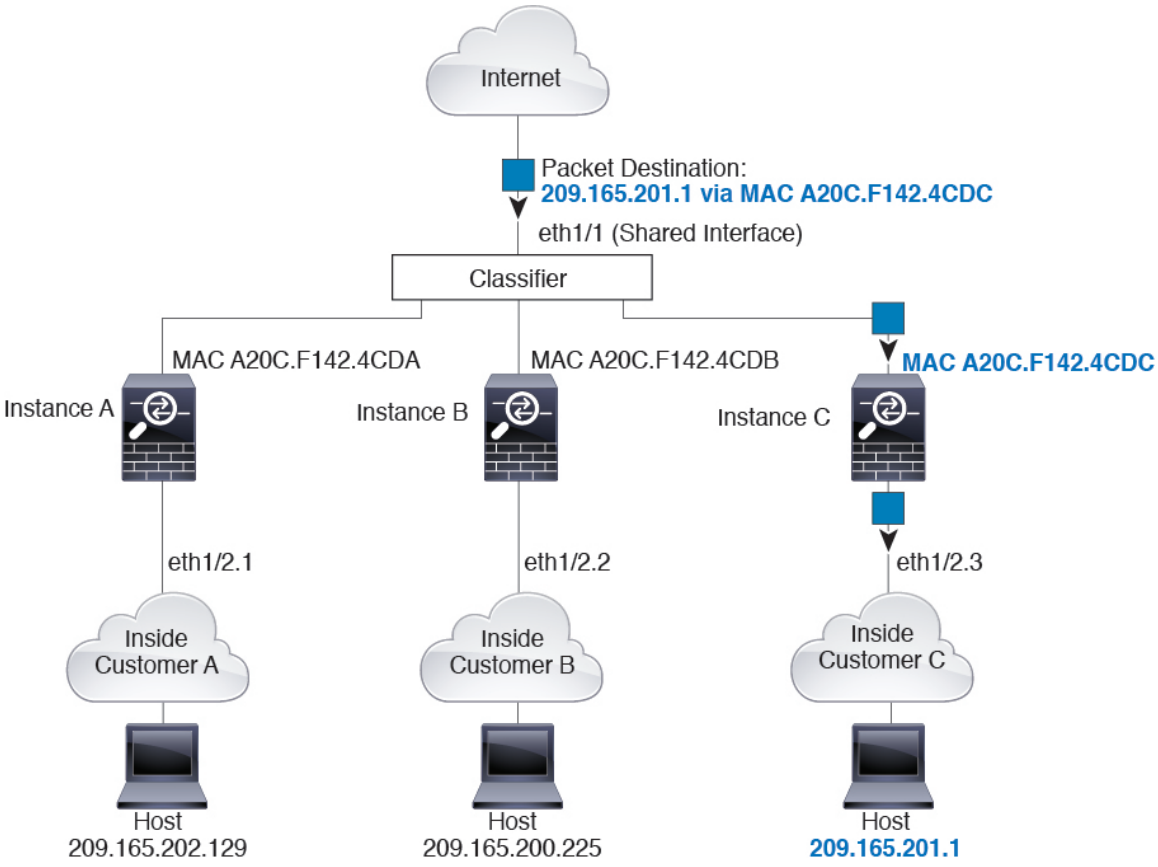
注释 如果目的 MAC 地址为组播或广播 MAC 地址，则数据包会复制并传递到每个实例。

分类示例

使用 MAC 地址通过共享接口进行数据包分类

下图显示共享外部接口的多个实例。因为实例 C 包含路由器将数据包发送到的 MAC 地址，因此分类器会将该数据包分配至实例 C。

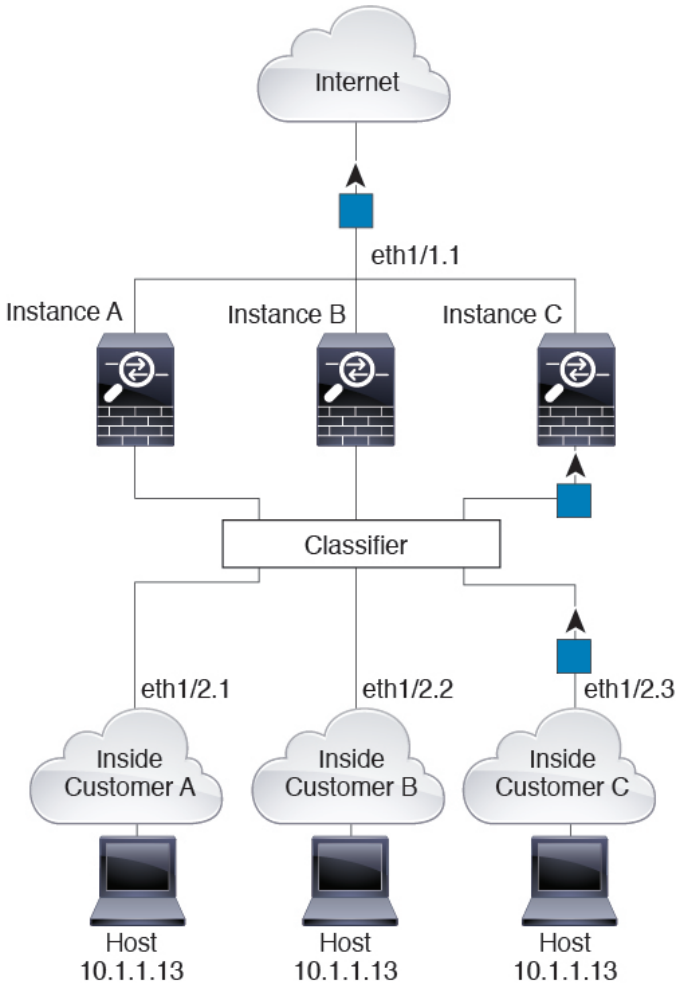
图 *6:* 使用 *MAC* 地址通过共享接口进行数据包分类



来自内部网络的传入流量

请注意，必须对所有新的传入流量加以分类，即使其来自内部网络。下图展示了实例 C 内部网络上的主机访问互联网。由于传入接口是分配至实例 C 的以太网接口 1/2.3，因此分类器会将数据包分配至实例 C。

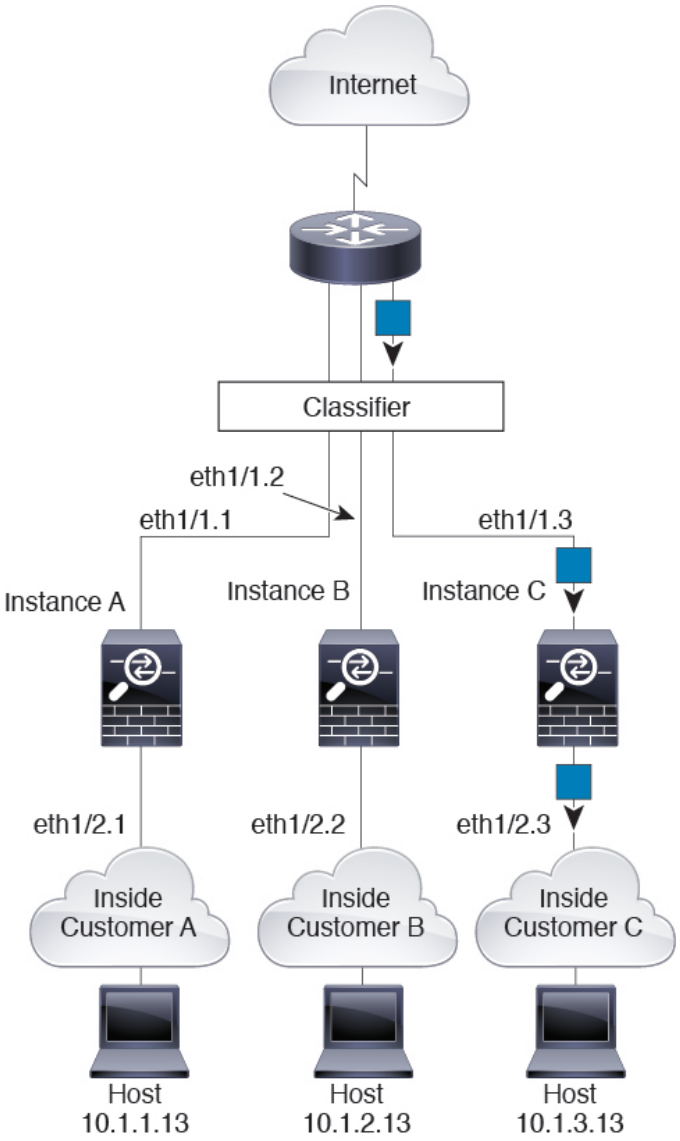
图 7: 来自内部网络的传入流量



透明防火墙实例

对于透明防火墙，您必须使用唯一接口。下图展示了来自互联网并以实例 C 内部网络上的主机为目标的数据包。由于传入接口是分配至实例 C 的以太网接口 1/2.3，因此分类器会将数据包分配至实例 C。

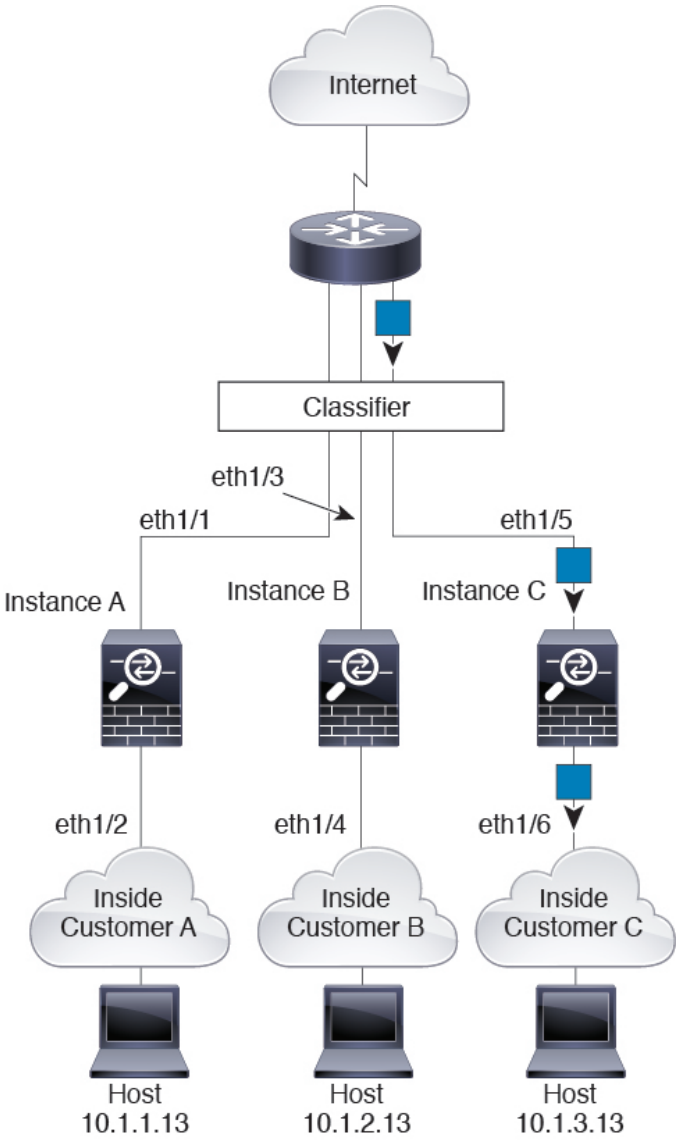
图 *8:* 透明防火墙实例



内联集

对于内联集，必须使用唯一接口，并且这些接口必须为物理接口或 Etherchannel 接口。下图展示了来自互联网并以实例 C 内部网络上的主机为目标的数据包。由于传入接口是分配至实例 C 的以太网接口 1/5，因此分类器会将数据包分配至实例 C。

图 *9:* 内联集

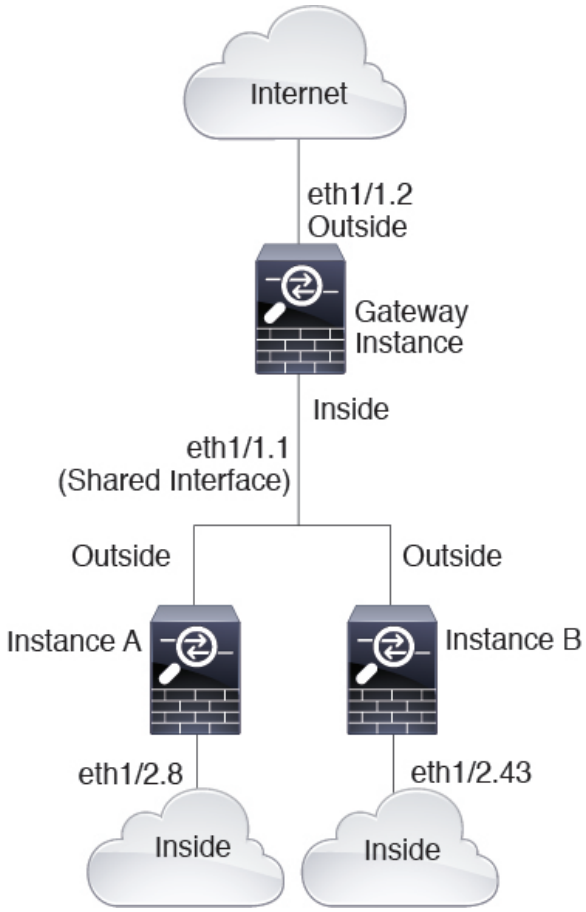


级联实例

直接在一个实例前面放置另一个实例的行为称为 级联实例；一个实例的外部接口与另一个实例的内部接口完全相同。如果您希望通过在顶级实例中配置共享参数，从而简化某些实例的配置，则可能要使用级联实例。

下图显示了在网关后有两个实例的网关实例。

图 *10:* 级联实例



注释 请勿使用具有高可用性的级联实例（使用共享接口）。发生故障转移且备用设备重新加入后，MAC 地址可能会暂时重叠并导致中断。您应改为为网关实例和内部实例使用唯一接口，使用外部交换机在实例之间传递流量。

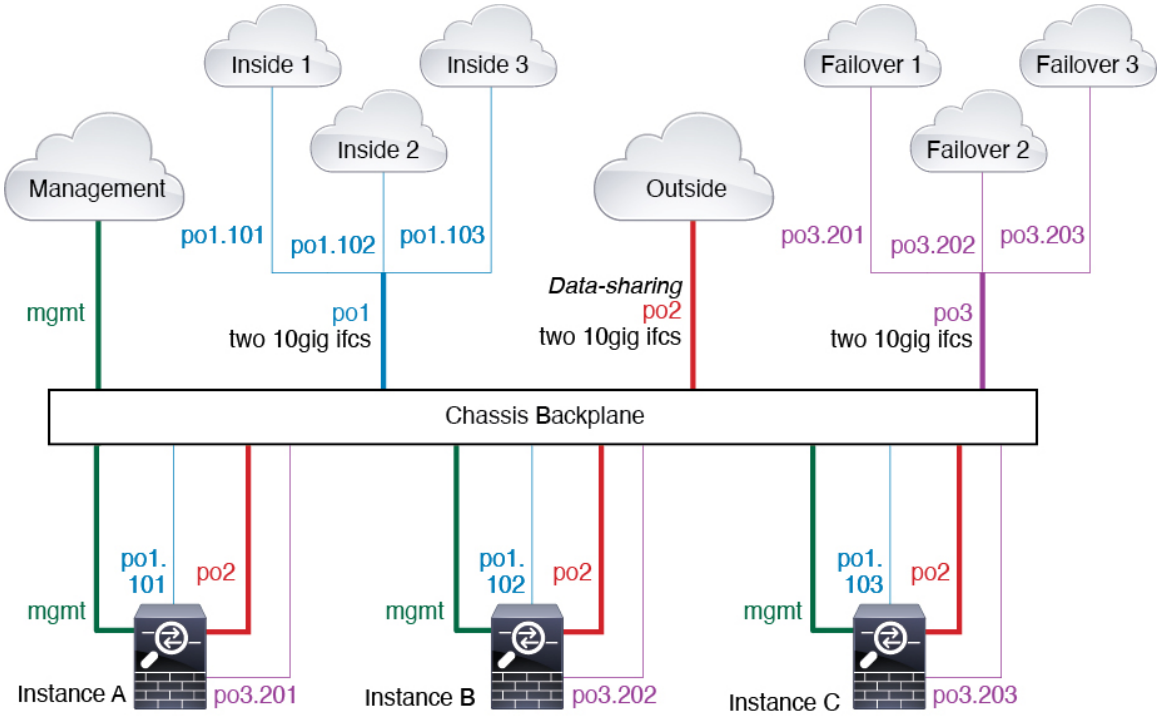
典型多实例部署

以下示例包括路由防火墙模式下的三个容器实例。这三个容器实例包括以下接口：

- 管理 - 所有实例和机箱均使用专用管理接口。在每个实例（和机箱）中，该接口都使用同一管理网络上的唯一 IP 地址。
- 内部 - 每个实例使用端口通道 1 上的子接口（数据类型）。此 EtherChannel 包括两个万兆以太网接口。每个子接口位于独立的网络中。
- 外部 - 所有实例都使用端口通道 2 接口（数据共享类型）。此 EtherChannel 包括两个万兆以太网接口。在每个应用内，该接口都使用同一外部网络上的唯一 IP 地址。

- 故障切换 - 每个实例都使用端口通道 3 上的子接口（数据类型）。此 EtherChannel 包括两个万兆以太网接口。每个子接口位于独立的网络中。

图 *11:* 典型多实例部署



实例接口的自动 MAC 地址

机箱会自动为实例接口自动生成 MAC 地址，以确保各个实例中的共享接口使用唯一 MAC 地址。

如果您手动为实例中的共享接口分配了一个 MAC 地址，则使用手动分配的 MAC 地址。如果您随后删除了手动 MAC 地址，则会使用自动生成的地址。在极少数情况下，生成的 MAC 地址会与网络中的其他专用 MAC 地址冲突，我们建议您在实例中为接口手动设置 MAC 地址。

由于自动生成的地址以 A2 开头，因此您不应该分配以 A2 开头的手动 MAC 地址，以避免出现地址重叠。

机箱使用以下格式生成 MAC 地址：

A2*xx.yyzz.zzzz*

其中， *xx.yy* 是用户定义的前缀或系统定义的前缀，*zz.zzzz* 是由机箱生成的内部计数器。系统定义的前缀与已在 IDPROM 中编程的烧录 MAC 地址池中的第一个 MAC 地址的 2 个低位字节相匹配。使用 **connect fxos**，然后通过 **show module** 查看 MAC 地址池。例如，如果显示的适用于模块 1 的 MAC 地址范围为 b0aa.772f.f0b0 至 b0aa.772f.f0bf，则系统前缀将是 f0b0。

用户定义的前缀是转换为十六进制的整数。如何使用用户定义前缀的示例如下：如果将前缀设置为 77，则机箱会将 77 转换为十六进制值 004D (*yyxx*)。在 MAC 地址中使用时，该前缀会反转 (*xxyy*)，以便与机箱的本地形式匹配：

A2**4D.00***zz.zzzz*

对于前缀 1009 (03F1)，MAC 地址为：

A2**F1.03***zz.zzzz*

多实例功能的性能扩展因素

计算平台的最大吞吐量（连接数、VPN 会话数）是为了得出设备的内存和CPU 使用情况（此值显示在 **show resource usage** 中）。如果使用多个实例，则需要根据分配给实例的 CPU 核心百分比来计算吞吐量。例如，如果使用具有 50% 核心的实例，则最初应计算 50% 的吞吐量。此外，尽管扩展可能会因为您的网络而更好或更差，但实例可用的吞吐量可能低于应用可用的吞吐量。

有关计算实例吞吐量的详细说明，请参阅https://www.cisco.com/c/en/us/products/collateral/security/firewalls/white-paper-c11-744750.html。

实例与高可用性

您可以在 2 个独立机箱上使用实例来实现高可用性；例如，如果您有 2 个机箱，每个机箱设 10 个实例，您可以创建10个高可用性对。您还可以在高可用性实例所在的机箱上设置独立实例。有关详细要求，请参阅 实例的要求和前提条件 ，第 14 页。

注释 不支持群集。

实例的许可证

所有许可证均按机箱使用，而不是按实例使用。请查看以下详细信息：

- 基础版 许可证作为一个整体分配给机箱，每个机箱一个。
- 功能许可证分配到每个实例；但每个机箱每个功能只能 使用 一个许可证。

实例的要求和前提条件

型号支持

- Cisco Secure Firewall 3110
- Cisco Secure Firewall 3120
- Cisco Secure Firewall 3130
- Cisco Secure Firewall 3140

- Cisco Secure Firewall 4215
- Cisco Secure Firewall 4225
- Cisco Secure Firewall 4245

注释 不支持 Cisco Secure Firewall 3105。

每个型号的最大容器实例数和资源容量

对于每个容器实例，您可以指定要分配至实例的CPU核心数量（或更具体地说，线程数）。我们通常使用术语“核心”来表示不同的硬件架构。系统会根据核心数量动态分配RAM，并将每个实例的磁盘空间设为 40 GB。

表 *1:* 每个型号的最大容器实例数和资源容量

型号	最大容器实例数	可用 **CPU** 核心（线程数）
Cisco Secure Firewall 3110	3	22
Cisco Secure Firewall 3120	5	30
Cisco Secure Firewall 3130	7	46
Cisco Secure Firewall 3140	10	62
Cisco Secure Firewall 4215	10	62
Cisco Secure Firewall 4225	15	126
Cisco Secure Firewall 4245	34	254

软件要求

- 您可以在每个实例上运行不同版本的 软件，只要它们都与机箱上运行的 FXOS 版本兼容。
- 您无法部署带有 软件补丁程序版本的实例，因为它不是一个完整的捆绑包。您需要先部署主要或维护版本，然后在部署后安装补丁程序。

高可用性要求

- 高可用性配置中的两个实例必须：
  - 位于单独的机箱上。
  - 位于相同的型号。
  - 分配相同的接口。启用高可用性之前，所有接口必须在机箱中进行相同的预配置。
  - 使用相同的资源配置文件属性。配置文件名称可以不同，但定义需要匹配。

防火墙管理中心 要求

对于机箱管理和机箱上的所有实例，由于许可实施，您必须使用相同的 防火墙管理中心 。

实例的准则和限制

一般准则

- 单个 防火墙管理中心 必须管理机箱上的所有实例，以及管理机箱本身。
- 对于实例，不支持以下功能：
  - TLS 加密加速
  - 集群
  - 防火墙管理中心 UCAPL/CC 模式
  - 到硬件的数据流分流
- 不支持通过 安全云控制 云交付 防火墙管理中心 对机箱进行主要管理，也不支持通过本地部署 防火墙管理中心 对机箱进行单独的仅分析管理。但是，您可以将 安全云控制 托管的实例添加到本地分析专用 防火墙管理中心。

管理界面

- 不支持用于机箱管理的数据接口；只能使用专用的管理接口
- 管理接口无 DHCP 寻址

VLAN 子接口

- 本文档仅讨论 机箱 VLAN 子接口。您还可以在实例内单独创建子接口。
- 如果将父接口分配至实例，该接口将仅传递未标记（非 VLAN）流量。除非您想要传递未标记流量，否则不予分配父接口。
- 子接口在数据或数据共享型接口。
- 最多可以创建 500 个 VLAN ID。
- 不得将子接口用于内联集或用作被动接口。
- 如果将子接口用于故障转移链路，则该父接口及其上的所有子接口仅限于用作故障转移链路。不得将某些子接口用作故障转移链路，而将某些用作常规数据接口。

EtherChannel

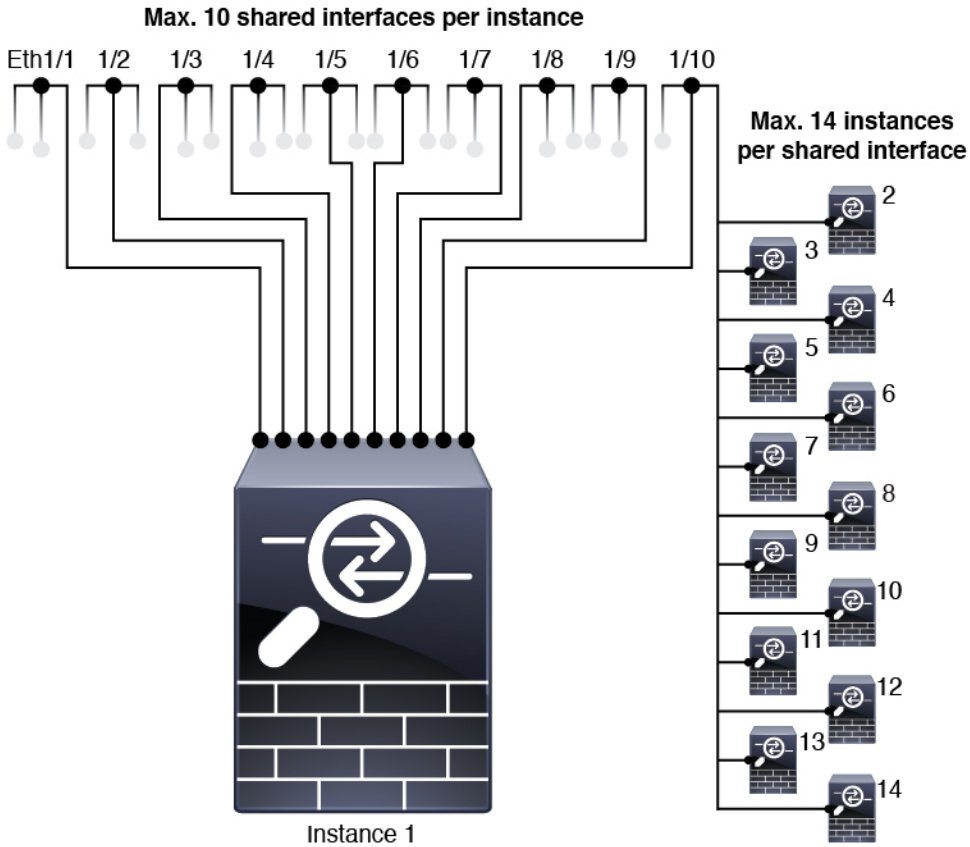
- 您最多可以配置 48 个 EtherChannel，受物理接口数量限制。

- EtherChannel 最多可以有 8 个主用接口。
- EtherChannel 中的所有接口必须具有相同的介质类型和速度容量。介质类型可以是 RJ-45 或 SFP；可以混合使用不同类型（铜缆和光纤）的 SFP。除非将速度设置为**检测 SFP**，否则不能通过将较大容量接口的速度设置为较低来混合接口容量（例如 1GB 和 10GB 接口）;在这种情况下，您可以使用不同的接口容量，并使用最低的通用速度。
- 机箱不支持带有 VLAN 标记的 LACPDU。如果使用思科 IOS **vlan dot1Q tag native** 命令在相邻交换机上启用本地 VLAN 标记，则机箱将会丢弃已标记的 LACPDU。请务必禁用相邻交换机上的本地 VLAN 标记。
- 在低于 15.1(1)S2 的思科 IOS 软件版本中，机箱不支持将 EtherChannel 连接到交换机堆叠。在默认交换机设置下，如果跨堆叠连接机箱 EtherChannel，则当主要交换机关闭时，连接到其余交换机的 EtherChannel 不会正常工作。要提高兼容性，请将 **stack-mac persistent timer** 命令设置为一个足够大的值，以考虑重新加载时间；例如，8 分钟或无限接近 0。或者，您可以升级到更加稳定的交换机软件版本，例如 15.1(1)S2。

数据共享接口

- 每个共享接口最多 14 个实例。例如，您可以将以太网接口 1/1 分配至实例 1 至实例 14。

  每个实例最多 10 个共享接口。例如，您可以将以太网接口 1/1.1 至以太网接口 1/1.10 分配至实例 1。



- 不得结合使用数据共享接口和透明防火墙模式接口。
- 不得结合数据共享接口和内联集或被动接口。
- 不得将数据共享接口用于故障转移链路。

默认 MAC 地址

- 所有接口的 MAC 地址均取自一个 MAC 地址池。对于子接口，如果决定要手动配置 MAC 地址，请确保将唯一 MAC 地址用于同一父接口上的所有子接口，从而确保分类正确。请参阅实例接口的自动 MAC 地址，第 13 页。

配置实例

在配置实例之前，您需要启用多实例模式，将机箱添加到 防火墙管理中心，并配置机箱接口。您还可以自定义机箱设置。

将设备转换为多实例模式

使用此程序将 防火墙管理中心 中的设备转换为多实例模式。转换大约需要 15 分钟。系统将重新启动，并在更改模式时清除配置，但管理网络设置和管理员密码除外。机箱主机名设置为“firepower-*model*”。管理 IP 地址分配给机箱，用于通过 防火墙管理中心 进行管理连接。当您添加实例时，它们将在管理接口上使用单独的 IP 地址并维护自己的管理连接。

在转换为多实例模式后，您可以使用 防火墙管理中心 配置所有机箱设置以及实例。不支持 FXOS CLI 上的 Cisco Secure Firewall 机箱管理器 或配置。

注释 如果您希望在将设备添加到 防火墙管理中心 之前使用 CLI 转换为多实例模式，请参阅在 CLI 启用多实例模式，第 55 页。

开始之前

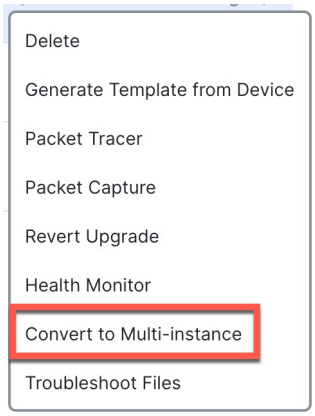
将设备模式设备作为独立设备添加到 防火墙管理中心 。此设备无法使用：

- 用于管理器访问的数据接口
- 管理接口的 DHCP
- 零接触调配

过程

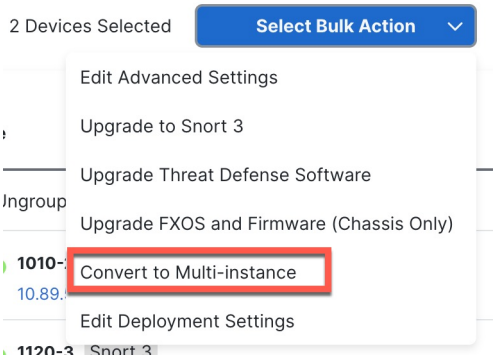
步骤 1 在 **设备** > **设备管理** 上，在要转换为多实例模式的设备旁边，选择 **更多** (⋮) > **转换为多实例**。

图 *12:* 转换为多实例



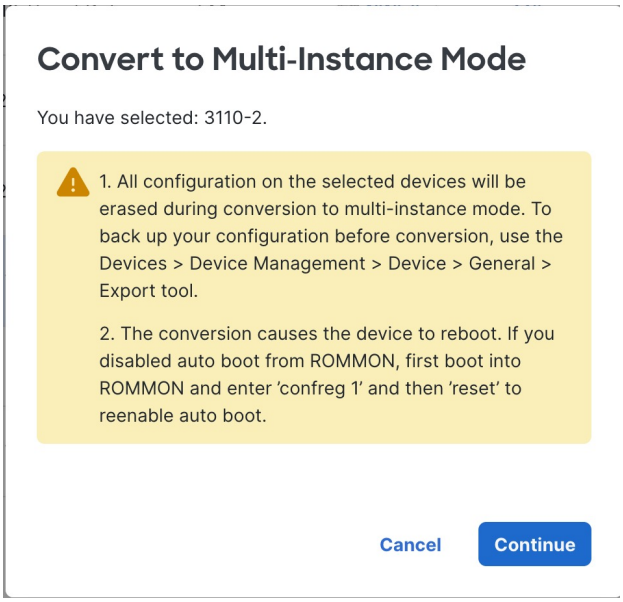
您也可以选中要转换的多个设备旁边的复选框，然后选择**选择批量操作 (Select Bulk Action)** > **转换为多实例 (Convert to Multi-Instance)**。

图 *13:* 批量转换



步骤 2 确认您要执行转换，然后点击**继续**。

图 *14:* 转换确认



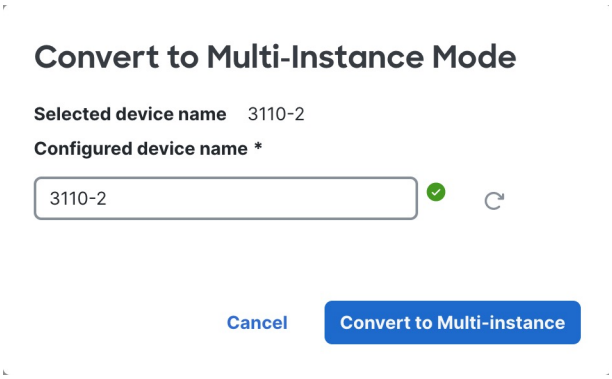
执行就绪性检查。例如，如果部署正在进行，则检查可能会失败。

步骤 3 或者，更改机箱的名称，然后点击**转换为多实例 (Convert to Multi-Instance)**。默认情况下，使用设备名称，但您可能需要为多实例机箱使用不同的命名约定。

注释

如果就绪性检查失败（例如，由于正在进行部署），您可以等待该过程完成，然后点击 以重新运行就绪性检查，以便继续。

图 *15:* 重命名机箱

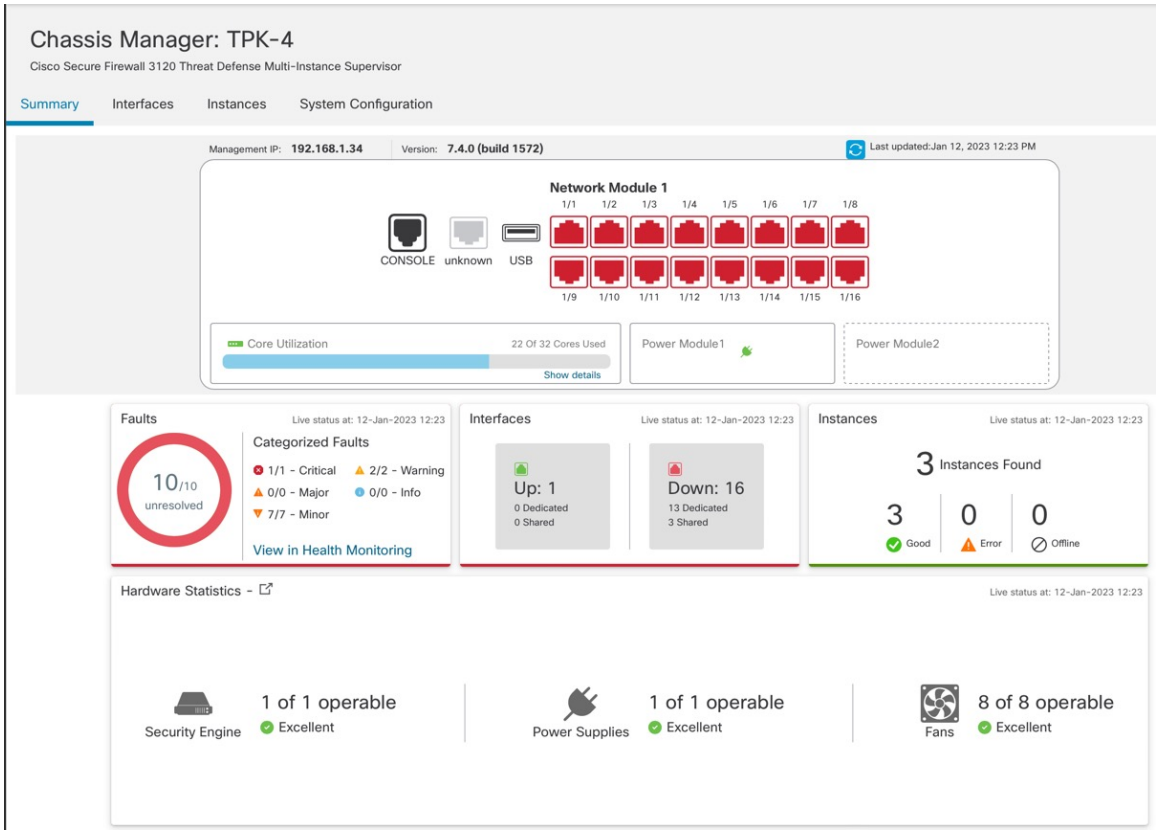


等待大约 15 分钟，在此期间设备将从设备列表中删除，然后在转换后将其重新添加为机箱。

步骤 4 要查看和配置机箱，请点击 **机箱** 列中的 **管理** ，或点击 **编辑** ()。

打开机箱的 **机箱管理器** 页面，进入 **摘要** 页面。

图 *16:* 机箱摘要



配置机箱接口

在机箱层面，配置物理接口、实例的 VLAN 子接口和 EtherChannel 接口的基本以太网设置。默认情况下，物理接口处于禁用状态。

注释 要配置分支端口并执行其他网络模块操作，请参阅 管理 Cisco Secure Firewall 3100/4200的网络模块。

注释 有关 **同步设备** 按钮的信息，请参阅 与 防火墙管理中心同步接口更改。

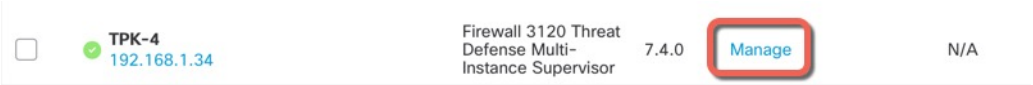
配置物理接口

您可以通过物理方式启用和禁用接口，并设置接口速度和双工及其他硬件设置。要使用某一接口，必须为机箱以物理方式启用它，并在ASA中以逻辑方式启用它。默认情况下，物理接口处于禁用状态。对于 VLAN 子接口，其管理状态继承自父接口。

过程

步骤 1 在 **设备** > **设备管理** 中，点击**机箱**列中的**管理**或点击**编辑** (✎)。

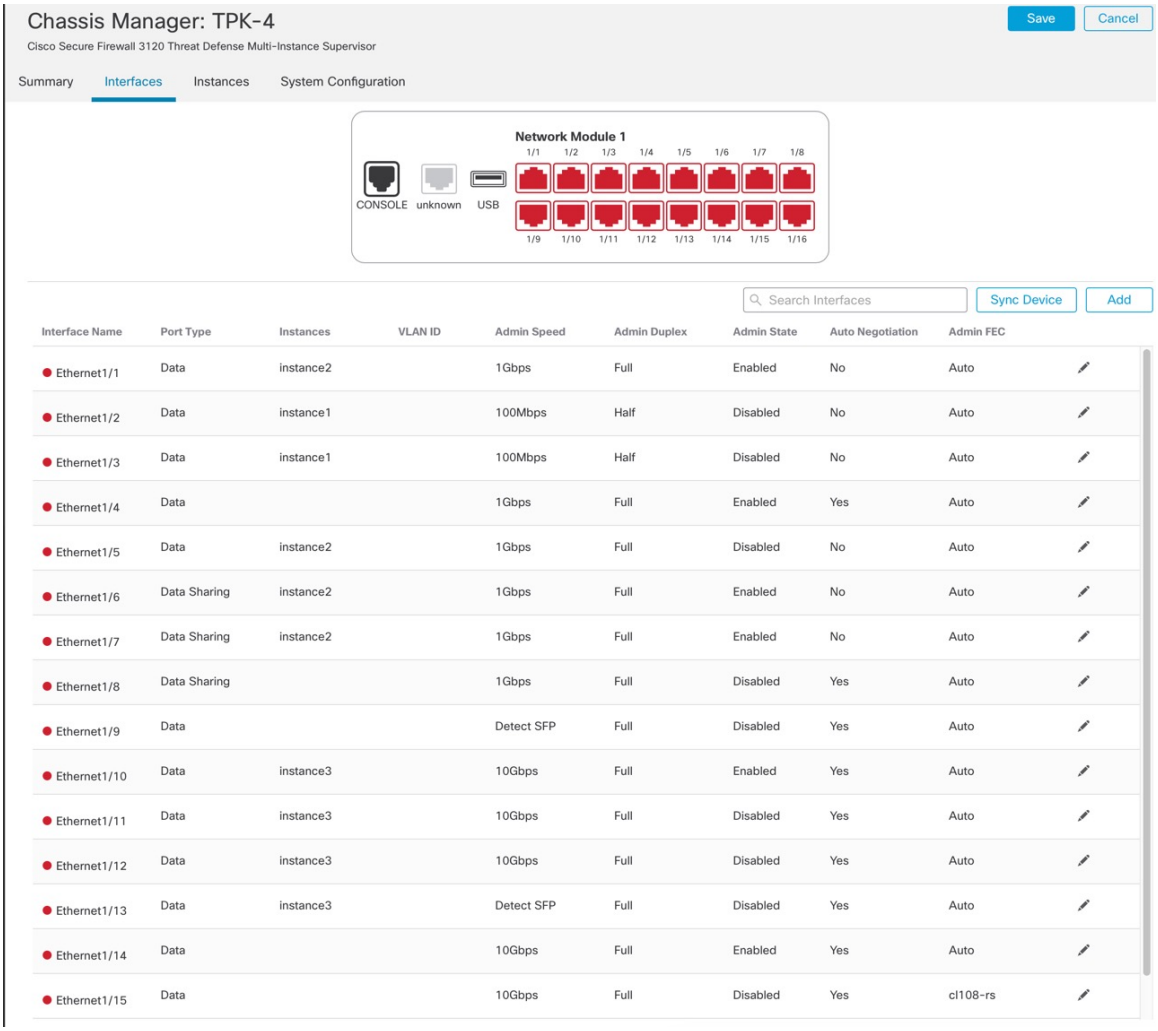
图 *17:* 管理机箱



打开机箱的 **机箱管理器** 页面，进入 **摘要** 页面。

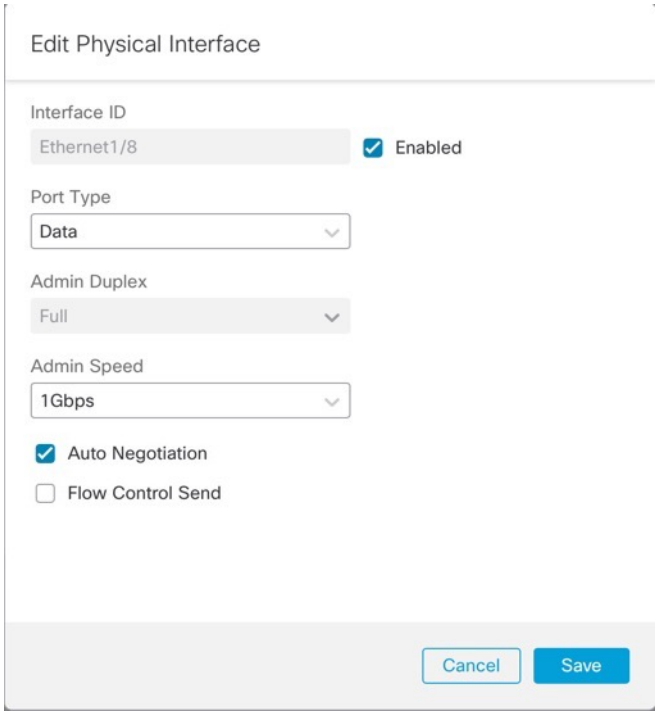
步骤 2 点击**接口 (Interfaces)**。

图 *18:* 接口



步骤 3 点击要编辑的接口的 **编辑** (✎)。

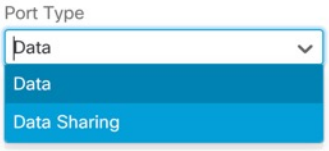
图 *19:* 编辑物理接口



步骤 4 选中**启用**复选框以启用此接口。

步骤 5 对于 **端口类型**，选择 **数据** 或 **数据共享**。

图 *20:* 端口类型



步骤 6 设置 **管理员双工**。

1Gbps 及更高的速度仅支持 **全双工** 。SFP 接口仅支持 **全** 复用。

步骤 7 设置 **管理员速度**。

对于 SFP，选择 **检测 SFP** 以检测已安装的 SFP 模块的速度并使用适当的速度。复用始终为全复用，并且始终启用自动协商。如果您稍后将网络模块更改为其他型号，并希望速度自动更新，则此选项非常有用。

步骤 8 （可选） 选中 **LLDP 传输** 和/或 **LLDP 接收** 以启用链路层发现协议 (LLDP) 数据包。

步骤 9 （可选） 选中 **流量控制发送** 以启用暂停 (XOFF) 帧以进行流量控制。

流量控制通过允许拥塞节点在另一端暂停链路操作，从而让连接的以太网端口能够在拥塞期间控制流量速率。如果威胁防御端口遇到拥塞（内部交换机上的排队资源耗尽）并且无法接收更多流量，

则它会通过发送暂停帧来通知另一个端口停止发送，直到状况恢复正常为止。在收到暂停帧后，发送设备会停止发送任何数据包，从而防止在拥塞期间丢失任何数据包。

注释
支持传输暂停帧，以便远程对等体可以对流量进行速率控制。

但是，不支持接收暂停帧。

内部交换机有一个包含 8000 个缓冲区的全局池，而每个缓冲区都有 250 个字节，并且交换机会为每个端口动态分配缓冲区。当缓冲区使用量超过全局高水位标记（2 MB [8000 个缓冲区]）时，会在每个启用了流量控制的接口上发送暂停帧；当特定接口的缓冲区超过端口高水位标记（0.3125 MB [1250 个缓冲区]）时，会从该接口发送暂停帧。在发送暂停后，如果缓冲区使用率降低至低水位标记之下（全局 1.25 MB [5000 个缓冲区]；每个端口 0.25 MB [1000 buffers]），则可发送 XON 帧。链接伙伴可在收到 XON 帧之后恢复流量。

系统仅支持 802.3x 中定义的流量控制帧。系统不支持基于优先级的流量控制。

步骤 10 （可选） 选中 **自动协商** 以设置接口以协商速度、链路状态和流量控制。对于低于 1 Gbps 的速度，无法编辑此设置。对于 SFP 接口，只能在速度设置为 1 Gbps 时禁用自动协商。

步骤 11 点击 **保存**，然后点击 **接口** 页面右上角的 **保存**。

现在，您可以将策略 **部署** 到机箱。在部署更改之后，更改才生效。

配置 EtherChannel

EtherChannel（也称为端口通道）最多可以包含 8 个同一介质类型和容量的成员接口，并且必须设置为相同的速度和双工模式。介质类型可以是 RJ-45 或 SFP；可以混合使用不同类型（铜缆和光纤）的 SFP。除非将速度设置为**检测 SFP**，否则不能通过将较大容量接口的速度设置为较低来混合接口容量（例如 1GB 和 10GB 接口）;在这种情况下，您可以使用不同的接口容量，并使用最低的通用速度。

链路汇聚控制协议 (LACP) 将在两个网络设备之间交换链路汇聚控制协议数据单元 (LACPDU)，进而汇聚接口。LACP 将协调自动添加和删除指向 EtherChannel 的链接，而无需用户干预。LACP 还会处理配置错误，并检查成员接口的两端是否连接到正确的通道组。如果接口发生故障且未检查连接和配置，“开启”模式将不能使用通道组中的备用接口。

机箱创建 EtherChannel 时，EtherChannel 将处于**挂起**状态（对于主动 LACP 模式）或**关闭**状态（对于打开 LACP 模式），直到将其分配给逻辑设备，即使物理链路是连通的。将 EtherChannel 添加到实例时，它将退出此 **挂起** 状态。

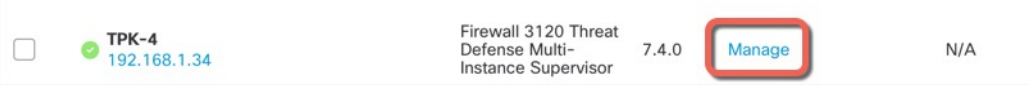
开始之前

启用物理接口并设置硬件参数。请参阅配置物理接口，第 21 页。

过程

步骤 1 在 **设备** > **设备管理** 中，点击**机箱**列中的**管理**或点击**编辑** (✎)。

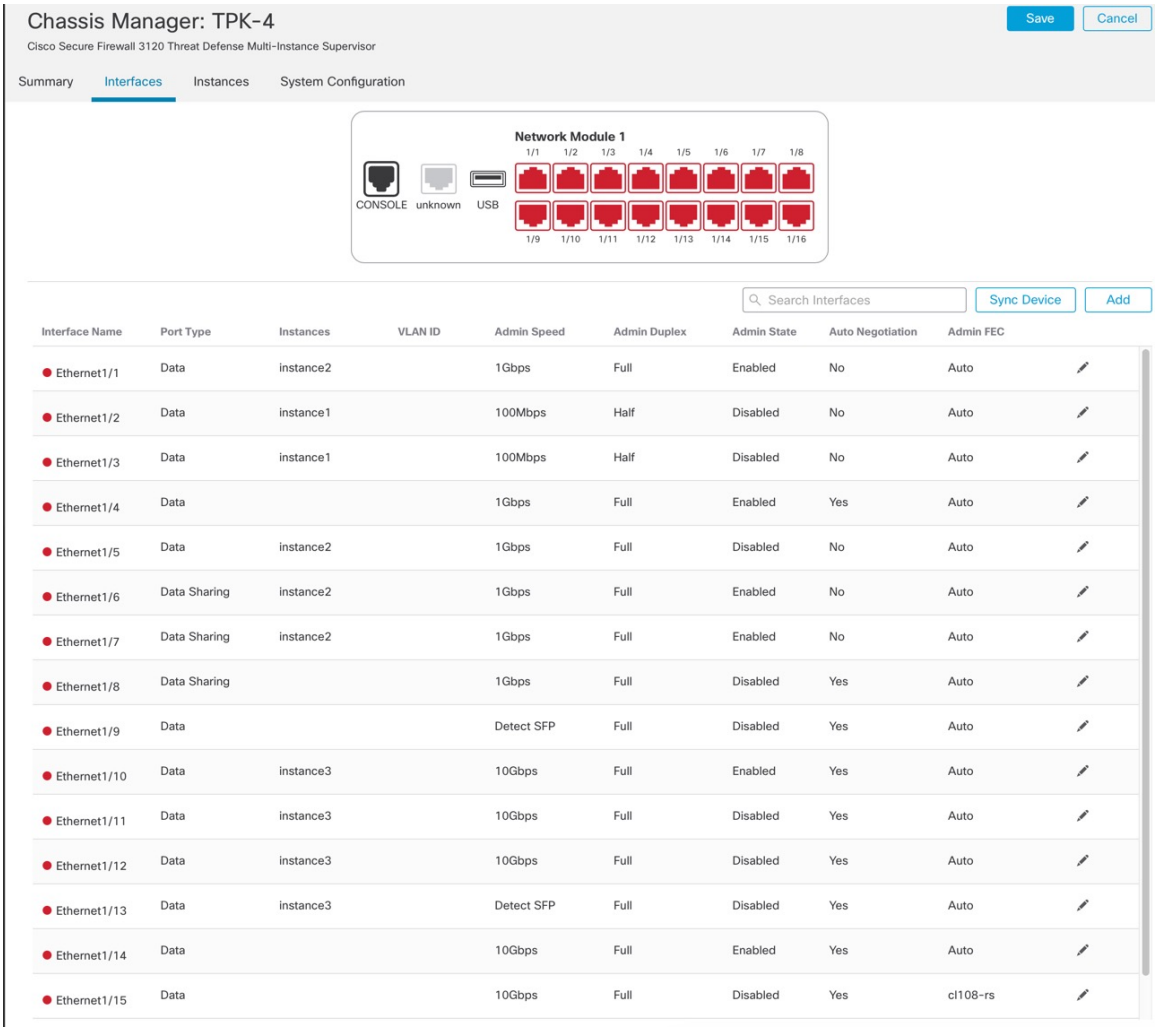
图 *21:* 管理机箱



打开机箱的 **机箱管理器** 页面，进入 **摘要** 页面。

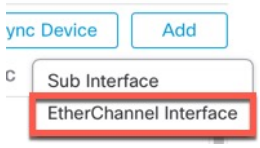
步骤 2 点击**接口 (Interfaces)**。

图 *22:* 接口



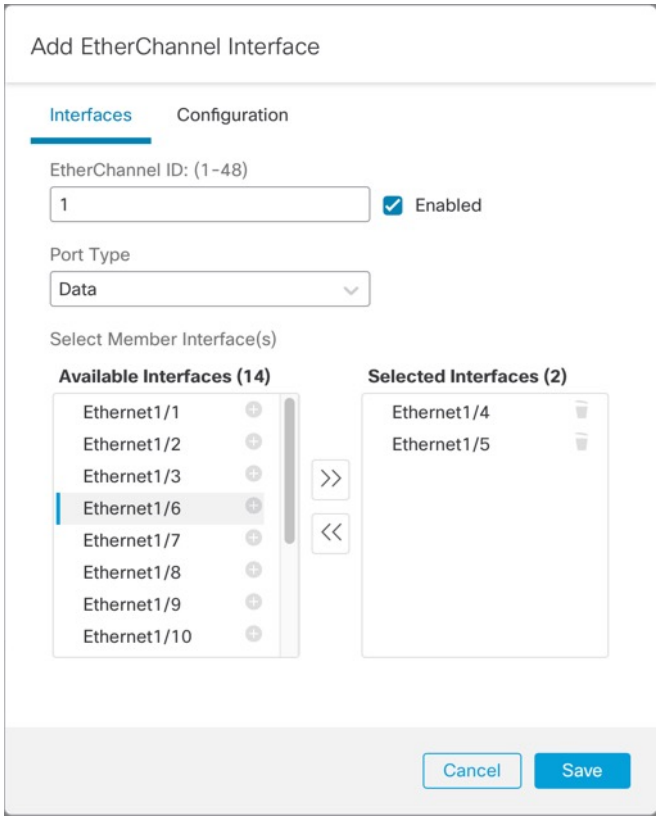
步骤 3 点击 **添加** > **EtherChannel 通道接口**

图 *23:* 添加 ***EtherChannel***



步骤 4 设置以下 **接口** 参数。

图 *24:* 接口设置



a) 对于 **EtherChannel ID**，请指定一个介于 1 和 48 之间的 ID。

b) 点击**已启用**。

c) 对于 **端口类型**，请选择 **数据** 或 **数据共享**。

有关端口类型的信息，请参阅 接口类型，第 2 页。

d) 要将物理接口添加到 EtherChannel，请在**可用接口**列表中选择点击 **添加** (⊕) 以将其移动到**选定的接口**列表。

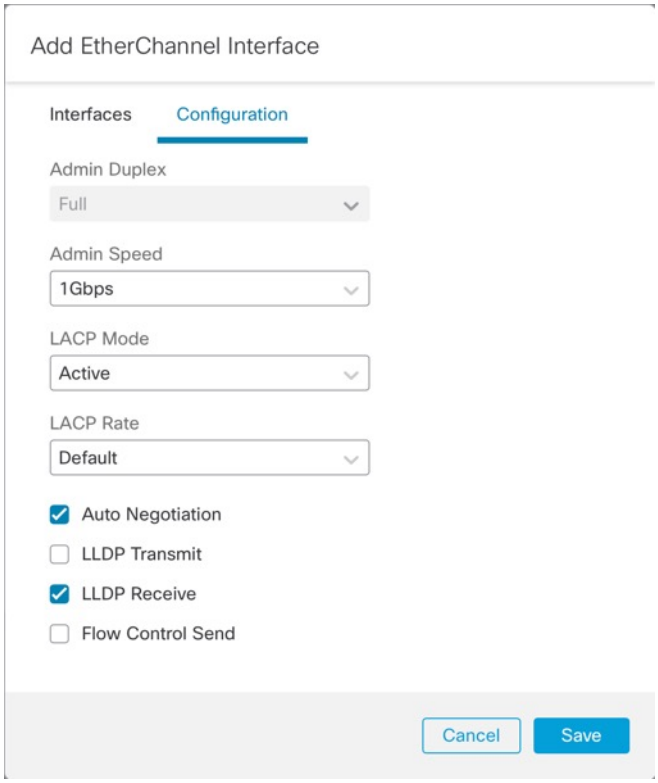
要添加或删除所有接口，请点击双箭头按钮。

注释
不能添加已分配给实例的接口。

步骤 5 （可选） 设置以下 **配置** 参数。

其中许多设置（不包括 LACP 设置）为要包含在 EtherChannel 中的接口设置了要求；它们不会覆盖成员接口的设置。例如，如果选中**LLDP传输**，则应仅添加具有该设置的接口。如果将 **管理速度** 设置为 1Gbps，则只能包括 1Gbps 接口。

图 *25:* 配置设置



a) 为成员接口、 **全双工** 或 **半双工** 选择所需的 **管理双工** 。

如果添加以指定双工配置的成员接口，接口将无法成功加入端口通道。

b) 从下拉列表选择成员接口要求的 **管理速度**。

如果添加未达到指定速度的成员接口，接口将无法成功加入端口通道。

c) 选择 **LACP 模式**、 **活动** 或 **打开**。

- **主用**-发送和接收 LACP 更新。主用 EtherChannel 可以与主用或备用 EtherChannel 建立连接。除非您需要最大限度地减少 LACP 流量，否则应使用主用模式。
- **开启** - EtherChannel 始终开启，并且不使用 LACP。“开启”的 EtherChannel 只能与另一个“开启”的 EtherChannel 建立连接。

注释
如果将其模式从打开更改为主用或从主用更改为打开状态，则可能需要多达三分钟的时间才能使 EtherChannel 进入运行状态。

d) 选择 **LACP Rate**、 **Default**、 **Fast**或 **Normal**。

默认值为 **Fast**。

e) 通过选中 **LLDP 传输** 和/或 **LLDP 接收**，为成员接口选择所需的链路层发现协议 (LLDP) 设置。

f) 检查成员接口所需的 **流量控制发送** 设置。

步骤 6 点击 **保存**，然后点击 **接口** 页面右上角的 **保存** 。

现在，您可以将策略 **部署** 到机箱。在部署更改之后，更改才生效。

配置子接口

您最多可以将 500 个子接口连接到您的机箱。

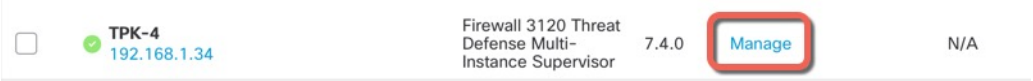
每个接口的 VLAN ID 都必须具有唯一性，并且在实例内，VLAN ID 在所有已分配接口上也必须具有唯一性。只要系统将 VLAN ID 分配至不同的实例，您就可以在 单独 接口上重新使用它们。然而，即使每个子接口使用相同的 ID，这些子接口仍将计入限值。

本部分仅讨论 *FXOS* VLAN 子接口。您还可以在实例内单独创建子接口。请参阅机箱接口与实例接口，第 3 页。

过程

步骤 1 在 **设备** > **设备管理** 中，点击**机箱**列中的**管理**或点击**编辑** (✎)。

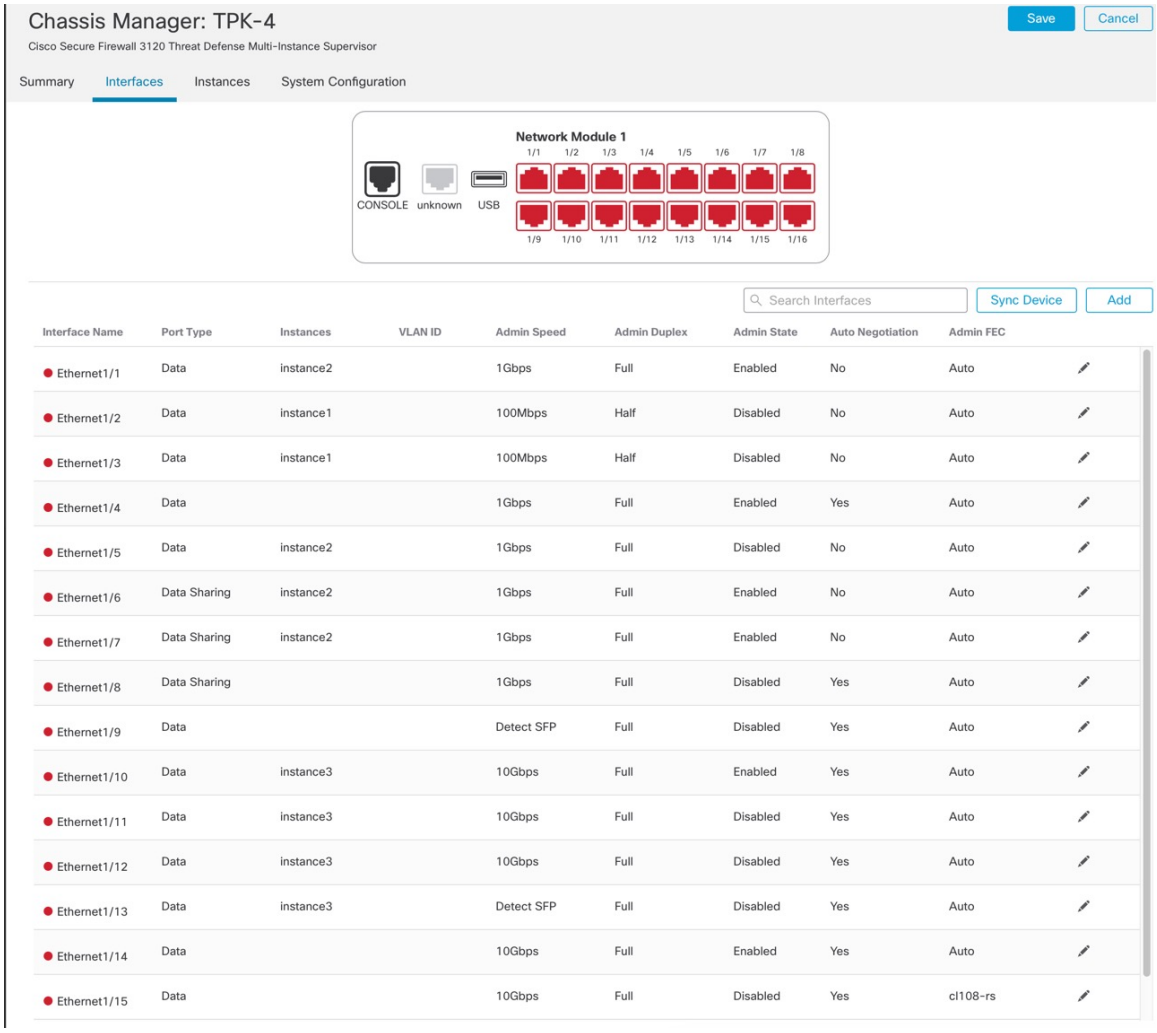
图 *26:* 管理机箱



打开机箱的 **机箱管理器** 页面，进入 **摘要** 页面。

步骤 2 点击**接口 (Interfaces)**。

图 *27:* 接口

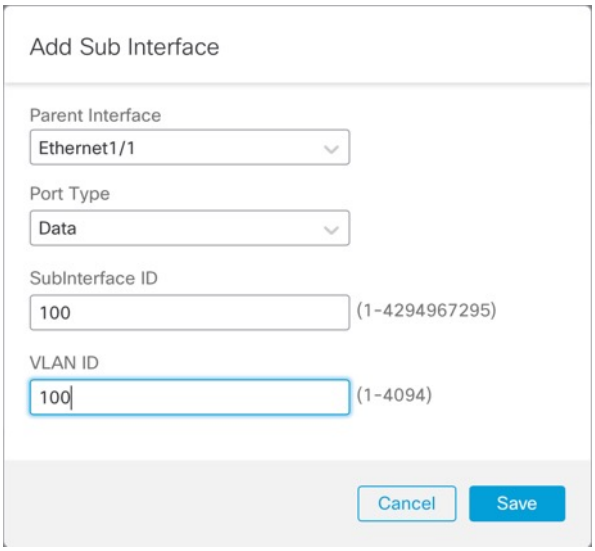


步骤 3 点击 添加 > 子接口

图 *28:* 添加子接口

步骤 4 设置以下参数。

图 *29:* 子接口设置



a)

步骤 5 点击 **保存**，然后点击 **接口** 页面右上角的 **保存**。

现在，您可以将策略 **部署** 到机箱。在部署更改之后，更改才生效。

添加实例

您可以在多实例模式下将一个或多个实例添加到机箱。支持的实例数量取决于您的型号；请参阅 实例的要求和前提条件，第 14 页。

开始之前

将设备转换为多实例模式，第 18 页。

过程

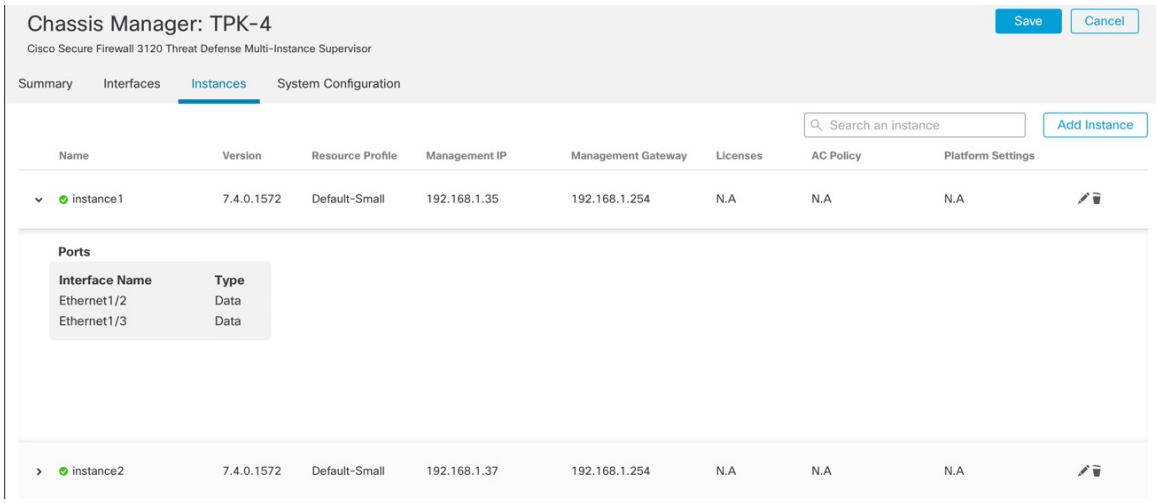
步骤 1 在 **设备** > **设备管理** 中，点击**机箱**列中的**管理**或点击**编辑** (✎)。

图 *30:* 管理机箱

打开机箱的 **机箱管理器** 页面，进入 **摘要** 页面。

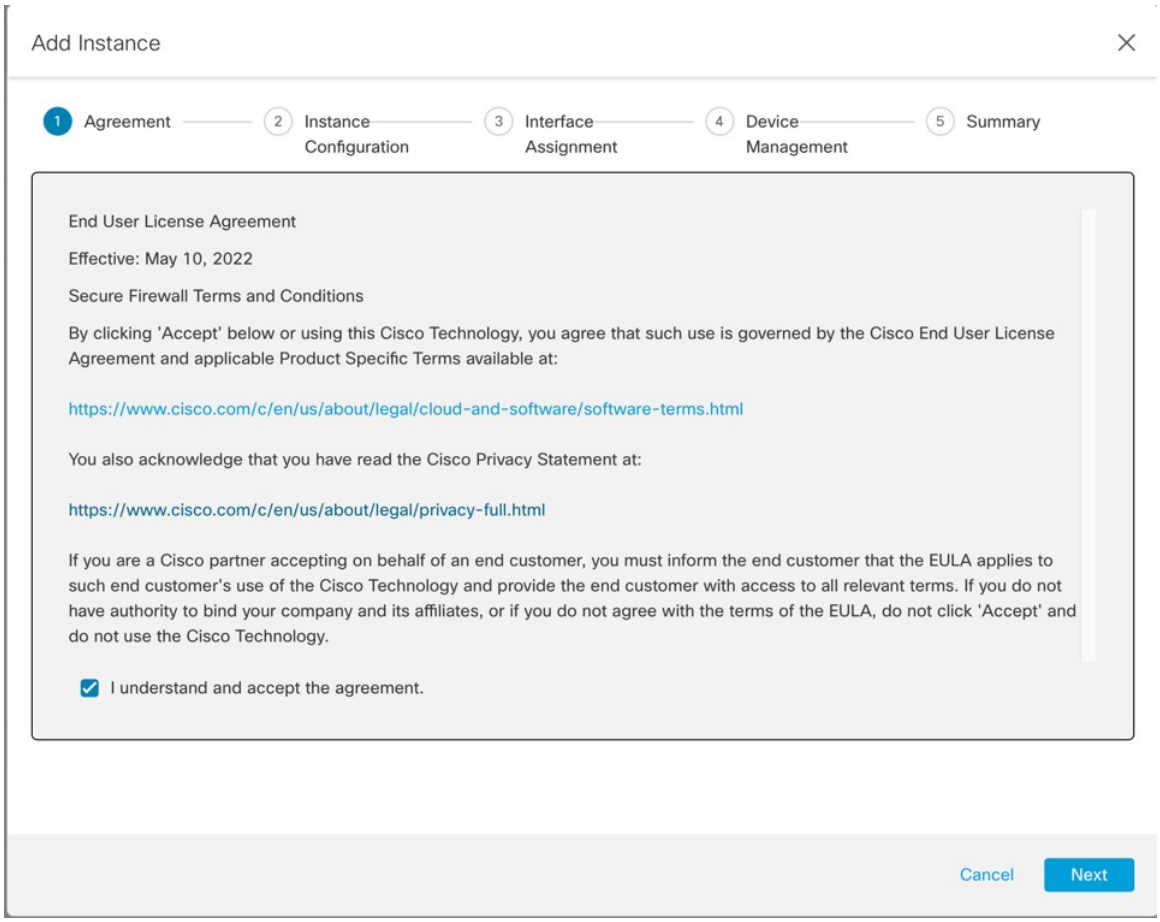
步骤 2 点击 **实例**，然后点击 **添加实例**。

图 *31:* 实例



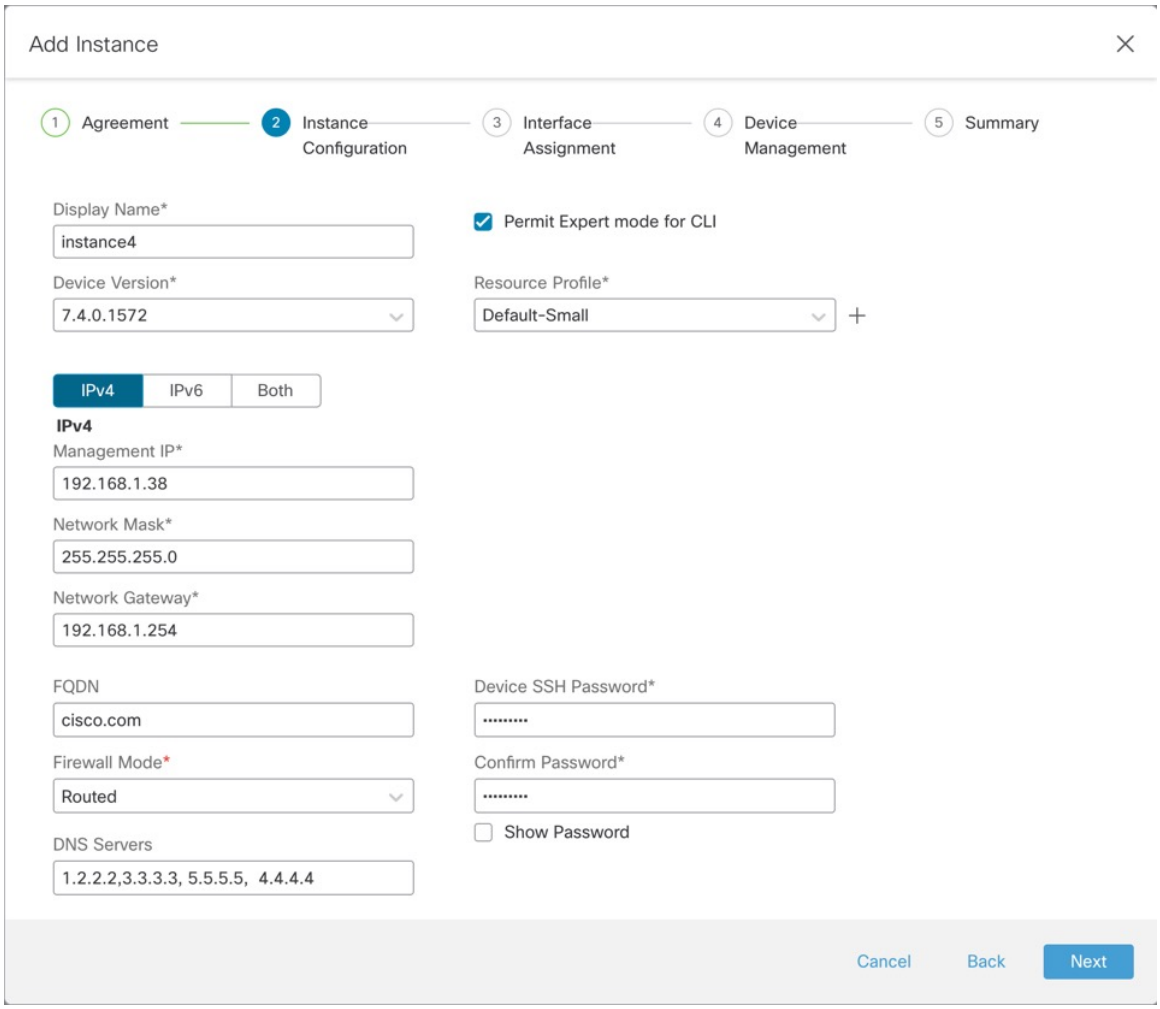
步骤 **3** 在 协议中，选中 **我了解并接受协议**，然后点击 **下一步**。

图 *32:* 协议



步骤 4 在 **实例配置**中，设置实例参数，然后点击 **下一步**。

图 *33:* 实例配置



- **显示名称**
- **设备版本**-列出的版本是当前下载到机箱的软件包。补丁版本没有列出，也不能使用，因为它们未包含整个软件包。要升级到新软件包，请参阅 **设备** > **升级** > **机箱升级**。升级时，旧 版本和新 版本都将在菜单中列出。要下载较旧的软件包，您需要使用 FXOS CLI。注意：FXOS 和 映像都包含在同一软件包中。有关详细信息，请参阅 故障排除指南 。

  例如：

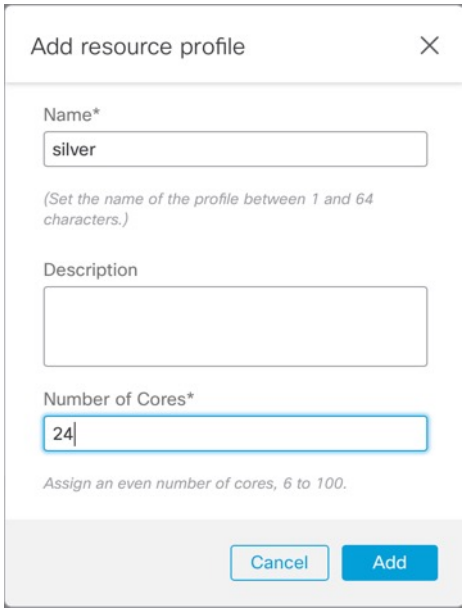
```
firepower-3110# scope firmware
firepower-3110# download image
https://10.10.7.89/Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-1.sh.DEV.tar
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
% Download-task Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-1.sh.DEV.tar : completed successfully.
```

- **IPv4、IPv6 或两者 (Both)** - 在与机箱管理接口相同的网络上设置**管理 IP (Management IP)** 地址。设置**网络掩码 (Network Mask)** 和网关（可能与机箱相同）。机箱管理接口与每个实例共享，每个实例在网络上都有自己的 IP 地址。默认情况下，您可以通过 SSH 连接到此 IP 地址以访问 CLI。
- （可选） **FQDN**
- **防火墙模式 - 路由** 或 **透明**。有关防火墙模式的详细信息，请参阅透明或路由防火墙模式。
- **DNS 服务器**- 输入仅用于管理流量的 DNS 服务器列表（以逗号分隔）。
- （可选）**适用于 CLI 的专家模式许可**-专家模式提供 外壳访问权限以确保实现高级故障排除。

  如果启用此选项，拥有直接从 SSH 会话访问实例的权限的用户可以输入专家模式。如果禁用此选项，只有拥有从 FXOS CLI 访问实例的权限的用户可以输入专家模式。我们建议禁用此选项以加强实例之间的隔离。

  仅当书面程序指出必须使用或思科技术支持中心要求使用专家模式时，才使用专家模式。要进入此模式下，请在 CLI 中使用 **专家** 命令。
- **资源配置文件** - 资源配置文件会设置 CPU 核心数量；系统会根据核心数量动态分配 RAM，并将每个实例的磁盘空间设为 40 GB。机箱包括以下默认资源配置文件：Default-Small、Default-Medium 和 Default-Large。您可以通过点击 **添加** (+)为此机箱添加其他配置文件。以后无法编辑资源配置文件。

图 *34:* 添加资源配置文件



  - 最小核心数量为 6。

    注释
    与具有较大内核数量的实例相比，具有较小核心数量的实例可能具有相对更高的CPU利用率。具有较小核心数量的实例对流量负载变化更敏感。如果出现流量丢弃情况，请尝试分配更多核心。

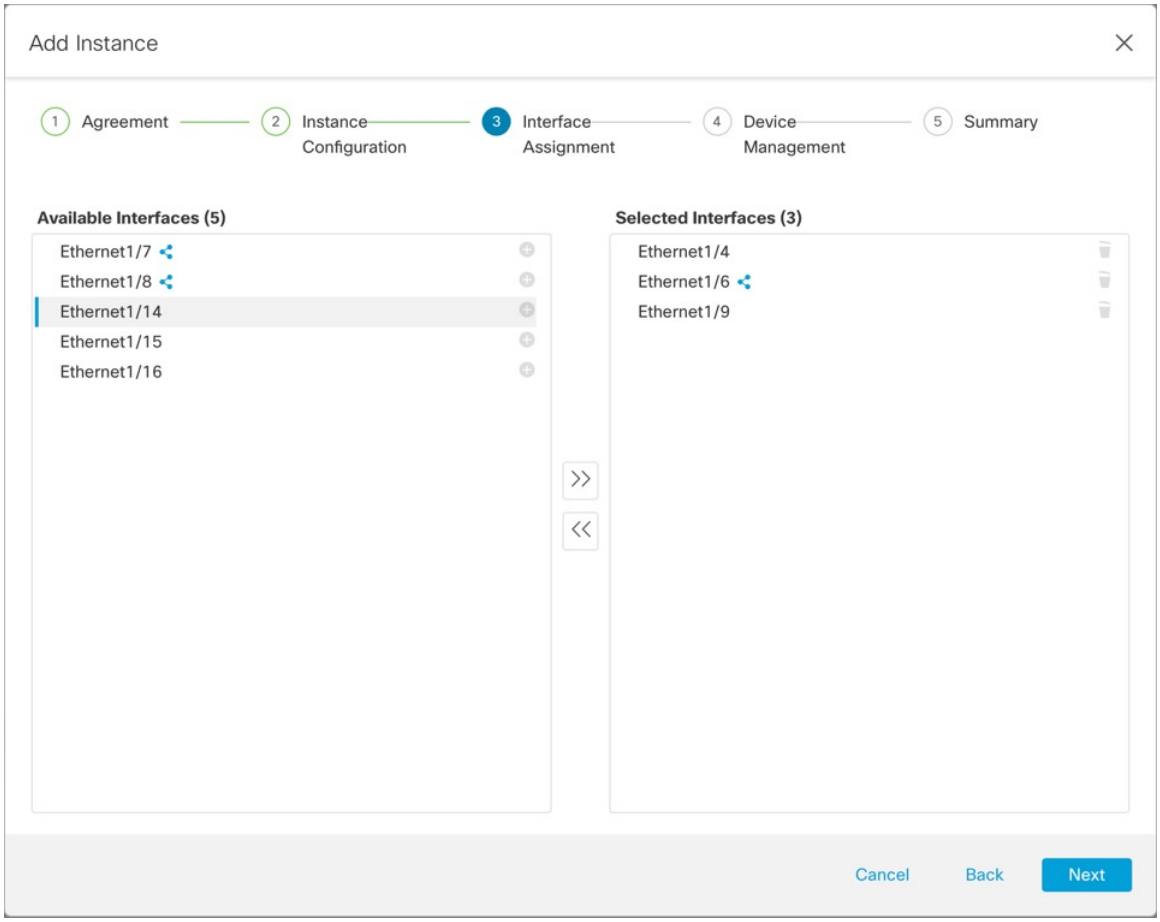
- 您可以分配偶数（6、8、10、12、14 等）个核心，乃至最大值。
- 最大可用核心数取决于型号，请参阅实例的要求和前提条件，第 14 页。

如果您稍后分配一个不同的资源配置文件，则实例将重新加载，这可能需要大约 5 分钟的时间。请注意，对于已建立的高可用性对，如果分配不同大小的资源配置文件，请务必尽快确保所有成员大小一致。

- **设备 SSH 密码** - 为 CLI 访问（SSH 或控制台）设置管理员用户密码。在 **确认密码** 字段中重复密码。

步骤 5 在 **接口分配**中，将机箱接口分配给实例，然后点击 **下一步**。

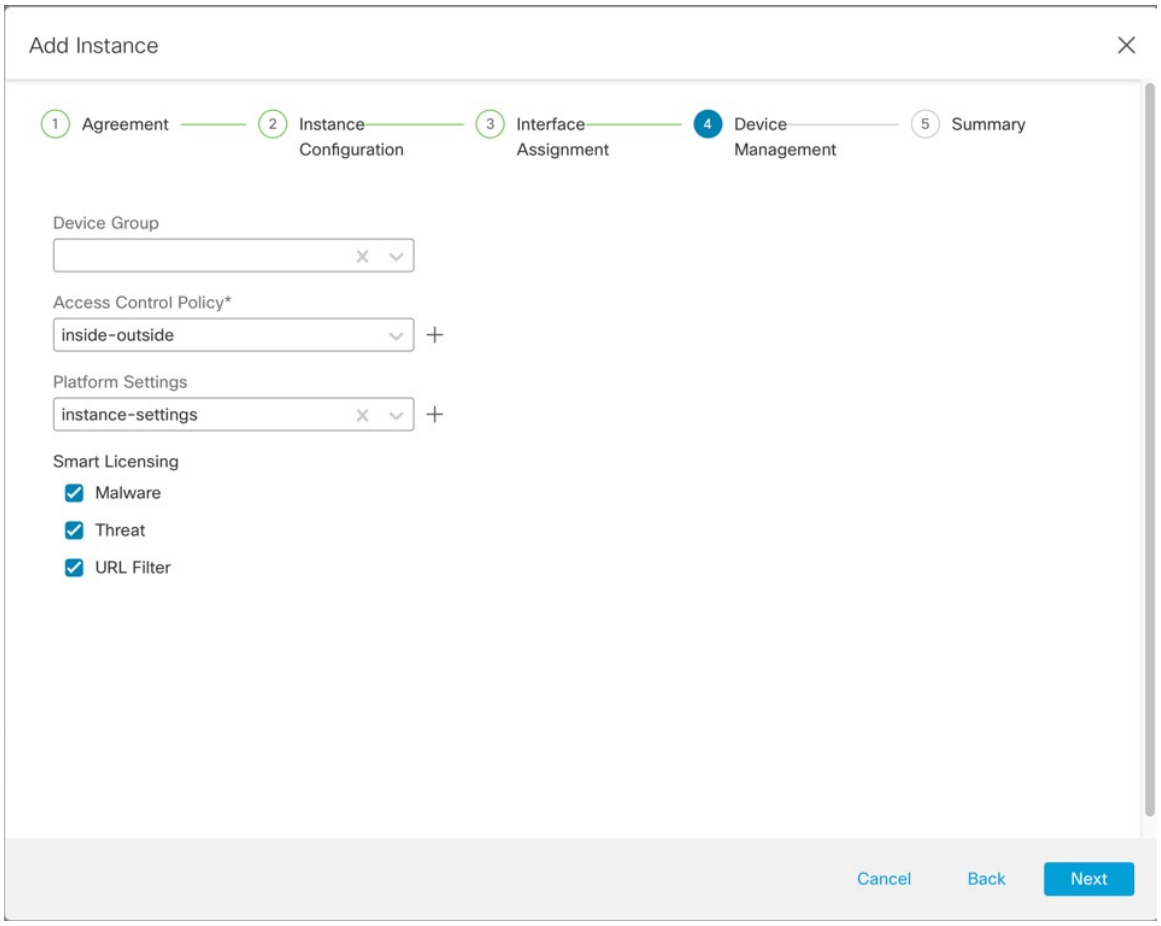
图 *35*: 接口分配



共享接口显示共享图标 ( )。

步骤 6 在 **设备管理**上，设置设备特定的设置，然后点击 **下一步**。

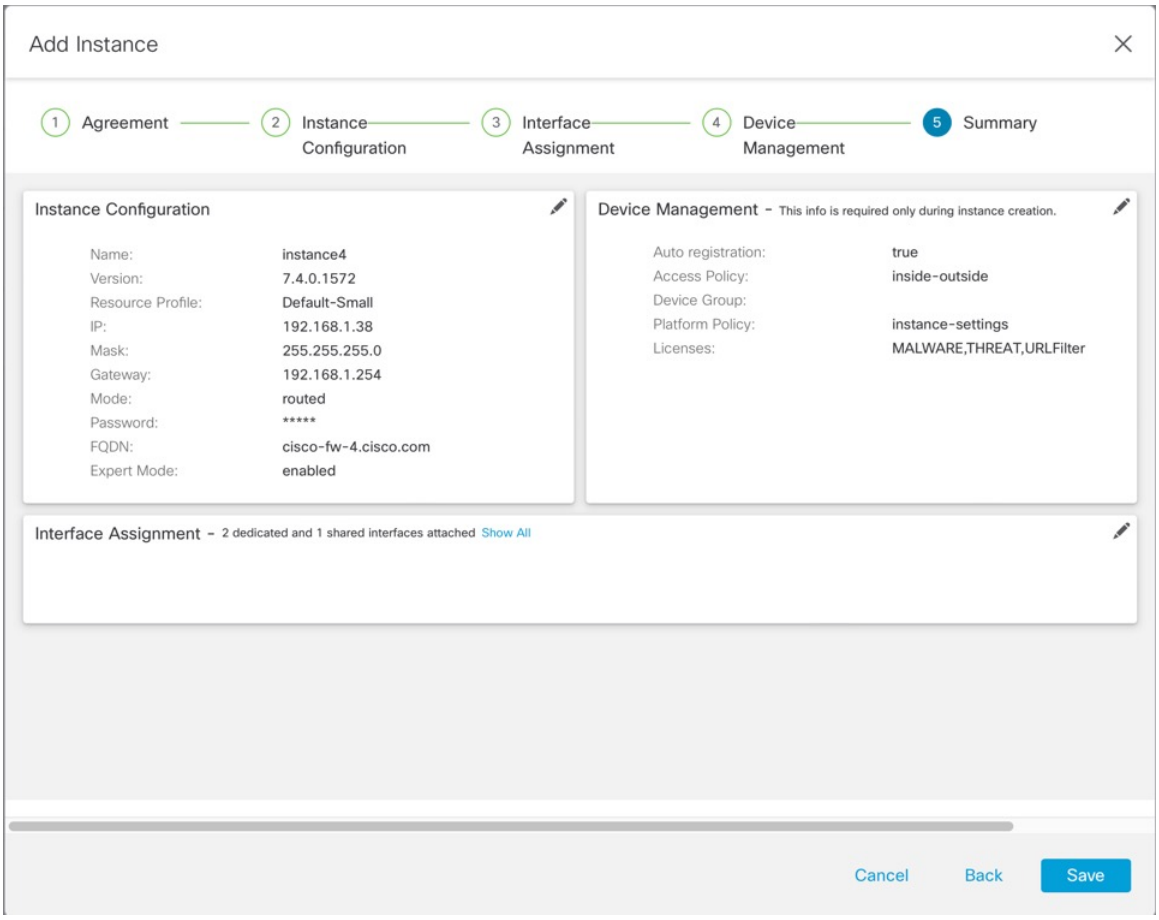
图 *36:* 设备管理



- **设备组**
- **访问控制策略**- 选择现有访问控制策略，或创建新策略。
- **平台设置**-选择现有平台设置策略或创建新策略。
- **智能许可**

步骤 7 在 **摘要**中，确认您的设置，然后点击 **保存**。

图 *37:* 摘要



您可以在保存实例之前编辑此屏幕上的任何设置。保存后，实例将添加到 **实例** 屏幕。

步骤 8 在 **实例** 屏幕上，点击 **保存**。

步骤 9 部署机箱配置。

部署后，该实例将在**设备管理**页面上添加为设备。

自定义系统配置

您可以配置机箱级别的设置，例如 SNMP。您还可以导入或导出机箱 FXOS 配置。

配置 SNMP

您可以通过在机箱系统配置中指定的其中一个实例的数据接口访问机箱级 MIB。您只能将此实例用于机箱 SNMP 信息。您无法通过机箱管理接口访问 SNMP。

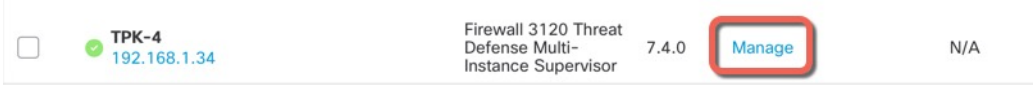
开始之前

为其中一个实例配置 SNMP。请参阅SNMP。

过程

步骤 1 在 **设备** > **设备管理** 中，点击**机箱**列中的**管理**或点击**编辑** (✎)。

图 *38:* 管理机箱

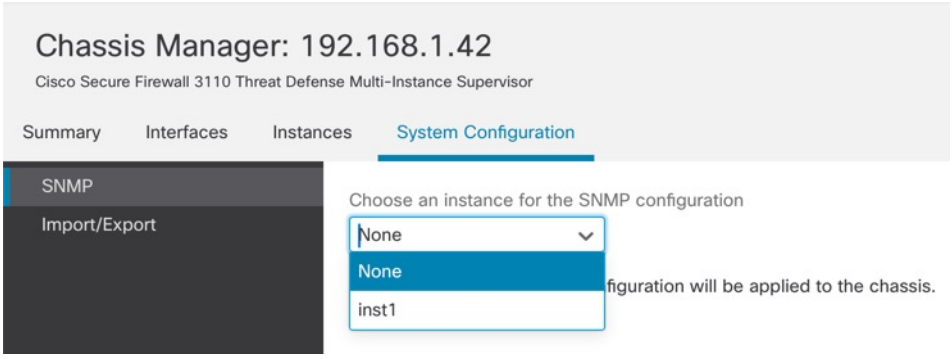


打开机箱的 **机箱管理器** 页面，进入 **摘要** 页面。

步骤 2 点击 **系统配置**。

步骤 3 选择 **SNMP**，然后从下拉列表中选择实例。

图 *39: SNMP*



可从所选实例访问机箱上的 SNMP。

步骤 4 点击**保存**。

步骤 5 部署机箱配置。

导入或导出机箱配置

使用配置导出功能将包含机箱配置设置的 XML 文件导出到本地计算机。之后，您便可以导入此配置文件，快速将配置设置应用于机箱，以返回到已知的正确配置，或从系统故障中恢复。只要满足前提条件，您还可以将机箱配置导入到新机箱（例如 RMA）。

导出时，仅导出机箱配置；不导出实例配置设置。需要使用设备备份/恢复功能单独备份实例。

导入时，机箱上的所有现有配置都将替换为导入文件中的配置。

开始之前

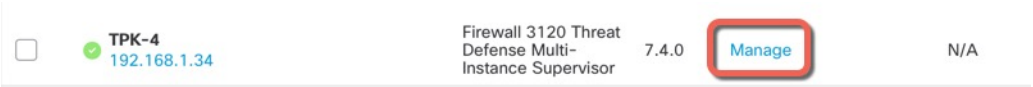
对于要导入配置的机箱，以下特征必须匹配：

- 相同的机箱软件版本
- 相同的 实例映像
- 相同的网络模块

过程

步骤 1 在 **设备** > **设备管理** 中，点击**机箱**列中的**管理**或点击**编辑** (✎)。

图 *40:* 管理机箱



打开机箱的 **机箱管理器** 页面，进入 **摘要** 页面。

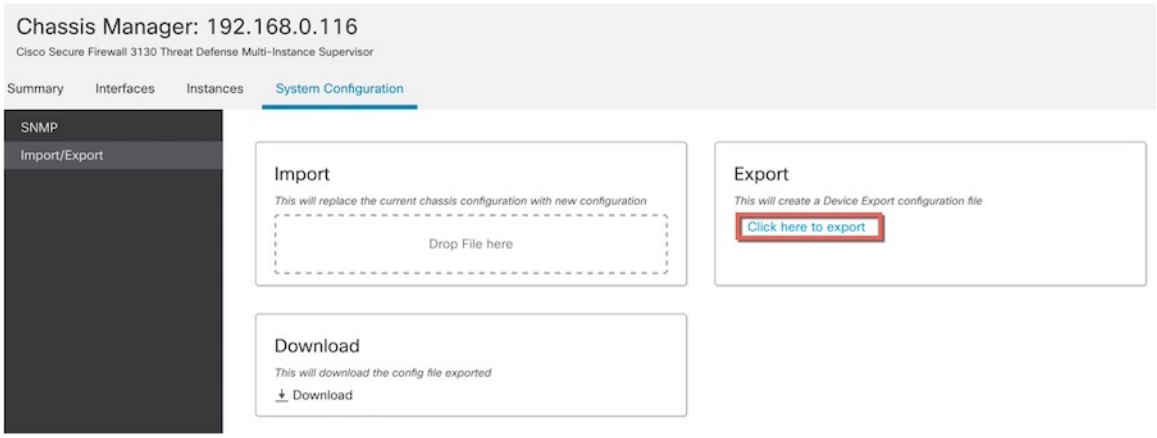
步骤 2 点击 **系统配置**。

步骤 3 点击 **导入/导出**。

步骤 4 要导出配置，请执行以下步骤。

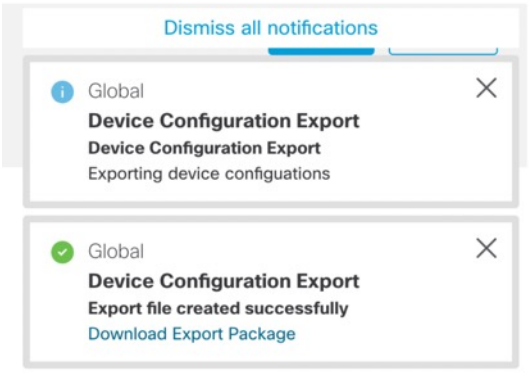
a) 在 **导出** 区域中，点击 **点击此处导出**。

图 *41:* 创建导出文件



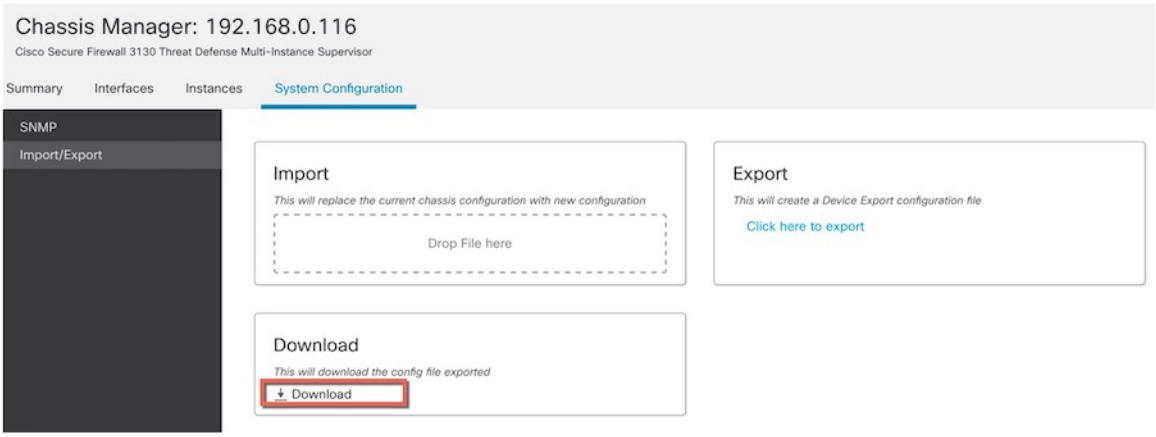
b) 监控 **导出文件创建成功** 消息的通知。

图 *42:* 创建的文件导出成功



c) 点击通知消息（**下载导出包**）或点击 **下载**，下载导出文件。

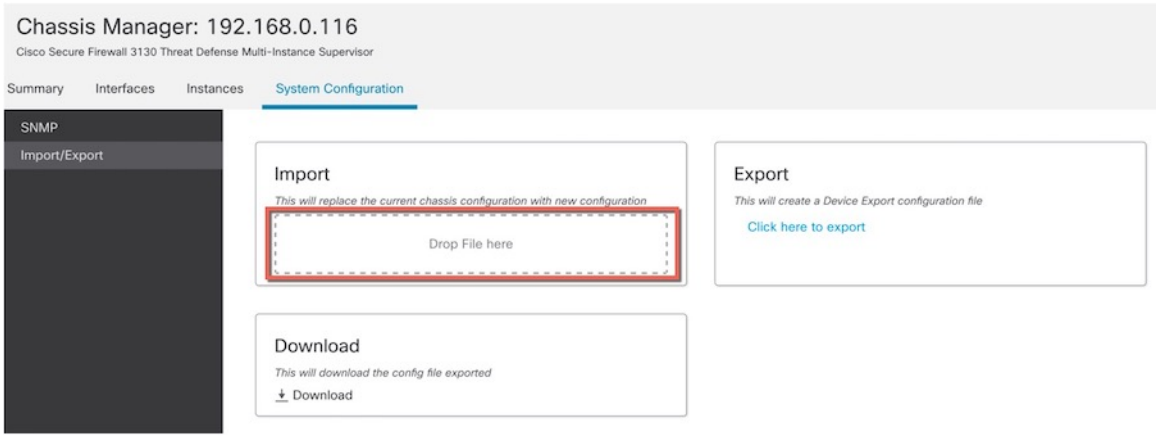
图 *43:* 下载



文件以 **.sfo** 扩展名保存。

步骤 5 要导入配置，请将 **.sfo** 文件拖动到**导入** > **放置文件**区域。

图 *44:* 导入



配置机箱平台设置

机箱平台设置可配置一系列用于管理机箱的功能。您可以在多个机箱之间共享策略。如果您希望每个机箱使用不同的设置，则必须创建多个策略。

创建机箱平台设置策略

使用 **平台设置** 页面（**设备** > **平台设置**）管理平台设置策略。此页面指示每个策略的设备类型。 **状态** 列显示策略的设备目标。

过程

步骤 1 选择**设备** > **平台设置**。

步骤 2 对于现有策略，您可以**复制** ()、**编辑** ()或**删除** ()策略。

注意
不应删除上一次部署于任何目标设备的策略，即使该策略已过时。在完全删除该策略之前，最好是将其他策略部署到这些目标。

步骤 3 要创建新策略，请点击**新建策略 (New Policy)**。

a) 从下拉列表中选择 **机箱平台设置** 。
b) 为新策略输入**名称 (Name)** 和**说明 (Description)**（可选）。
c) （可选）选择要应用策略的**可用机箱**，然后点击**添加 (Add)**（或拖放）以添加所选机箱。可以在**搜索** 字段中输入搜索字符串以缩小机箱列表。
d) 点击**保存**。

系统创建策略，并打开以进行编辑。

步骤 4 要更改策略的目标机箱，请点击要编辑的平台设置策略旁边的 **编辑** (✎) 图标。

a) 点击**策略分配 (Policy Assignment)**。
b) 要将机箱分配给策略，请在 **可用机箱** 列表中选择该机箱，然后点击 **添加**。还可以进行拖放。
c) 要删除机箱分配，请点击 **所选机箱** 列表中机箱旁边的 **删除** (🗑) 。
d) 点击**确定**。

配置 DNS

如果机箱要求将主机名解析为 IP 地址，则您需要指定 DNS 服务器。这些机箱 DNS 设置独立于每个实例的 DNS 设置，后者在设备平台设置中配置。

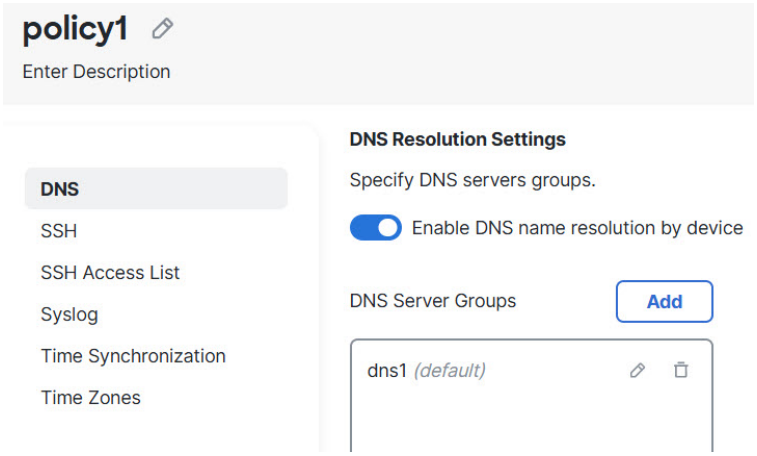
配置多个 DNS 服务器时，机箱仅以任意随机顺序使用服务器。您最多可以在四个 DNS 服务器组中配置四个服务器。例如，可以为单个服务器组配置四台服务器，也可以为四个服务器组配置每组一台服务器。

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑机箱策略。

步骤 2 选择 **DNS**。

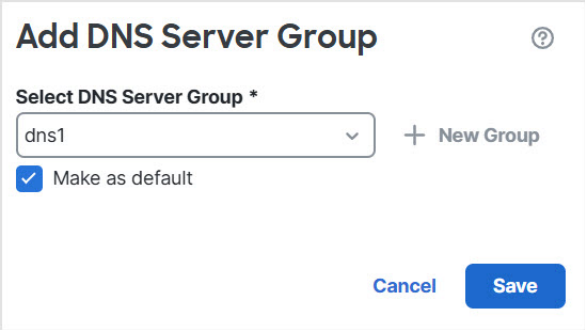
图 *45: DNS*



步骤 3 启用 **启用按设备 DNS 域名解析** 滑块。

步骤 4 点击 **添加** 以添加 DNS 服务器组。

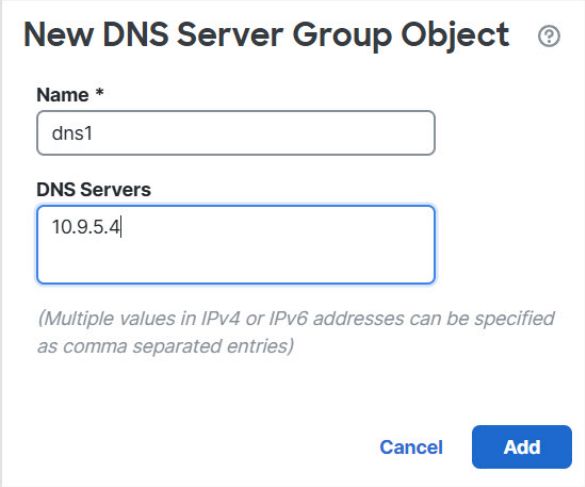
图 *46:* 添加 ***DNS*** 服务器组



步骤 5 选择现有的 DNS 服务器组（请参阅创建 DNS 服务器组对象），或点击 (+) **新建组 (New Group)**。

如果添加新组，您会看到以下对话框。以逗号分隔值提供名称和最多四个 DNS 服务器 IP 地址，然后点击 **添加**。

图 *47:* 新建 ***DNS*** 服务器组对象



步骤 6 点击 **保存**，将 DNS 服务器添加到列表中。

步骤 7 重复这些步骤添加其他服务器组。

确保在所有合并的组中最多只能识别四个 DNS 服务器。

步骤 8 点击**保存**以保存对策略的所有更改。

配置 SSH 和 SSH 访问列表

要在管理接口上允许从管理员用户到机箱的 SSH 会话，请启用 SSH 服务器并配置允许的网络。

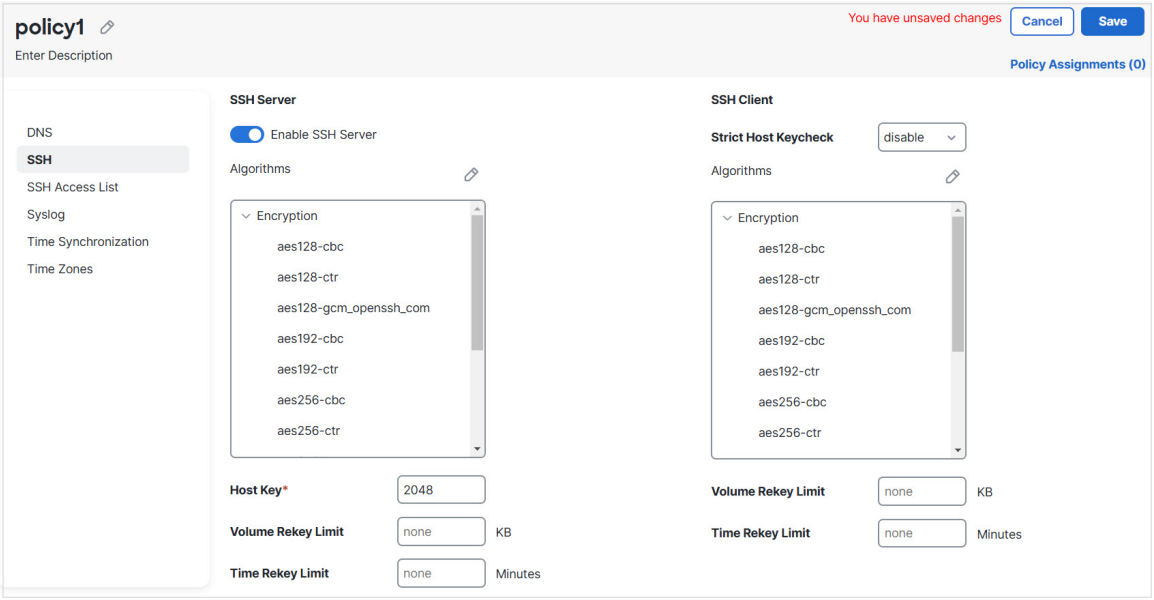
过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑机箱策略。

步骤 2 选择 **SSH**。

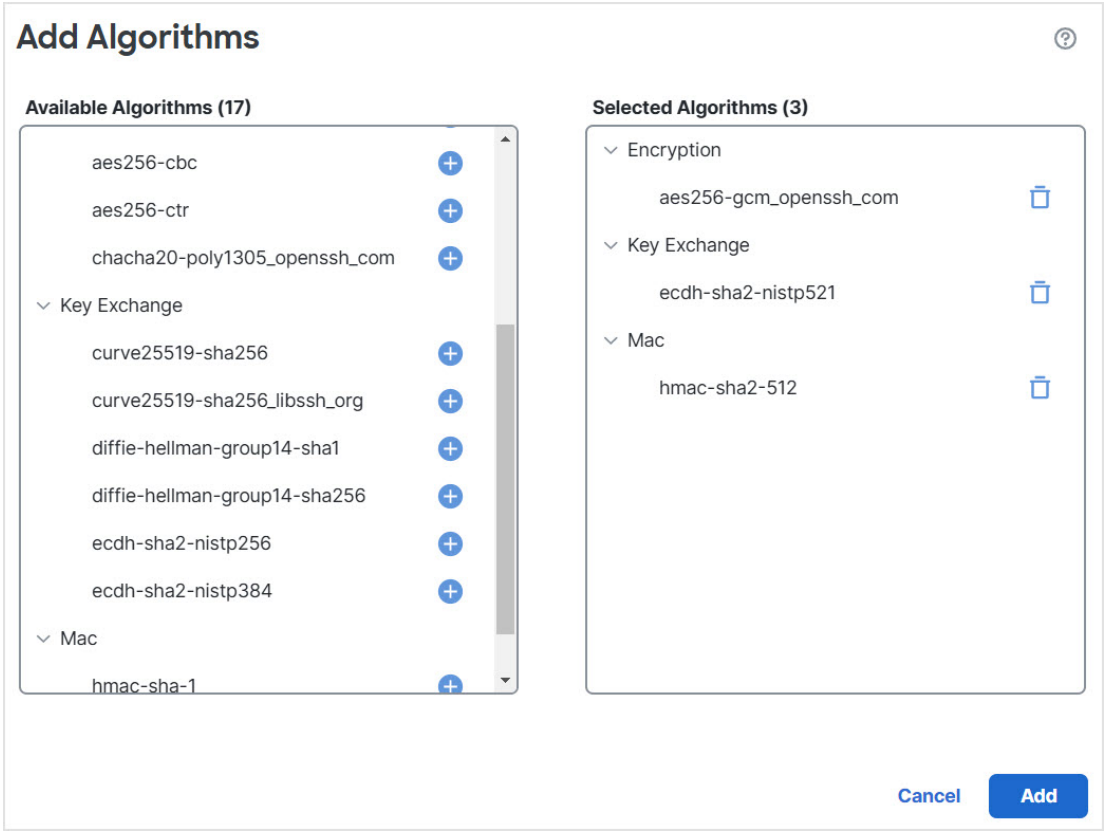
步骤 3 要启用到机箱的 SSH 访问，请选中 **启用 SSH (Enable SSH)** 滑块。

图 *48: SSH*



步骤 4 要设置允许的**算法**，请点击 **编辑** ()。

图 *49:* 添加算法



a) 选择**加密**算法：

b) 选择**密钥交换**算法。

密钥交换提供无法由任何一方单独确定的共享密钥。密钥交换与签名和主机密钥配合使用，以提供主机身份验证。此密钥交换方法提供显式服务器身份验证。

c) 选择 **Mac** 完整性算法。

步骤 5 对于**主机密钥**，请输入 RSA 密钥对的模块大小。

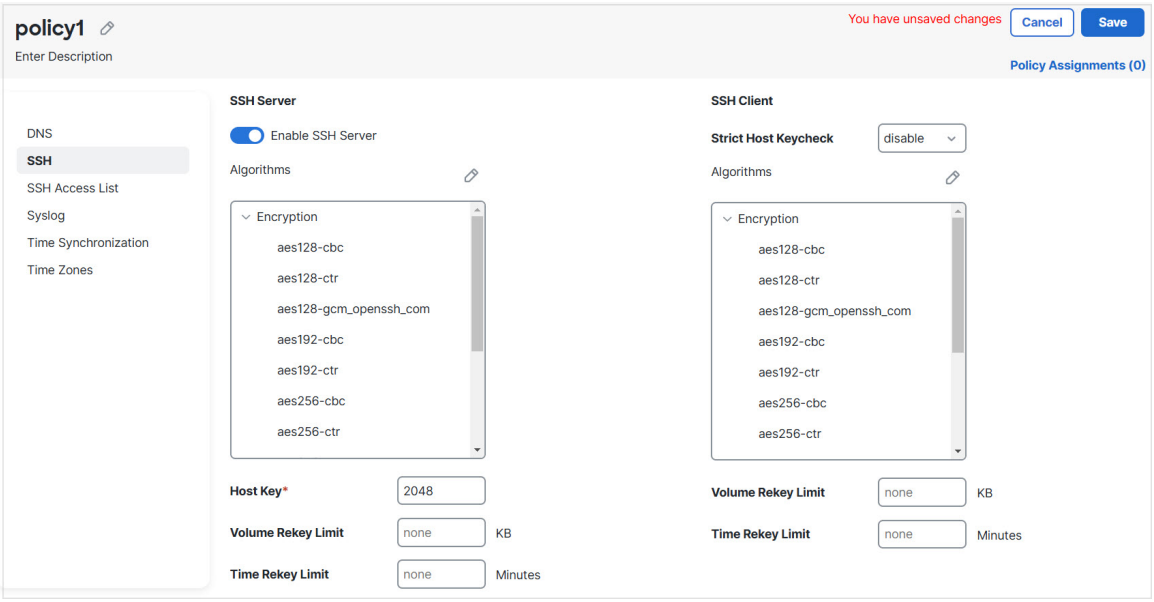
模数值（以位为单位）应为 8 的倍数，且介于 1024 到 2048 之间。指定的密钥模块大小越大，生成 RSA 密钥对所需的时间就越长。建议值为 2048。

步骤 6 对于服务器**密钥更新数量限制**，请设置 FXOS 断开会话连接之前连接上允许的流量（以 KB 为单位）。

步骤 7 对于服务器**密钥更新时间限制**，请设置 FXOS 断开会话连接之前允许的 SSH 会话空闲时间（以分钟为单位）。

步骤 8 对于 **SSH 客户端**，请配置以下设置。

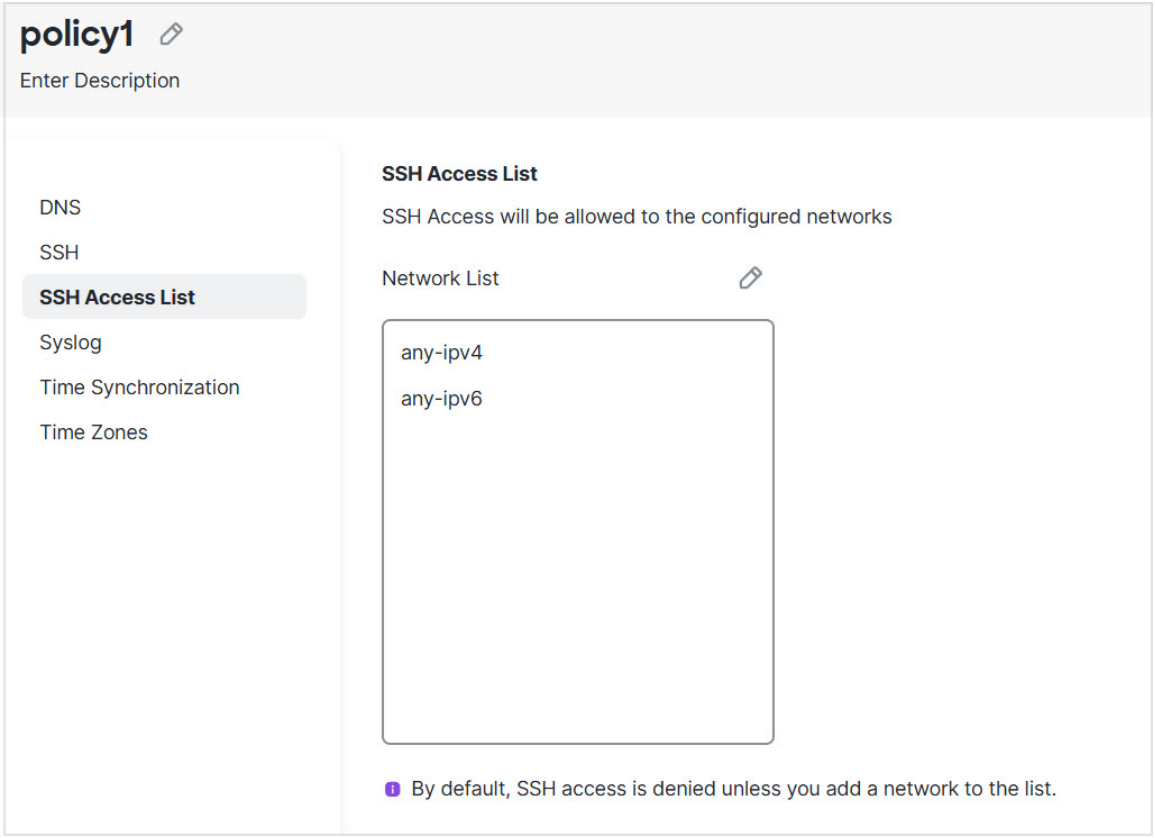
图 *50: SSH*



- **严格主机密钥检查 (Strict Host Keycheck)** - 选择**启用 (enable)**、**禁用 (disable)**或**提示 (prompt)**来控制 SSH 主机密钥检查。
  - **启用 (enable)** - 如果 FXOS 已知的主机文件中不包括主机密钥，连接将被拒绝。您必须在 FXOS CLI 中使用系统/服务范围的 **enter ssh-host** 命令手动添加主机。
  - **提示 (prompt)** - 对于机箱中未存储的主机密钥，系统会提示您接受或拒绝该主机密钥。
  - **禁用 (disable)** -（默认）机箱将自动接受以前未存储的主机密钥。
- **算法 (Algorithms)** - 点击 **编辑** ()，然后选择**加密 (Encryption)**、**密钥交换 (Key Exchange)** 和 **Mac** 算法。
- **密钥更新数量限制 (Volume Rekey Limit)** - 请设置 FXOS 断开会话连接之前连接上允许的流量（以 KB 为单位）。
- **密钥更新时间限制 (Time Rekey Limit)** - 请设置 FXOS 断开会话连接之前允许的 SSH 会话空闲时间（以分钟为单位）。

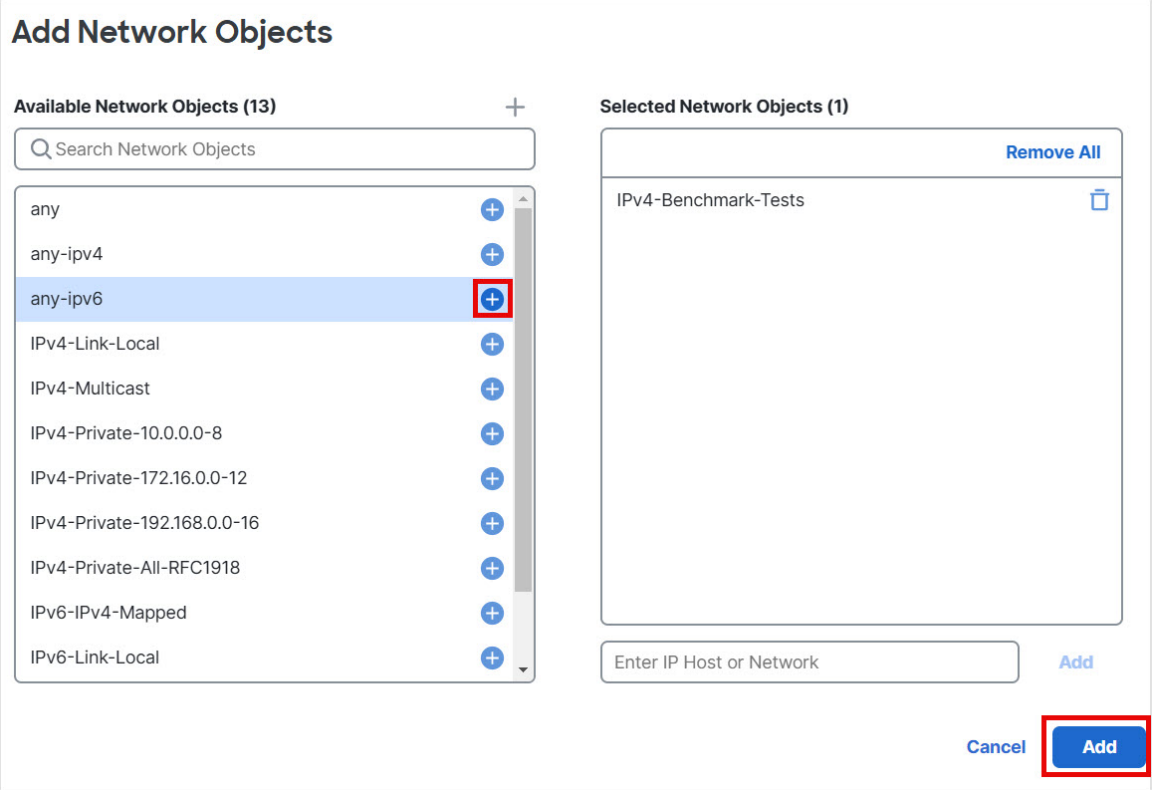
步骤 9 选择 **SSH 访问列表 (SSH Access List)**。您需要先允许访问 IP 地址或网络，然后才能使用 SSH。

图 *51: SSH* 访问列表



步骤 10 点击 **编辑** (✎) 添加网络对象，然后点击**保存**。您也可以手动输入 IP 地址。

图 *52:* 网络对象



步骤 11 点击**保存**以保存对策略的所有更改。

配置系统日志

您可以从机箱启用系统日志。这些系统日志来自机箱的 FXOS 操作系统。

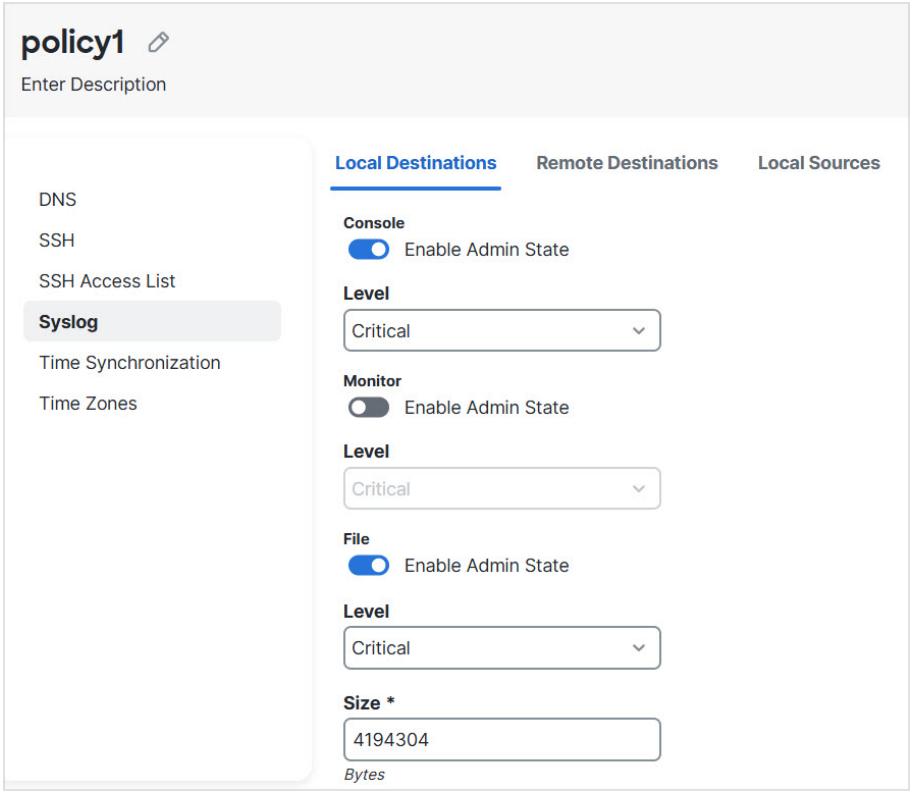
过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑机箱策略。

步骤 2 选择 **系统日志**。

步骤 3 在 **本地目的** 选项卡上，填写以下字段。

图 *53:* 系统日志本地目标

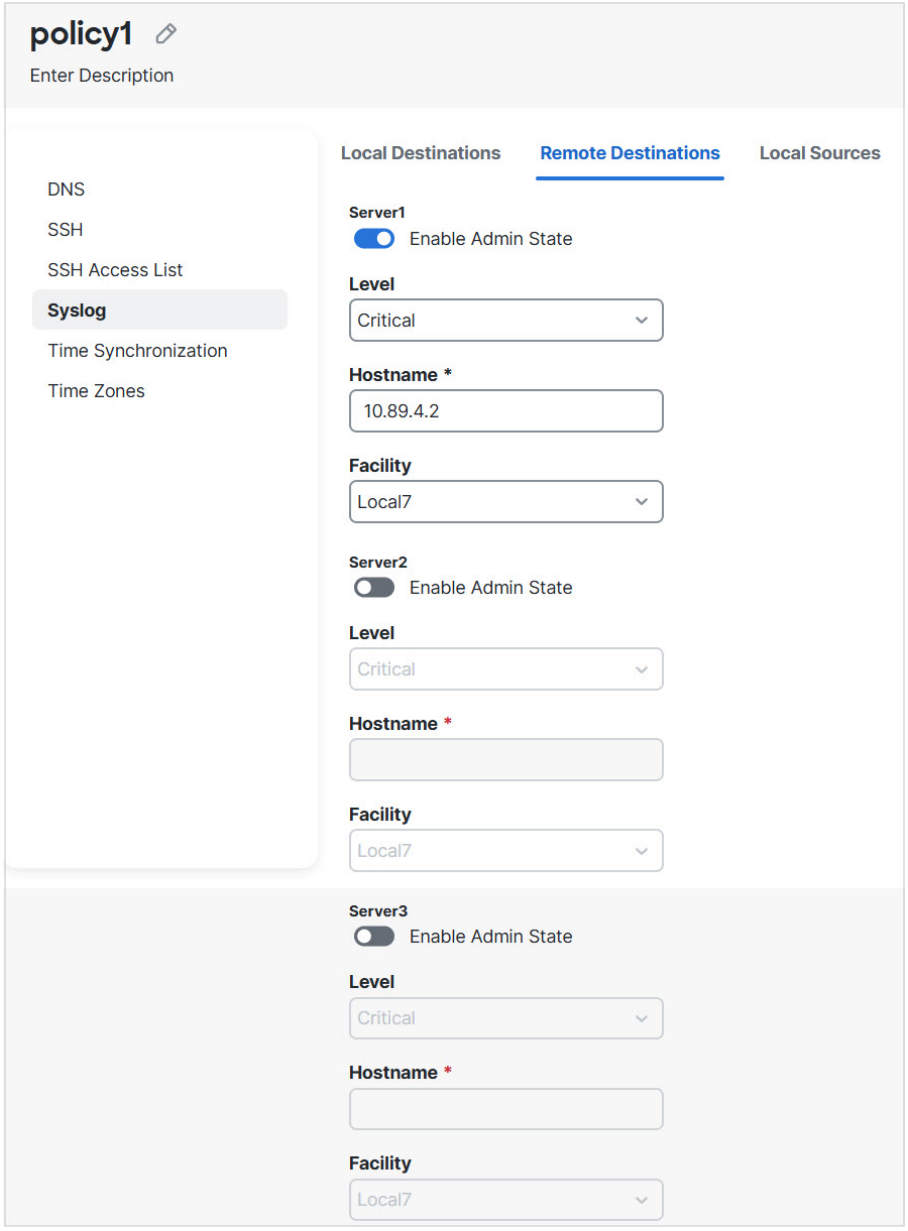


名称	说明
控制台 (Console) 部分	
管理状态 (Admin State) 字段	机箱是否在控制台上显示系统日志消息。 如果您想在控制台上显示系统日志消息并将这些日志消息添加到日志中，请选中**启用 (Enable)** 复选框。如果取消选中**启用 (Enable)** 复选框，系统日志消息将会添加到日志中，但不会显示在控制台上。
级别 (Level) 字段	如果选中了**控制台 - 管理状态 (Console - Admin State)** 的**启用 (Enable)** 复选框，请选择您想在控制台上显示的最低消息级别。机箱在控制台上显示此级别及以上消息。这可以是以下其中一项： • **紧急** • **提醒** • **严重**
监视器 (Monitor) 部分	

名称	说明
管理状态 (Admin State) 字段	机箱是否在监视器上显示系统日志消息。 如果您想在监视器上显示系统日志消息并将这些日志消息添加到日志中，请选中**启用 (Enable)** 复选框。如果取消选中**启用 (Enable)** 复选框，系统日志消息将会添加到日志中，但不会显示在监视器上。
级别 (Level) 下拉列表	如果选中了**监视器 - 管理状态 (Monitor - Admin State)** 的**启用 (Enable)** 复选框，请选择您想在监视器上显示的最低消息级别。系统在监视器上显示此级别及以上消息。这可以是以下其中一项： • **紧急** • **提醒** • **严重** • **错误** • **警告** • **通知** • **信息** • **调试**

步骤 4 在**远程目的 (Remote Destinations)** 选项卡上，为最多三个外部日志填写下列字段，这些日志可以存储机箱生成的消息：

图 *54:* 系统日志远程目的



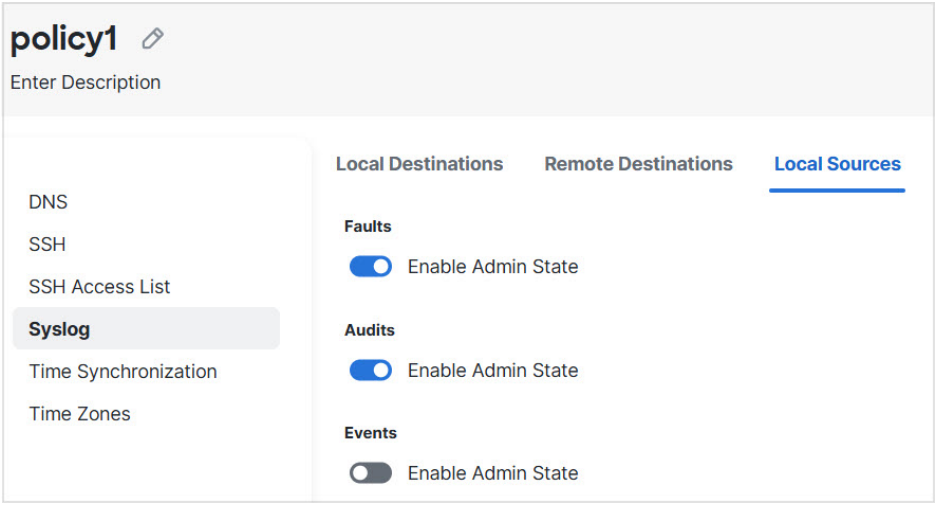
通过将系统日志消息发送到远程目的，您可以根据外部系统日志服务器上的可用磁盘空间存档消息，并在保存日志记录数据后对其进行处理。例如，可以指定在记录特定类型的系统日志消息后要执行的操作，从日志提取数据并将记录保存到其他文件以进行报告，或者使用特定于站点的脚本跟踪统计信息。

名称	说明
管理状态 (Admin State) 字段	如果您想在远程日志文件中存储系统日志消息，请选中**启用 (Enable)** 复选框。

名称	说明
级别 (Level) 下拉列表	选择您想让系统存储的最低消息级别。系统在远程文件中存储此级别及以上消息。这可以是以下其中一项： • 紧急 • 提醒 • 严重 • 错误 • 警告 • 通知 • 信息 • 调试
主机名/IP 地址 (Hostname/IP Address) 字段	远程日志文件所驻留的主机名或 IP 地址。 注释 如果使用主机名而不使用 IP 地址，必须配置 DNS 服务器。
设备 (Facility) 下拉列表	为系统日志服务器选择要用作文件消息基础的系统日志设备。这可以是以下其中一项： • **Local0** • **Local1** • **Local2** • **Local3** • **Local4** • **Local5** • **Local6** • **Local7**

步骤 5 在 **本地源** 选项卡上，填写以下字段。

图 *55:* 系统日志本地源



名称	说明
故障 > 启用管理状态	启用系统故障日志记录。
审核 > 启用管理状态	启用审核日志。
事件 > 启用管理状态	启用系统事件日志记录。

步骤 6 点击**保存**以保存对策略的所有更改。

配置时间同步

NTP 用于实施分层服务器系统，可在网络系统中提供精确的同步时间。时间敏感性操作需要这种精确度，例如验证 CRL，其包括精确时间戳。您最多可以配置 4 个 NTP 服务器。

注释

- FXOS 使用 NTP 版本 3。
- 如果外部NTP服务器的层值为13或更大，则应用实例无法同步到FXOS机箱上的NTP服务器。每次 NTP 客户端同步到 NTP 服务器时，层值就会增加 1。

  如果您已设置自己的 NTP 服务器，则可以在服务器上的 /etc/ntp.conf 文件中找到它的层值。如果 NTP 服务器的层值大于或等于 13，则可以更改 ntp.conf 文件中的层值并重新启动服务器，或者使用其他 NTP 服务器（例如：pool.ntp.org）。

开始之前

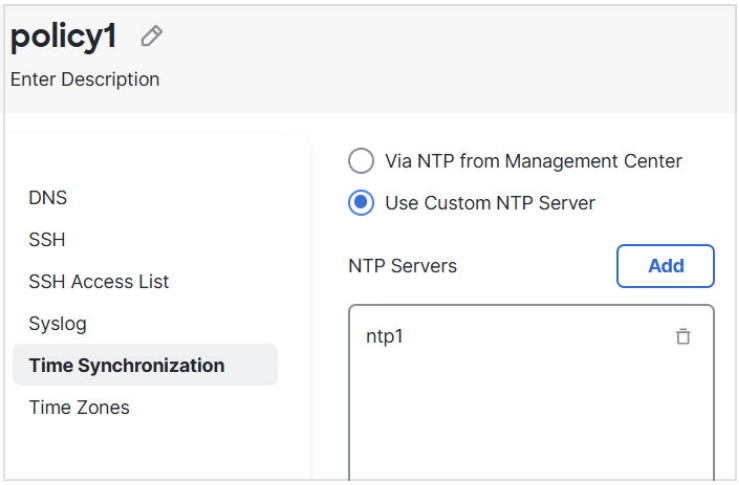
如果您要将主机名用于 NTP 服务器，则必须配置 DNS 服务器。请参阅 配置 DNS，第 41 页。

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑机箱策略。

步骤 2 选择 **时间同步**。

图 *56:* 时间同步



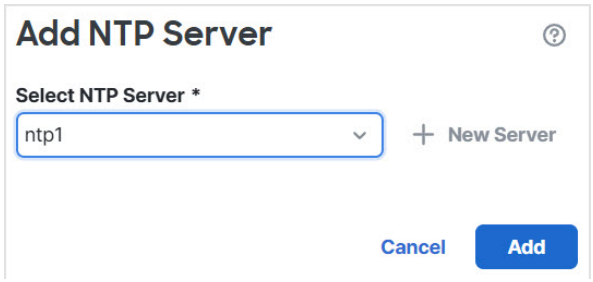
步骤 3 如果要从 防火墙管理中心获取时间，请 **从管理中心点击通过 NTP**。

此选项可确保机箱和 防火墙管理中心 具有相同的时间。

步骤 4 要使用外部 NTP 服务器，请点击 **使用自定义 NTP 服务器**。

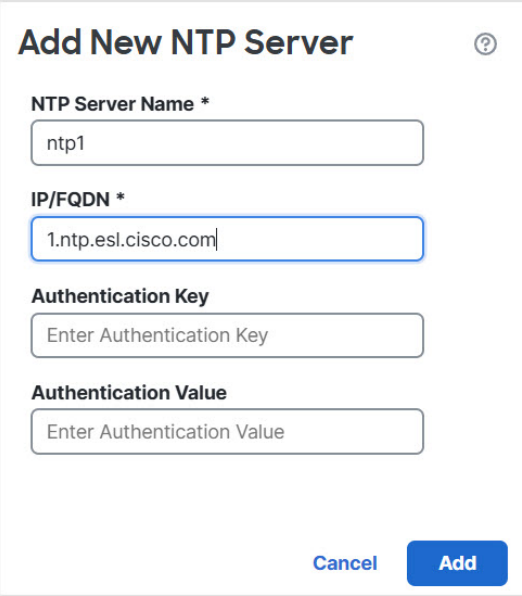
a) 点击 **添加** 来添加服务器。

图 *57:* 添加 *NTP* 服务器



b) 从下拉菜单中选择任何已定义的服务器，然后点击 **添加**，或点击 **新建服务器** 以添加新服务器。

图 *58:* 添加新的 *NTP* 服务器



c) 对于新服务器，请输入以下字段，然后点击 **添加**。

- **NTP 服务器名称**- 用于标识此服务器的名称。
- **IP/FQDN**- 服务器的 IP 地址或主机名。
- **验证密钥**和**验证值** - 从 NTP 服务器获取密钥 ID 和值。例如，要在安装了 OpenSSL 的 NTP 服务器 4.2.8p8 版或更高版本上生成 SHA1 密钥，请输入 **ntp-keygen -M** 命令，然后在 ntp.keys 文件中查看密钥 ID 和值。密钥用于告知客户端和服务器在计算消息摘要时要使用哪个值。

  仅支持使用 SHA1 进行 NTP 服务器身份验证。

步骤 5 点击**保存**以保存对策略的所有更改。

配置时区

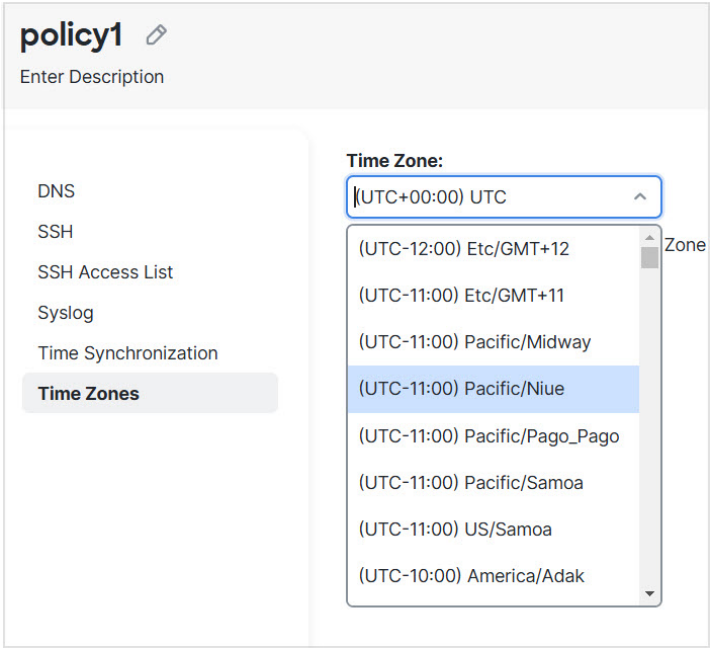
设置机箱的时区。

过程

步骤 1 选择 **设备** > **平台设置** 并创建或编辑机箱策略。

步骤 2 选择 **时区**。

图 *59:* 时区



步骤 3 从下拉菜单中选择 **时区** 。

步骤 4 点击**保存**以保存对策略的所有更改。

管理多实例模式

本节介绍不太常见的任务，包括在 FXOS CLI 中更改设置或更改分配给机箱的接口。

在 CLI 启用多实例模式

如果要在将设备添加到防火墙管理中心之前将其预配置为多实例模式，则可以执行此程序。要使用防火墙管理中心 来转换为多实例模式，请参阅 将设备转换为多实例模式 ，第 18 页。

您需要在控制台端口连接到 CLI，以启用多实例模式。配置模式后，可以将其添加到 防火墙管理中心。

注释 虽然您可以在管理端口上连接到 SSH，但我们建议使用控制台端口来避免多次断开连接。此程序涉及控制台端口。

过程

步骤 1 连接到机箱控制台端口。

控制台端口连接到 FXOS CLI。

步骤 2 使用用户名 **admin** 和密码 **Admin123** 登录。

第一次登录FXOS时，系统会提示您更改密码。

注释
如果密码已更改，但您不知道，则必须重新映像设备以将密码重置为默认值。有关重新映像程序的信息，请参阅 FXOS 故障排除指南。

示例：

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

步骤 3 检查您当前的模式：本地模式或容器模式。如果模式为本地模式，您可以继续执行此程序以转换为多实例（容器）模式。

show system detail

示例：

```
firepower # show system detail

Systems:
    Name: firepower
    Mode: Stand Alone
    System IP Address: 172.16.0.50
    System IPv6 Address: ::
    System Owner:
    System Site:
    Deploy Mode: Native
    Description for System:
firepower #
```

步骤 4 连接到 CLI。

connect ftd

示例：

```
firepower# connect ftd
>
```

步骤 5 首次登录 时，系统会提示您接受一般条款。然后，系统将显示 CLI 设置脚本。

设置脚本允许您设置管理接口 IP 地址和其他设置。但是，当您转换为多实例模式时，仅保留以下设置。

- 管理员密码（您在初始登录时设置）
- DNS 服务器
- 搜索域

您将在多实例模式命令中重置管理 IP 地址和网关。转换为多实例模式后，您可以在 FXOS CLI 中更改管理设置。请参阅 在 FXOS CLI 中更改机箱管理设置，第 60 页。

步骤 6 启用多实例模式，设置机箱管理接口设置，并识别 防火墙管理中心。您可以使用 IPv4 和/或 IPv6 静态寻址；不支持 DHCP。输入命令后，系统将提示您清除配置并重新启动。输入 **ERASE**（全部大写）。系统将重新启动，并在更改模式时清除配置，但您在 命令中设置的管理网络设置和管理员密码除外。机箱主机名设置为“firepower-*model*”。

IPv4：

configure multi-instance network ipv4 *ip_address network_mask gateway_ip_address* **manager** *manager_name* {*hostname* | *ipv4_address* | **DONTRESOLVE**} *registration_key nat_id*

IPv6：

configure multi-instance network ipv6 *ipv6_address prefix_length gateway_ip_address* **manager** *manager_name* {*hostname* | *ipv6_address* | **DONTRESOLVE**} *registration_key nat_id*

请参阅以下 **manager** 组件：

- {*hostname* | *ipv4_address* | **DONTRESOLVE**}—Specifies either the FQDN or IP address of the 防火墙管理中心. 必须至少有一个设备（防火墙管理中心 或机箱）具有可访问的 IP 地址，才能在两个设备之间建立双向 SSL 加密的通信信道。如果未在此命令中指定管理器主机名或 IP 地址，然后输入 **DONTRESOLVE**；这种情况下，机箱必须具有可访问的 IP 地址或主机名，并且必须指定 *nat-id*。
- *registration_key*-输入您选择的一次性注册密钥，注册时也要在 防火墙管理中心 上指定它。注册密钥不得超过 37 个字符。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。
- *nat_id*-指定您选择的唯一的一次性字符串，注册机箱时若一方没有指定可访问的 IP 地址或主机名，则也要在 防火墙管理中心 上指定它。如果您不指定管理器地址或主机名，则必须设置，但我们建议您始终设置 NAT ID，即使您指定了主机名或 IP 地址。NAT ID 不得超过 37 个字符。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。此 ID 不能用于将任何其他设备注册到 防火墙管理中心。

要将模式更改回设备模式，必须使用 FXOS CLI 并输入 **scope system** 及 **set deploymode native**。请参阅在 FXOS CLI 中更改机箱管理设置，第 60 页。

示例：

```
> configure multi-instance network ipv4 172.16.0.104 255.255.255.0 172.16.0.1 manager
fmc1 172.16.0.103 impala67 winchester1
WARNING: This command will discard any FTD configuration (except admin's credentials).
```

```
Make sure you backup your content. All previous content will be lost. System is going to
be re-initialized.
Type ERASE to confirm:ERASE
Exit...
>
```

步骤 7 将机箱添加到 防火墙管理中心。请参阅添加机箱。

更改分配给实例的接口

您可以在实例上分配或取消分配接口。添加新接口或删除未使用接口对实例配置的影响最小。您也可以编辑已分配的 EtherChannel 的成员，而不影响实例。但是，删除安全策略中使用的接口会影响配置。

可以直接在实例配置中的很多位置引用接口，包括访问规则、NAT、SSL、身份规则、VPN、DHCP 服务器等。删除接口将删除与该接口相关的任何配置。

引用安全区域的策略不受影响。

注释 为实现高可用性，您需要对另一台设备进行相同的接口更改。否则，高可用性可能无法正常运行。

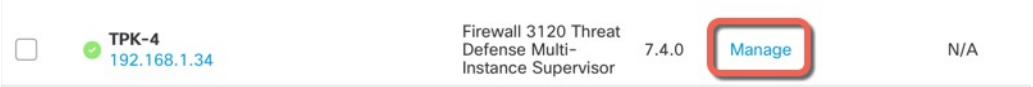
开始之前

- 根据 配置实例， 第 18 页配置接口。
- 如果您要将已分配的接口添加到 EtherChannel，则需要先从实例取消分配接口，然后再将该接口添加到 EtherChannel。对于新的 EtherChannel，您可以随后将 EtherChannel 分配到实例。

过程

步骤 1 在 **设备** > **设备管理** 中，点击**机箱**列中的**管理**或点击**编辑** ()。

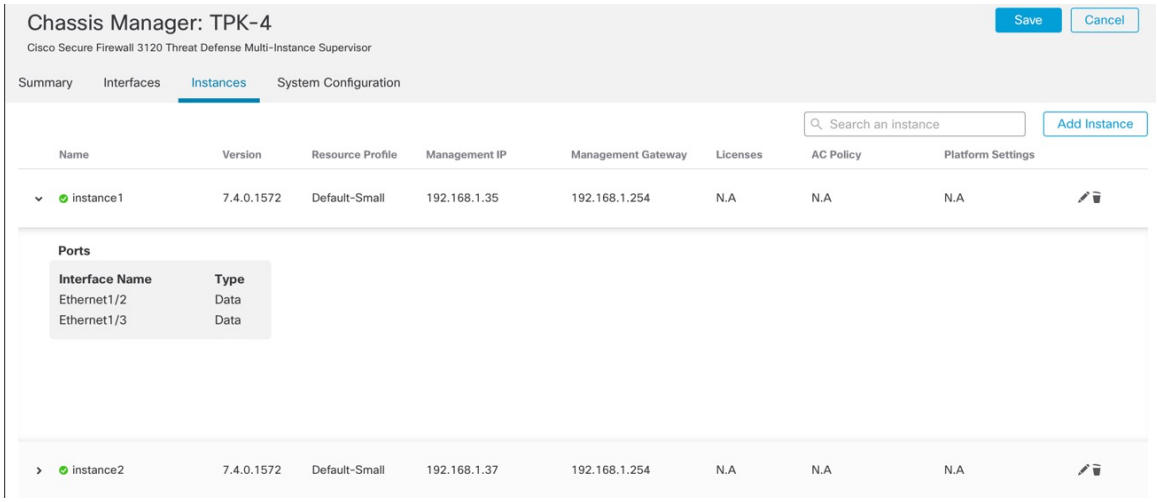
图 *60:* 管理机箱



打开机箱的 **机箱管理器** 页面，进入 **摘要** 页面。

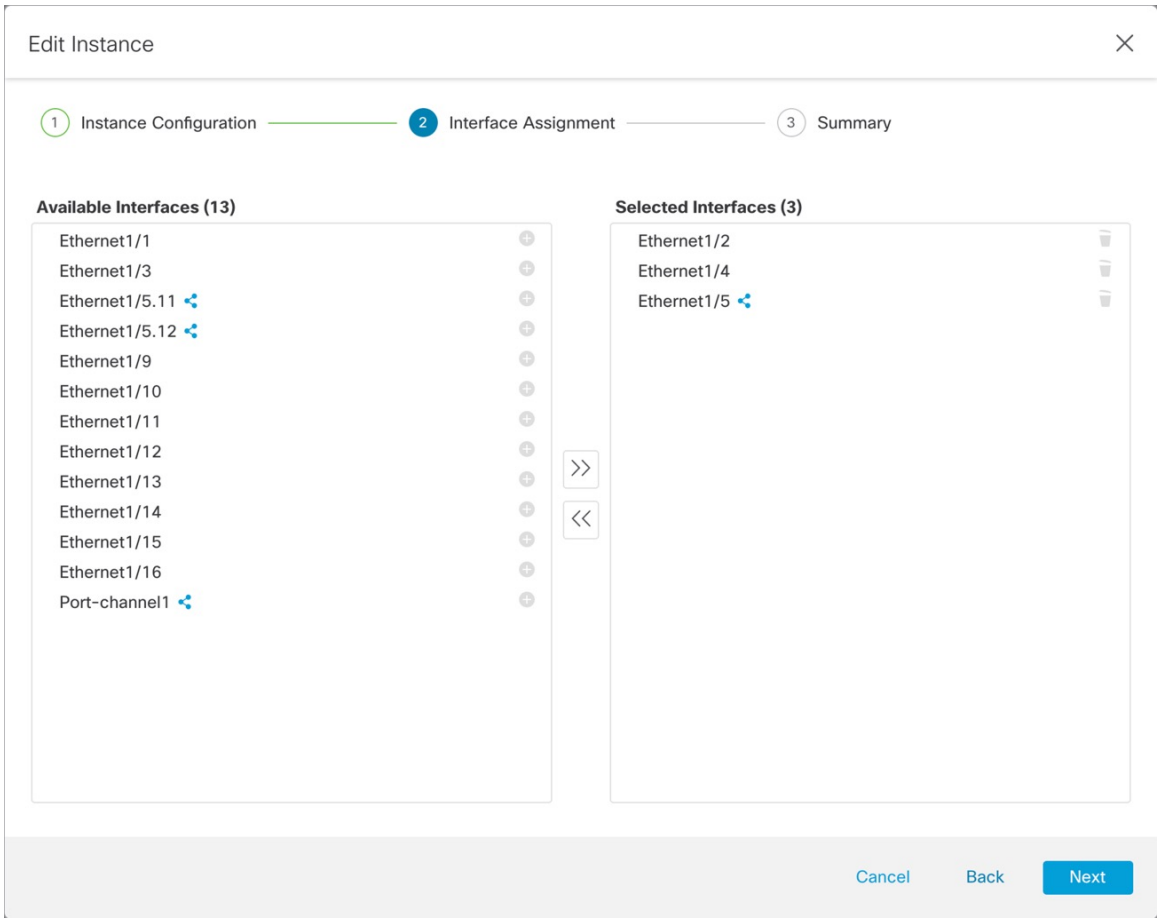
步骤 2 点击 **实例**，然后点击要为其更改接口的实例旁边的 **编辑** () 。

图 *61:* 实例



步骤 3 点击 **下一步**，直到进入 **接口分配** 屏幕。

图 *62:* 接口分配



共享接口显示共享图标 ( )。

步骤 4 更改接口，然后点击 **下一步**。

步骤 5 点击 **摘要** 屏幕上的 **保存**。

步骤 6 为实现高可用性，您需要对另一台设备进行相同的接口更改。否则，高可用性可能无法正常运行。

在 FXOS CLI 中更改机箱管理设置

如果要更改机箱管理接口 IP 地址和网关，将 防火墙管理中心 更改为新的管理器、更改管理员密码或禁用多实例模式，可以从 FXOS CLI 执行此操作。

过程

步骤 1 连接到机箱控制台端口。

控制台端口连接到 FXOS CLI。

注释
我们建议使用控制台端口。您还可以使用SSH连接到管理接口（如果在防火墙管理中心中的机箱平台设置中进行了配置）；但是，如果更改管理 IP 地址，则会断开连接。

步骤 2 使用用户名 **admin** 和初始设置期间设定的密码登录。

步骤 3 更改管理 IP 地址。您可以使用静态 IPv4 和/或 IPv6 地址。

IPv4：

scope fabric-interconnect

set out-of-band static ip *ip_address* **netmask** *network_mask* **gw** *gateway_ip_address*

IPv6：

scope fabric-interconnect

scope ipv6-config

set out-of-band static ipv6 *ipv6_address* **ipv6-prefix** *prefix_length* **ipv6-gw** *gateway_address*

示例：

IPv4：

```
firepower-3110# scope fabric-interconnect
firepower-3110 /fabric-interconnect # set out-of-band static ip 10.5.23.8 netmask
255.255.255.0
gw 10.5.23.1
```

IPv6：

```
firepower-3110# scope fabric-interconnect
firepower-3110 / fabric-interconnect # scope ipv6-config
firepower-3110 / fabric-interconnect /ipv6-config # set out-of-band static ipv6 2001:DB8::34
ipv6-prefix 64 ipv6-gw 2001:DB8::1
```

步骤 4 更改 防火墙管理中心。

您应先从当前 防火墙管理中心取消注册机箱。

enter device-manager *manager_name* [**hostname** {*hostname* | *ipv4_address* | *ipv6_address*}] [**nat-id** *nat_id*]

系统将提示您输入注册密钥。

您可以从任何范围输入此命令。

- **hostname** {*hostname* | *ipv4_address* | *ipv6_address*}—Specifies either the FQDN or IP address of the 防火墙管理中心。必须至少有一个设备（防火墙管理中心或机箱）具有可访问的IP地址，才能在两个设备之间建立双向 TLS-1.3 加密的通信通道。如果未在此命令中指定 **hostname**，则机箱必须具有可访问的 IP 地址或主机名，并且必须指定 **nat-id**。
- **nat-id** *nat_id*- 指定您选择的唯一的一次性字符串，注册机箱时若一方没有指定可访问的 IP 地址或主机名，则也要在 防火墙管理中心 机箱上指定它。如果您不指定 **hostname**，则必须设置，但我们建议您始终设置 NAT ID，即使您指定了主机名或 IP 地址。NAT ID 不得超过 37 个字符。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。此 ID 不能用于将任何其他设备注册到 防火墙管理中心。
- **Registration Key:** *reg_key*- 系统将提示您输入选择的一次性注册密钥，注册机箱时也要在 防火墙管理中心 上指定它。注册密钥不得超过 37 个字符。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。

示例：

```
firepower-3110# enter device-manager boulder_fmc hostname 10.89.5.35 nat-id 93002
(Valid registration key characters: [a-z],[A-Z],[0-9],[-]. Length: [2-36])
Registration Key: Impala67
```

步骤 5 更改 admin 密码。

scope security

set password

输入密码：*password*

确认密码：*password*

示例：

```
firepower-3110# scope security
firepower-3110 /security # set password
Enter new password: Sw@nsong67
Confirm new password: Sw@nsong67
firepower-3110 /security #
```

步骤 6 禁用多实例模式并将系统设置回设备模式。

scope system

set deploymode native

系统会提示您重新启动 。

示例：

```
firepower-3110# scope system
firepower-3110 /system # set deploymode native
All configuration and bootable images will be lost and system will reboot.
If there was out of band upgrade, it might reboot with the base version and
need to re-image to get the expected running version.
Do you still want to change deploy mode? (yes/no):yes
firepower-3110 /system #
```

要将模式更改回多实例模式，请输入 **set deploymode container**。您可以使用 **show system detail** 命令来检测当前模式。

监控多实例模式

本部分可帮助您对多实例模式机箱和实例进行故障排除和诊断。

监控多实例设置

显示系统详细信息

此 FXOS 命令显示当前模式：本地或容器。如果模式为本地（也称为设备模式），则可以转换为多实例（容器）模式。请注意，多实例模式下的提示/名称是通用的“firepower-<model> "，而设备模式下的提示符是您为 设置的主机名（默认情况下为“firepower”）

```
firepower # show system detail

Systems:
    Name: firepower
    Mode: Stand Alone
    System IP Address: 172.16.0.50
    System IPv6 Address: ::
    System Owner:
    System Site:
    Deploy Mode: Native
    Description for System:
firepower #
```

范围系统 > 显示

此 FXOS 命令以表格格式显示当前模式。请注意，多实例模式下的提示/名称是通用的“firepower-<model> "，而设备模式下的提示符是您为 设置的主机名。

```
firepower-3110# scope system
firepower-3110 /system # show

Systems:
    Name       Mode        Deploy Mode System IP Address System IPv6 Address
    ---------- ----------- ----------- ----------------- -------------------
    firepower-3110
               Stand Alone Container   10.89.5.42        ::


3110-1# scope system
3110-1 /system # show

Systems:
    Name       Mode        Deploy Mode System IP Address System IPv6 Address
    ---------- ----------- ----------- ----------------- -------------------
    3110-1     Stand Alone Native      10.89.5.41        ::
3110-1 /system #
```

监控实例接口

show portmanager switch forward-rules hardware mac-filter

此命令显示两个实例的内部交换机转发规则，为每个实例分配一个专用物理接口。以太网接口 1/2 分配给 ftd1，以太网接口 1/1 分配给 ftd2。

ECMP 组 1540 分配给 ftd1，ECMP 组 1541 分配给 ftd2。

```
secfw-3140(local-mgmt)# show portmanager switch forward-rules hardware mac-filter
      VLAN   SRC_PORT   PC_ID   SRC_ID   DST_PORT     PKT_CNT      DMAC
1        0         17       0       17         19       29164  0:0:0:0:0:0
2        0         19       0       19         17       67588  0:0:0:0:0:0
3        0          1       0      101       1541           0  a2:5b:83:0:0:15
4        0          1       0      101       1541        8181  ff:ff:ff:ff:ff:ff
5        0          2       0      102       1540           0  a2:5b:83:0:0:18
6        0          2       0      102       1540         431  ff:ff:ff:ff:ff:ff
7        0         17       0        0          0       11133  0:0:0:0:0:0
8        0         17       0        0          0           0  0:0:0:0:0:0
```

此命令显示共享物理接口分配给两个实例的两个实例的内部交换机转发规则。以太网接口 1/1 在 ftd1 和 ftd2 之间共享。

ECMP 组 1540 分配给 ftd1，ECMP 组 1541 分配给 ftd2。

MCAST 组 4096 用于在 ftd1 和 ftd2 之间复制广播流量。

```
firepower-3140(local-mgmt)# show portmanager switch forward-rules hardware mac-filter
      VLAN   SRC_PORT   PC_ID   SRC_ID   DST_PORT     PKT_CNT      DMAC
1        0         17       0       17         19         2268  0:0:0:0:0:0
2        0         19       0       19         17         4844  0:0:0:0:0:0
3        0          1       0      101       1541           0  a2:5b:83:0:0:9
4        0          1       0      101       4096          546  ff:ff:ff:ff:ff:ff
```

```
5         0          1        0       101       1540            0  a2:5b:83:0:0:c
6         0         17        0         0          0         1263  0:0:0:0:0:0
7         0         17        0         0          0            0  0:0:0:0:0:0
```

此命令显示分配给两个实例的共享子接口的两个实例的内部交换机转发规则。以太网接口 1/1.2452 在 ftd1 和 ftd2 之间共享。

ECMP 组 1540 分配给 ftd1，ECMP 组 1541 分配给 ftd2。

MCAST 组 4097 用于在 ftd1 和 ftd2 之间复制广播流量。

```
firepower-3140(local-mgmt)# show portmanager switch forward-rules hardware mac-filter
      VLAN    SRC_PORT    PC_ID    SRC_ID    DST_PORT      PKT_CNT       DMAC
1        0          17        0        17          19        21305  0:0:0:0:0:0
2        0          19        0        19          17        50976  0:0:0:0:0:0
3     2452           1        0       101        1541          430  a2:5b:83:0:0:f
4     2452           1        0       101        4097            0  ff:ff:ff:ff:ff:ff
5     2452           1        0       101        1540            0  a2:5b:83:0:0:12
6        0          17        0         0           0        11038  0:0:0:0:0:0
7        0          17        0         0           0            0  0:0:0:0:0:0
```

show portmanager switch ecmp-groups detail

使用此命令可列出每个实例 Ecmp-Vport-物理端口映射详细信息。

注释 物理端口 18 是内部交换机和实例之间的背板上行链路接口。

```
firepower-3140(local-mgmt)# show portmanager switch ecmp-groups detail
       ECMP-GROUP  VPORT      PHYSICAL-PORT
1      1536        256        18
2      1537        257        18
3      1538        258        18
4      1539        259        18
5      1540        260        18
6      1541        261        18
7      1542        262        18
8      1543        263        18
9      1544        264        18
10     1545        265        18
```

show portmanager switch mcast-groups detail

使用此命令可列出 MCAST 组成员身份详细信息。

```
firepower-3140(local-mgmt)# show portmanager switch mcast-groups detail
       MCAST-GROUP
1      4096
       Member-ports
       Ethernet 1/1
       ECMP-ID 1541
       ECMP-ID 1540
```

show portmanager counters mcast-group

使用此命令可检查 MCAST 组数据包计数器。

```
firepower-3140(local-mgmt)# show portmanager counters mcast-group 4096
PKT_CNT: 8106
```

show portmanager counters ecmp

使用此命令可检查 ECMP 组数据包计数器。

```
firepower-3140(local-mgmt)# show portmanager counters ecmp 1541
PKT_CNT: 430
```

多实例模式的历史记录

表 *2:*

功能	防火墙管理中心最低版本	最低版本	详细信息
防火墙管理中心中的多实例模式转换	7.6.0	7.6.0	现在，您可以将应用模式设备注册到防火墙管理中心，然后将其转换为多实例模式，而无需使用 CLI。 新增/修改的屏幕： • **设备** > **设备管理**，然后对于某个设备，点击 **更多** (⋮) > **转换为多实例** • **设备** > **设备管理**，然后选择多个设备并选择**选择批量操作** > **转换为多实例**
Cisco Secure Firewall 4200 的多实例模式	7.6.0	7.6.0	Cisco Secure Firewall 4200 现已支持多实例模式。

功能	防火墙管理中心最低版本	最低版本	详细信息
Cisco Secure Firewall 3100 的多实例模式。	7.4.1	7.4.1	您可以将 Cisco Secure Firewall 3100 作为单个设备（设备模式）或多个容器实例（多实例模式）进行部署。在多实例模式下，您可以在单个机箱上部署多个容器实例充当完全独立设备。请注意在多实例模式下，您可从容器实例（升级）单独升级操作系统和固件（机箱升级）。 新增/修改的菜单项： • **设备 (Devices)** > **设备管理 (Device Management)** > **添加 (Add)** > **机箱 (Chassis)** • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **机箱管理器 (Chassis Manager)** • **设备 (Devices)** > **平台设置 (Platform Settings)** > **新建策略 (New Policy)** > **机箱平台设置 (Chassis Platform Settings)** • **设备 (Devices)** > **机箱升级 (Chassis Upgrade)** 新增/修改的 CLI 命令：**configure multi-instance network ipv4**、**configure multi-instance network ipv6** 新增/修改的 FXOS 命令：**create device-manager**、**set deploymode** 平台限制：Cisco Secure Firewall 3105 上不支持。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。