Firepower 4100/9300 上的逻辑设备

Firepower 4100/9300 是具有灵活性的安全平台，可在其中安装一个或多个逻辑设备。在可将 Firewall Threat Defense 添加到防火墙管理中心 之前，必须配置机箱接口，添加逻辑设备，并使用 Cisco Secure Firewall 机箱管理器或 FXOS CLI 将接口分配到 Firepower 4100/9300机箱上的设备。本章介绍基本的接口配置以及如何使用 Cisco Secure Firewall 机箱管理器添加独立或高可用性逻辑设备。要添加集群逻辑设备，请参阅 集群：Firepower 4100/9300。要使用 FXOS CLI，请参阅 FXOS CLI 配置指南。有关更多高级 FXOS 程序和故障排除，请参阅 FXOS 配置指南。

关于接口

Firepower 4100/9300 机箱支持物理接口、容器实例的 VLAN 子接口和 EtherChannel（端口通道）接口。EtherChannel 接口最多可以包含同一类型的 16 个成员接口。

机箱管理接口

机箱管理接口用于通过 SSH 或 防火墙机箱管理器来管理 FXOS 机箱。此接口在**接口 (Interfaces)** 选项卡顶部显示为 **MGMT**，您只可在**接口 (Interfaces)** 选项卡上启用或禁用此接口。此接口独立于分配给应用管理用逻辑设备的 MGMT 型接口。

要配置此接口参数，必须从 CLI 进行配置。要在 FXOS CLI 中查看此接口，请连接到本地管理并显示管理端口：

Firepower # **connect local-mgmt**

Firepower(local-mgmt) # **show mgmt-port**

请注意，即使将物理电缆或小型封装热插拔模块拔下，或者执行了 **mgmt-port shut** 命令，或者逻辑设备已离线，机箱管理接口仍会保持正常运行状态。

注释 机箱管理接口不支持巨型帧。

接口类型

物理接口、容器实例的 VLAN 子接口， 和 EtherChannel（端口通道）接口可以是下列类型之一：

- 数据 - 用于常规数据。不能在逻辑设备之间共享数据接口，且逻辑设备无法通过背板与其他逻辑设备通信。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逻辑设备。
- 数据共享 - 用于常规数据。仅容器实例支持这些数据接口，可由一个或多个逻辑设备/容器实例（仅限Firewall Threat Defense-使用-防火墙管理中心 ）共享。 每个容器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容器实例的数量。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、集群或故障切换链路。
- 管理 - 用于管理应用实例。这些接口可以由一个或多个逻辑设备共享，以访问外部主机；逻辑设备无法通过此接口与共享接口的其他逻辑设备通信。只能为每个逻辑设备分配一个管理接口。根据您的应用和管理器，您可以稍后从数据接口启用管理；但必须将管理接口分配给逻辑设备，即使您不打算在启用数据管理后使用该接口。有关独立机箱管理接口的信息，请参阅机箱管理接口 ， 第 1 页。

注释 管理接口更改会导致逻辑设备重新启动，例如将管理接口从 e1/1 更改为 e1/2 会导致逻辑设备重新启动以应用新的管理接口。

- 事件 - 用作 Firewall Threat Defense-using-防火墙管理中心 设备的辅助管理接口。 要使用此接口，您必须在 Firewall Threat Defense CLI 上配置其 IP 地址和其他参数。例如，您可以将管理流量从活动（例如网络活动）中分隔出来。有关详细信息，请参阅《管理中心配置指南》。事件接口可以由一个或多个逻辑设备共享，以访问外部主机；逻辑设备无法通过此接口与共享接口的其他逻辑设备通信。 如果稍后为管理配置数据接口，则无法使用单独的事件接口。

注释 安装每个应用实例时，会分配一个虚拟以太网接口。如果应用不使用事件接口，则虚拟接口将处于管理员关闭状态。

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- 集群 - 用作集群逻辑设备的集群控制链路。默认情况下，系统会在端口通道 48 上自动创建集群控制链路。“集群”类型仅在 EtherChannel 接口上受支持。 对于多实例集群，无法在设备之间共享集群类型接口。您可以将 VLAN 子接口添加到集群 EtherChannel，以便为每个集群提供单独的集群控制链路。如果向某个集群接口添加子接口，则不能将该接口用于本地集群。防火墙设备管理器 和 Security Cloud Control 不支持群集技术。

注释 本章仅讨论 *FXOS* VLAN 子接口。您还可以在 Firewall Threat Defense 应用内单独创建子接口。有关详细信息，请参阅FXOS 接口与应用接口 ，第 4 页。

有关独立部署和集群部署中Firewall Threat Defense和 ASA 应用的接口类型支持，请参阅下表。

表 *1:* 接口类型支持

应用		数据	数据：子接口	数据共享	数据共享：子接口	管理	事件	集群（仅 EtherChannel）	集群：子接口
Firewall Threat Defense	独立本地实例	是	—	—	—	是	是	—	—
	独立容器实例	是	是	是	是	是	是	—	—
	集群本地实例	是（EtherChannel 仅用于机箱间集群）	—	—	—	是	是	是	—
	集群容器实例	是（EtherChannel 仅用于机箱间集群）	—	—	—	是	是	是	是
ASA	独立本地实例	是	—	—	—	是	—	是	—
	集群本地实例	是（EtherChannel 仅用于机箱间集群）	—	—	—	是	—	是	—

FXOS 接口与应用接口

Firepower 4100/9300 管理物理接口、容器实例的 VLAN 子接口和 EtherChannel（端口通道）接口的基本以太网设置。在应用中，您可以配置更高级别的设置。例如，您只能在 FXOS 中创建 EtherChannel；但是，您可以为应用中的 EtherChannel 分配 IP 地址。

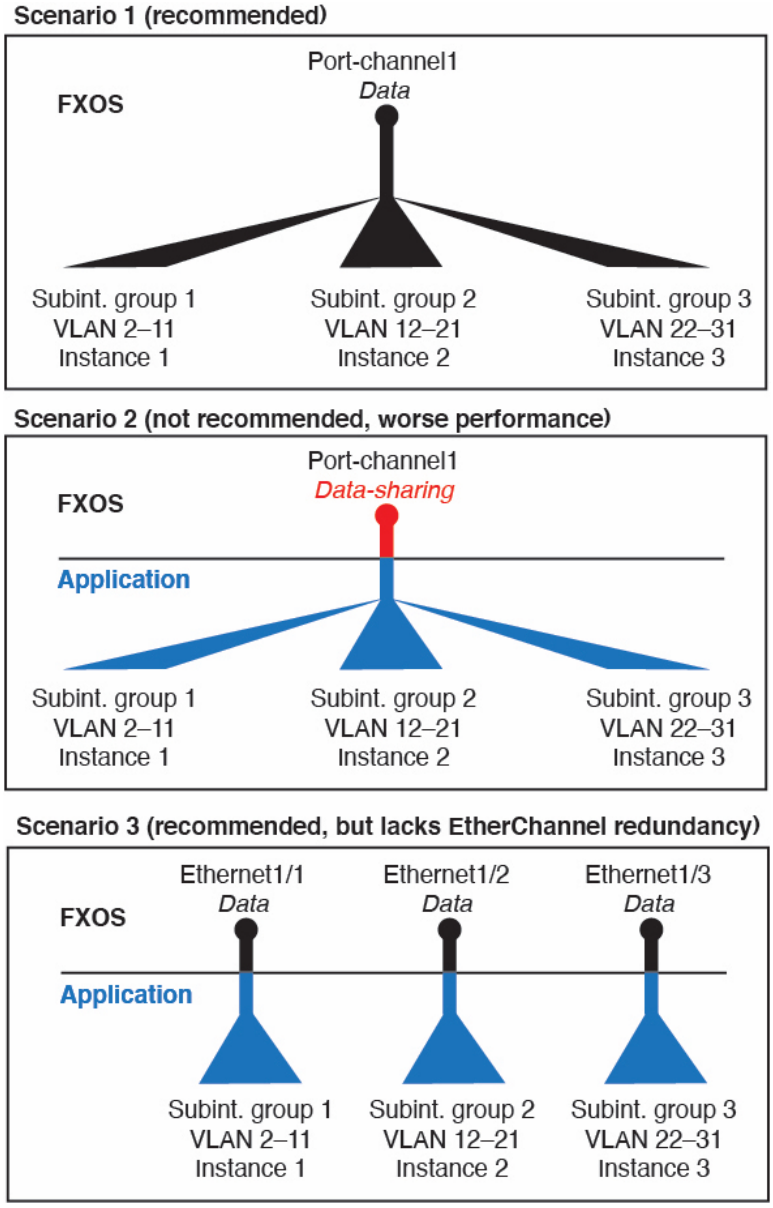
下文将介绍 FXOS 接口与应用接口之间的交互。

VLAN 子接口

对于所有逻辑设备，您可以在应用内创建 VLAN 子接口。

仅对于独立模式下的容器实例，您还可以在 FXOS 中创建 VLAN 子接口。 除集群类型接口外，多实例集群不支持 FXOS 中的子接口。应用定义的子接口不受 FXOS 限值的约束。选择在哪个操作系统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 FXOS 中创建子接口。偏好 FXOS 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。如果您在应用内创建这些子接口，则必须在 FXOS 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: FXOS* 中的 *VLAN* 与容器实例的应用



机箱和应用中的独立接口状态

您可以从管理上启用和禁用机箱和应用中的接口。必须在两个操作系统中都启用能够正常运行的接口。由于接口状态可独立控制，因此机箱与应用之间可能出现不匹配的情况。

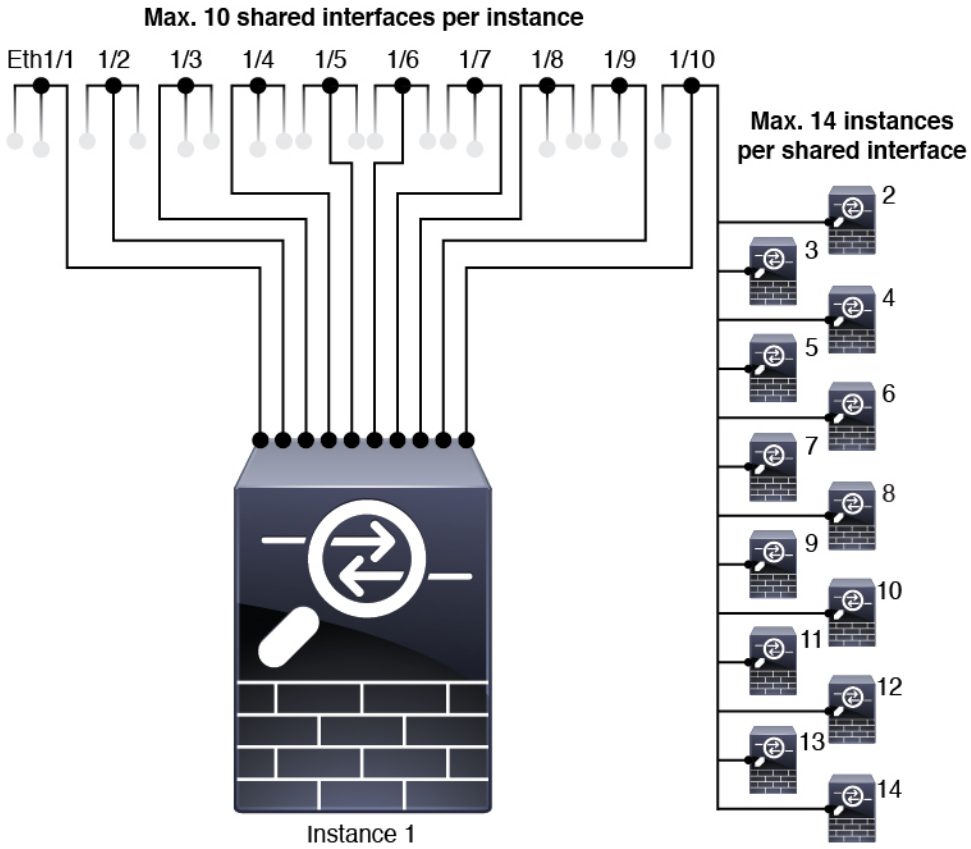
应用内接口的默认状态取决于接口类型。例如，在应用内，默认禁用物理接口或 EtherChannel，但默认启用子接口。

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。

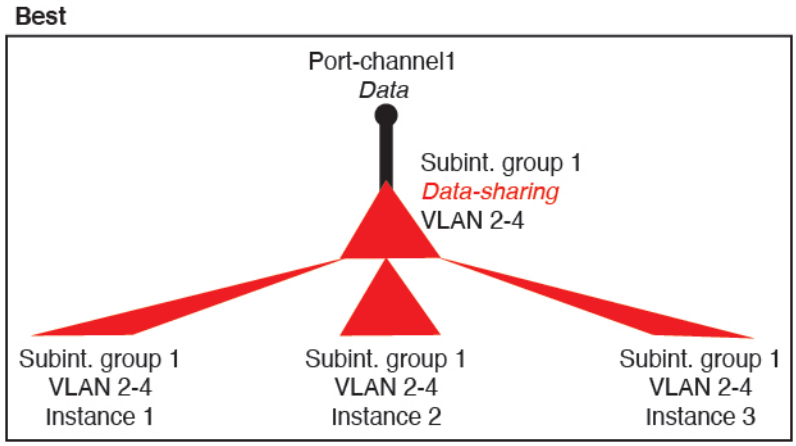
共享接口时，请按照可扩展性从高到低的顺序遵循这些最佳实践：

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

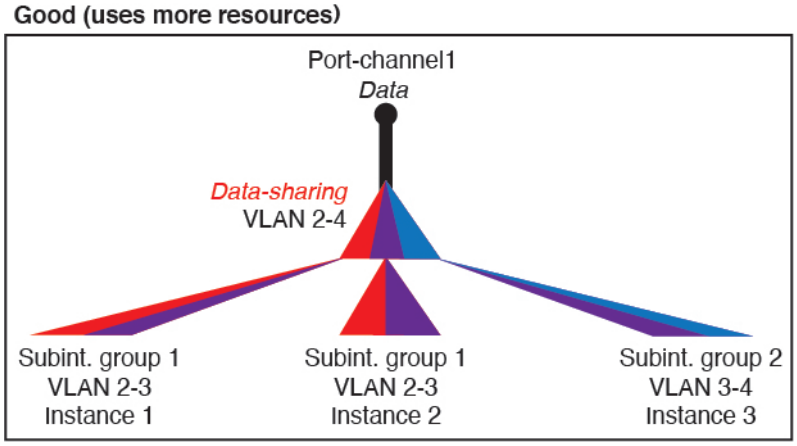
享物理/EtherChannel 接口或子接口相比，当您共享单父项子接口时，VLAN 组表提供更高的转发表可扩展性。

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。

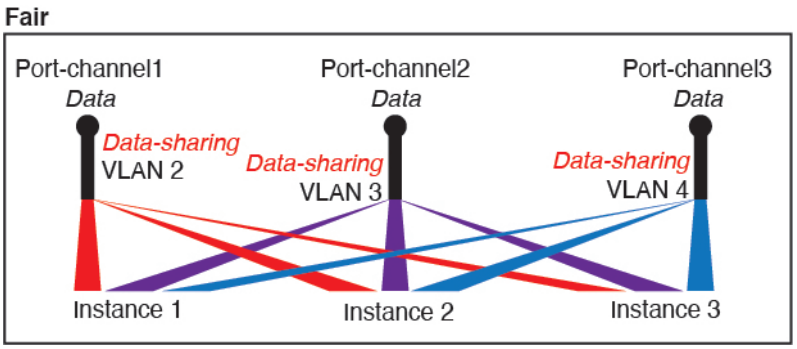
图 *3:* 良好：一个父项上共享多个子接口组



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。

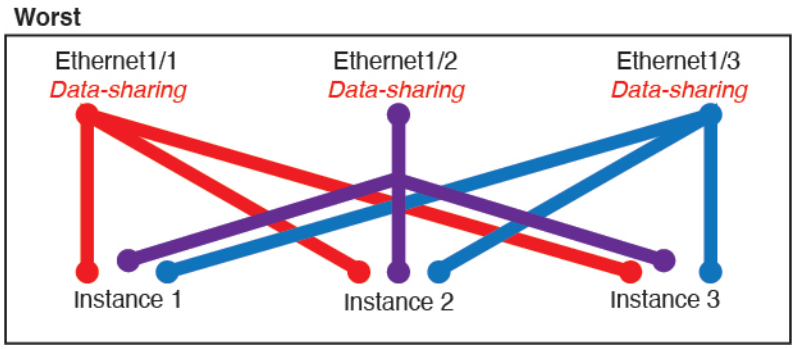
图 *4:* 一般：独立父项上的共享子接口



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



共享接口使用示例

有关接口共享示例和可扩展性，请参阅下表。以下情景假设使用一个在所有实例中共享的物理/EtherChannel 接口来实现管理，和另一个设有专用子接口的物理或 EtherChannel 接口，用于实现高可用性。

- 表 2: Firepower 9300（设有三个 SM-44）上的物理/EtherChannel 接口和实例， 第 9 页
- 表 3: Firepower 9300（设有三个 SM-44）上的一个父接口的子接口和实例， 第 11 页
- 表 4: Firepower 9300（设有一个 SM-44）上的物理/EtherChannel 接口和实例， 第 14 页
- 表 5: Firepower 9300（设有一个 SM-44）上的一个父接口的子接口和实例， 第 16 页

Firepower 9300（设有三个 SM-44）

下表适用于仅使用物理接口或 Etherchannel 的 9300 上的三个 SM-44 安全模块。在未设子接口的情况下，接口的最大数量受限。此外，与共享多个子接口相比，共享多个物理接口所使用的转发表资源更多。

每个 SM-44 模块最多可支持 14 个实例。如有必要，系统会拆分模块之间的实例，以将实例数维持在限值范围内。

表 *2: Firepower 9300*（设有三个 *SM-44*）上的物理*/EtherChannel* 接口和实例

专用接口	共享接口	实例数	转发表使用百分比
32: • 8 • 8 • 8 • 8	**0**	**4:** • 实例 1 • 实例 2 • 实例 3 • 实例 4	16%
30: • 15 • 15	**0**	**2:** • 实例 1 • 实例 2	14%
14: • 14（每个实例 1 个专用子接口）	**1**	**14:** • 实例 1 至实例 14	46%
33: • 11（每个实例 1 个专用子接口） • 11（每个实例 1 个专用子接口） • 11（每个实例 1 个专用子接口）	**3:** • 1 • 1 • 1	**33:** • 实例 1 至实例 11 • 实例 12 至实例 22 • 实例 23 至实例 33	98%

专用接口	共享接口	实例数	转发表使用百分比
33: • *11*（每个实例 *1* 个专用接口） • *11*（每个实例 *1* 个专用接口） • *12*（每个实例 *1* 个专用接口）	***3:*** • *1* • *1* • *1*	***34:*** • 实例 *1* 至实例 *11* • 实例 *12* 至实例 *22* • 实例 *23* 至实例 *34*	*102%* 禁止使用
30: • 30（每个实例 1 个专用接口）	**1**	**6：** • 实例 1 实例 6	25%
30: • 10（每个实例 5 个专用接口） • 10（每个实例 5 个专用接口） • 10（每个实例 5 个专用接口）	**3:** • 1 • 1 • 1	**6：** • 实例 1 至实例 2 • 实例 2 至实例 4 • 实例 5 至实例 6	23%
30: • 30（每个实例 6 个专用接口）	**2**	**5：** • 实例 1 至实例 5	28%

专用接口	共享接口	实例数	转发表使用百分比
30: • 12（每个实例 6 个专用接口） • 18（每个实例 6 个专用接口）	**4:** • 2 • 2	**5:** • 实例 1 至实例 2 • 实例 2 至实例 5	26%
24: • 6 • 6 • 6 • 6	**7**	**4:** • 实例 1 • 实例 2 • 实例 3 • 实例 4	44%
24: • 12（每个实例 6 个专用接口） • 12（每个实例 6 个专用接口）	**14:** • 7 • 7	**4:** • 实例 1 至实例 2 • 实例 2 至实例 4	41%

下表适用于使用单父项物理接口上子接口的 9300 的三个 SM-44 安全模块。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。与共享多个子接口相比，共享多个物理接口所使用的转发表资源更多。

每个 SM-44 模块最多可支持 14 个实例。如有必要，系统会拆分模块之间的实例，以将实例数维持在限值范围内。

表 *3: Firepower 9300*（设有三个 *SM-44*）上的一个父接口的子接口和实例

专用子接口	共享子接口	实例数	转发表使用百分比
168: • 168（每个实例 4 个专用子接口）	**0**	**42:** • 实例 1 至实例 42	33%

专用子接口	共享子接口	实例数	转发表使用百分比
224: • 224（每个实例 16 个专用子接口）	**0**	**14:** • 实例 1 至实例 14	27%
14: • 14（每个实例 1 个专用子接口）	**1**	**14:** • 实例 1 至实例 14	46%
33: • 11（每个实例 1 个专用子接口） • 11（每个实例 1 个专用子接口） • 11（每个实例 1 个专用子接口）	**3:** • 1 • 1 • 1	**33:** • 实例 1 至实例 11 • 实例 12 至实例 22 • 实例 23 至实例 33	98%
70: • 70（每个实例 5 个专用子接口）	**1**	**14:** • 实例 1 至实例 14	46%
165: • 55（每个实例 5 个专用子接口） • 55（每个实例 5 个专用子接口） • 55（每个实例 5 个专用子接口）	**3:** • 1 • 1 • 1	**33:** • 实例 1 至实例 11 • 实例 12 至实例 22 • 实例 23 至实例 33	98%

专用子接口	共享子接口	实例数	转发表使用百分比
70: • 70（每个实例 5 个专用子接口）	**2**	**14:** • 实例 1 至实例 14	46%
165: • 55（每个实例 5 个专用子接口） • 55（每个实例 5 个专用子接口） • 55（每个实例 5 个专用子接口）	**6:** • 2 • 2 • 2	**33:** • 实例 1 至实例 11 • 实例 12 至实例 22 • 实例 23 至实例 33	98%
70: • 70（每个实例 5 个专用子接口）	**10**	**14:** • 实例 1 至实例 14	46%
165: • *55*（每个实例 *5* 个专用子接口） • *55*（每个实例 *5* 个专用子接口） • *55*（每个实例 *5* 个专用子接口）	***30:*** • *10* • *10* • *10*	***33:*** • 实例 *1* 至实例 *11* • 实例 *12* 至实例 *22* • 实例 *23* 至实例 *33*	*102%* 禁止使用

Firepower 9300（设有一个 SM-44）

下表适用于仅使用物理接口或 Etherchannel 的 Firepower 9300（设一个 SM-44）。在未设子接口的情况下，接口的最大数量受限。此外，与共享多个子接口相比，共享多个物理接口所使用的转发表资源更多。

Firepower 9300（设有一个 SM-44）最多可支持 14 个实例。

表 *4: Firepower 9300*（设有一个 *SM-44*）上的物理*/EtherChannel* 接口和实例

专用接口	共享接口	实例数	转发表使用百分比
32: • 8 • 8 • 8 • 8	**0**	**4:** • 实例 1 • 实例 2 • 实例 3 • 实例 4	16%
30: • 15 • 15	**0**	**2:** • 实例 1 • 实例 2	14%
14: • 14（每个实例 1 个专用子接口）	**1**	**14:** • 实例 1 至实例 14	46%
14: • 7（每个实例 1 个专用子接口） • 7（每个实例 1 个专用子接口）	**2:** • **1** • **1**	**14:** • 实例 1 至实例 7 • 实例 8 至实例 14	37%
32: • 8 • 8 • 8 • 8	**1**	**4:** • 实例 1 • 实例 2 • 实例 3 • 实例 4	21%

专用接口	共享接口	实例数	转发表使用百分比
32: • 16（每个实例 8 个专用接口） • 16（每个实例 8 个专用接口）	**2**	**4:** • 实例 1 至实例 2 • 实例 3 至实例 4	20%
32: • 8 • 8 • 8 • 8	**2**	**4:** • 实例 1 • 实例 2 • 实例 3 • 实例 4	25%
32: • 16（每个实例 8 个专用接口） • 16（每个实例 8 个专用接口）	**4:** • 2 • 2	**4:** • 实例 1 至实例 2 • 实例 3 至实例 4	24%
24: • 8 • 8 • 8	**8**	**3:** • 实例 1 • 实例 2 • 实例 3	37%
10: • 10（每个实例 2 个专用接口）	**10**	**5:** • 实例 1 至实例 5	69%

专用接口	共享接口	实例数	转发表使用百分比
10: • 6（每个实例2个专用接口） • 4（每个实例2个专用接口）	**20:** • 10 • 10	**5：** • 实例 1 至实例 3 • 实例 4 至实例 5	59%
14: • *12*（每个实例 *2* 个专用接口）	***10***	***7***： • 实例 *1* 至实例 *7*	*109%* 禁止使用

下表适用于使用单父项物理接口上子接口的Firepower 9300（设有一个SM-44）。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。与共享多个子接口相比，共享多个物理接口所使用的转发表资源更多。

Firepower 9300（设有一个 SM-44）最多可支持 14 个实例。

表 *5: Firepower 9300*（设有一个 *SM-44*）上的一个父接口的子接口和实例

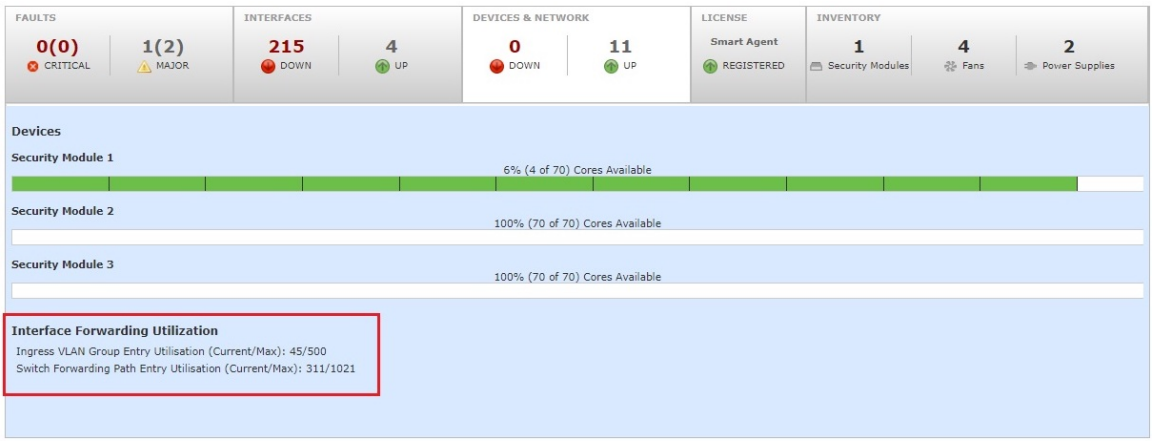
专用子接口	共享子接口	实例数	转发表使用百分比
112： • 112（每个实例 8 个专用子接口）	**0**	**14:** • 实例 1 至实例 14	17%
224: • 224（每个实例 16 个专用子接口）	**0**	**14:** • 实例 1 至实例 14	17%
14: • 14（每个实例 1 个专用子接口）	**1**	**14:** • 实例 1 至实例 14	46%

专用子接口	共享子接口	实例数	转发表使用百分比
14: • 7（每个实例1个专用子接口） • 7（每个实例1个专用子接口）	**2:** • 1 • 1	**14:** • 实例 1 至实例 7 • 实例 8 至实例 14	37%
112： • 112（每个实例 8 个专用子接口）	**1**	**14:** • 实例 1 至实例 14	46%
112： • 56（每个实例 8 个专用子接口） • 56（每个实例 8 个专用子接口）	**2:** • 1 • 1	**14:** • 实例 1 至实例 7 • 实例 8 至实例 14	37%
112： • 112（每个实例 8 个专用子接口）	**2**	**14:** • 实例 1 至实例 14	46%
112： • 56（每个实例 8 个专用子接口） • 56（每个实例 8 个专用子接口）	**4：** • 2 • 2	**14:** • 实例 1 至实例 7 • 实例 8 至实例 14	37%
140: • 140（每个实例 10 个专用子接口）	**10**	**14:** • 实例 1 至实例 14	46%

专用子接口	共享子接口	实例数	转发表使用百分比
140: • 70（每个实例10个专用子接口） • 70（每个实例10个专用子接口）	**20:** • 10 • 10	**14:** • 实例 1 至实例 7 • 实例 8 至实例 14	37%

查看共享接口资源

要查看转发表和 VLAN 组使用情况，请参阅**设备和网络 (Devices & Network)** > **接口转发利用率 (Interface Forwarding Utilization)** 区域 下输入 **show detail** 命令。例如：



防火墙威胁防御 支持的内联集链路状态传播

内联集类似于导线上的凹凸，用于将两个接口绑定在一起插入到现有网络中。此功能使系统可以安装在任何网络环境中，而无需配置相邻网络设备。内联接口无条件接收所有流量，但是，除非已明确丢弃，否则这些接口上接收的所有流量将在内联集外重传。

当您在 防火墙威胁防御 应用中配置内联集并启用链路状态传播时，防火墙威胁防御 会向 FXOS 机箱发送内联集成员身份。链路状态传播意味着，当内联集的一个接口断开时，机箱将自动关闭内联接口对的第二个接口。当被关闭的接口恢复运行时，第二个接口也将自动恢复运行。换句话说，如果一个接口的链路状态更改，机箱会感知该更改并更新其他接口的链路状态以与其匹配。请注意，机箱最多需要 4 秒即可传播链路状态更改。在将路由器配置为在处于故障状态的网络设备上自动重新路由流量的弹性网络环境中，链路状态传播特别有用。

注释 请勿为同一内联集启用 硬件旁路 和传播链路状态。

关于逻辑设备

逻辑设备允许您运行一个应用实例（ASA 或 防火墙威胁防御）和一个可选修饰器应用 (Radware DefensePro) 以形成服务链。

当您添加逻辑设备时，还应定义应用实例类型和版本，分配接口，并配置推送至应用配置的引导程序设置。

注释 对于Firepower9300，可以在机箱中的独立模块上安装不同类型的应用（ASA 和防火墙威胁防御）。还可以在独立模块上运行一种应用实例的不同版本。

独立和集群逻辑设备

您可以添加以下类型的逻辑设备：

- 独立 - 独立逻辑设备作为独立单元或高可用性对中的单元运行。
- 集群 - 集群逻辑设备允许您将多个单元集合在一起，具有单个设备的全部便捷性（管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。Firepower 9300 等多模块设备支持机箱内集群。对于Firepower 9300，所有三个模块必须参与集群，同时适用于本地实例和容器实例。防火墙设备管理器不支持集群。

逻辑设备应用实例：容器和本地

应用实例在以下类型部署中运行：

- 本地实例 - 本地实例使用安全模块/引擎的所有资源（CPU、RAM 和磁盘空间），因此您仅可安装一个本地实例。
- 容器实例 - 容器实例使用安全模块/引擎的部分资源，因此您可以安装多个容器实例。仅使用 防火墙管理中心 的 防火墙威胁防御 支持多实例功能；ASA 或使用 防火墙设备管理器 的 防火墙威胁防御 不支持。

注释 尽管实现方式不同，但多实例功能与 ASA 多情景模式类似。多情景模式下区分了单个应用实例，而多实例功能允许独立容器实例。容器实例允许硬资源分离、单独配置管理、单独重新加载、单独软件更新和完全防火墙威胁防御功能支持。由于共享资源，多情景模式支持给定平台上的更多情景。防火墙威胁防御 的多情景模式不可用。

对于 Firepower 9300，可以在某些模块上使用本地实例，在其他模块上使用容器实例。

容器实例接口

要确保灵活使用容器实例的物理接口，可以在 FXOS 中创建 VLAN 子接口，还可以在多个实例之间共享接口（VLAN 或物理接口）。本地实例不得使用 VLAN 子接口或共享接口。 多实例集群不得使用 VLAN 子接口或共享接口。集群控制链路例外，它可以使用集群 EtherChannel 的子接口。请参阅共享接口可扩展性，第 6 页和为容器实例添加 VLAN 子接口，第 41 页。

注释 本文档仅讨论 *FXOS* VLAN 子接口。您还可以在 Firewall Threat Defense 应用内单独创建子接口。有关详细信息，请参阅FXOS 接口与应用接口，第 4 页。

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。

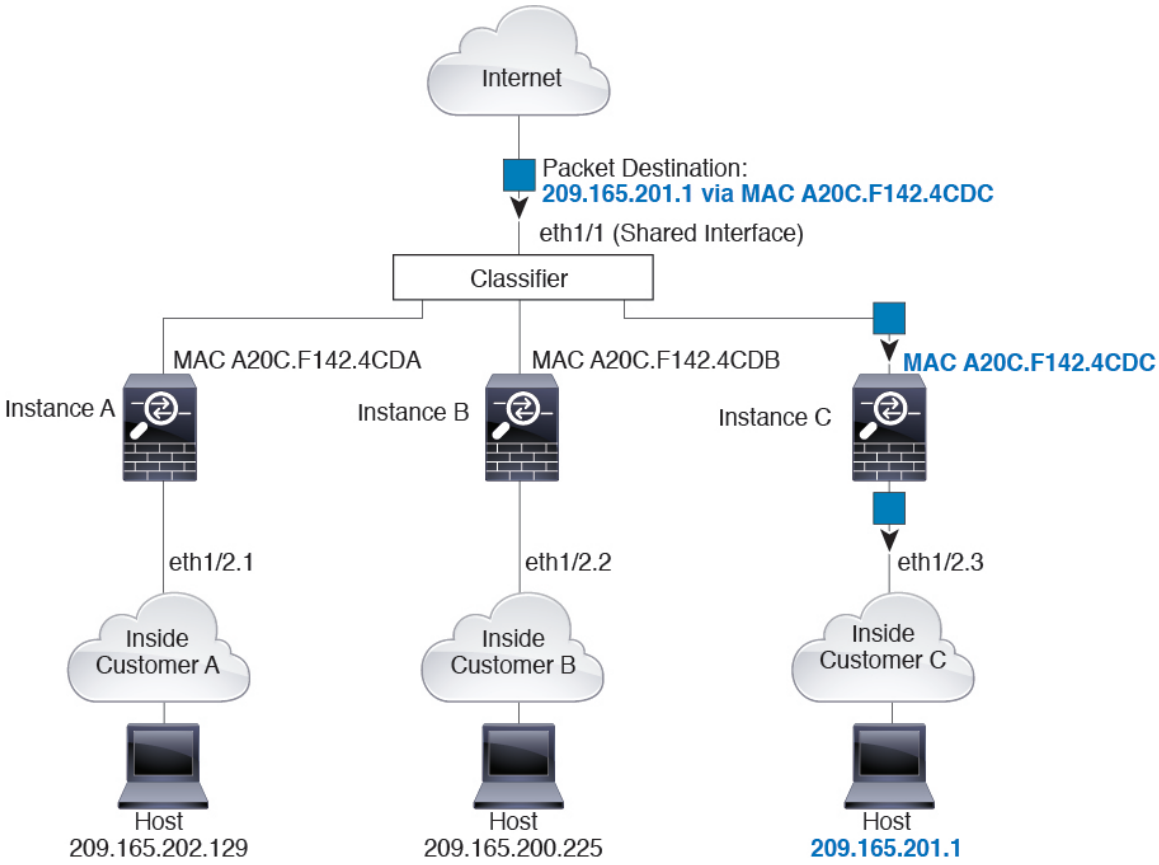
注释 如果目的 MAC 地址为组播或广播 MAC 地址，则数据包会复制并传递到每个实例。

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。

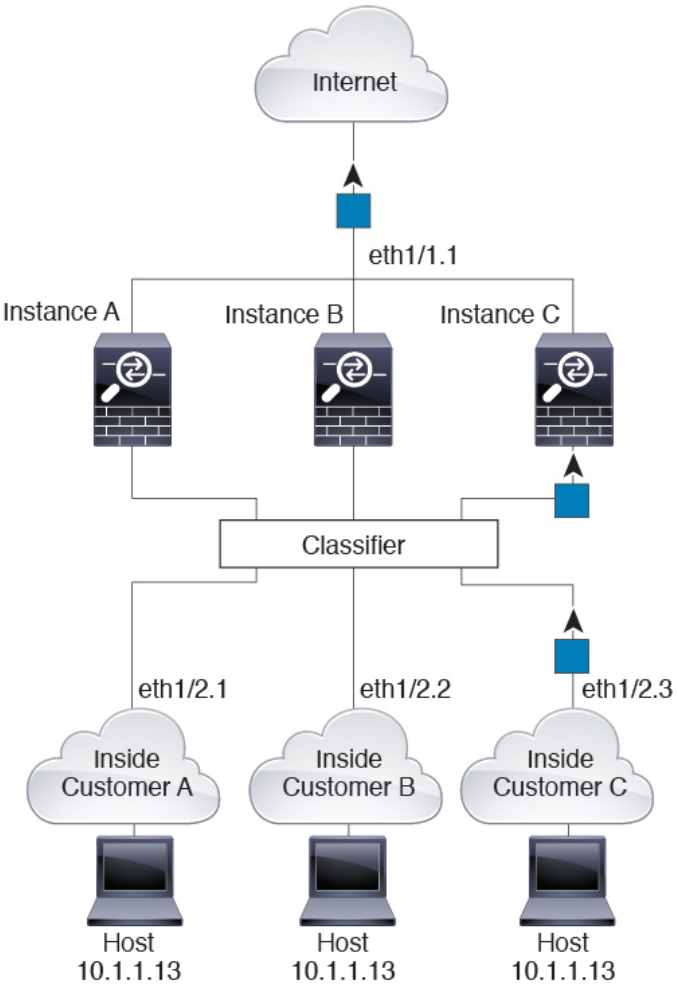
图 *6:* 使用 ***MAC*** 地址通过共享接口进行数据包分类



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。

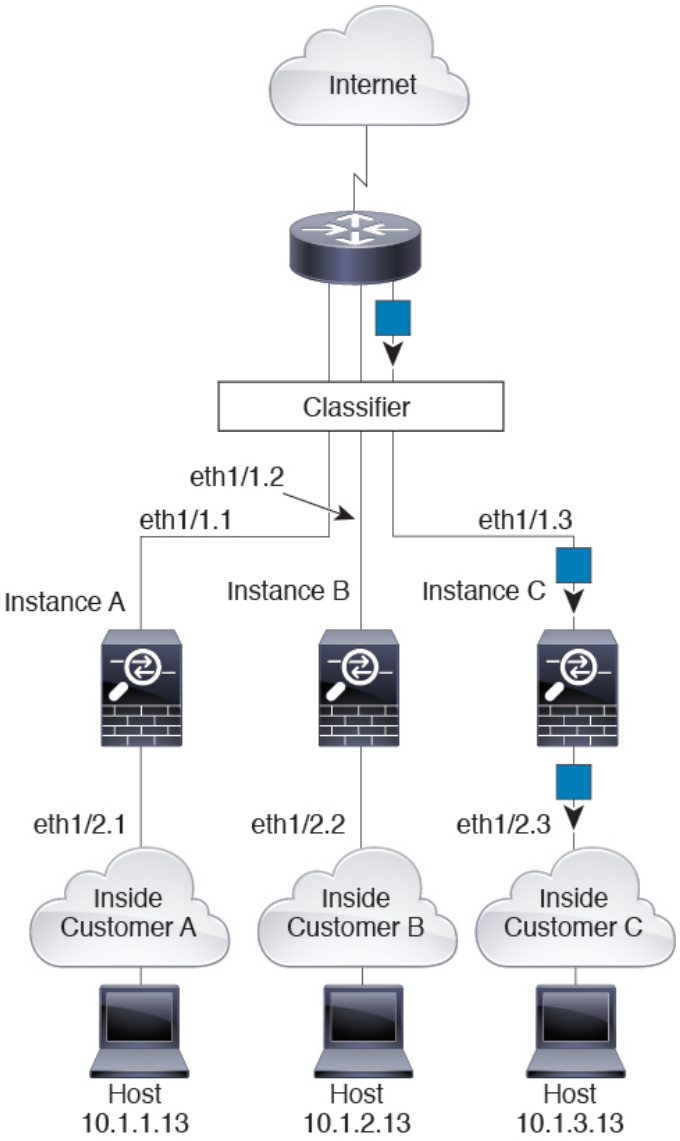
图 7: 来自内部网络的传入流量



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。

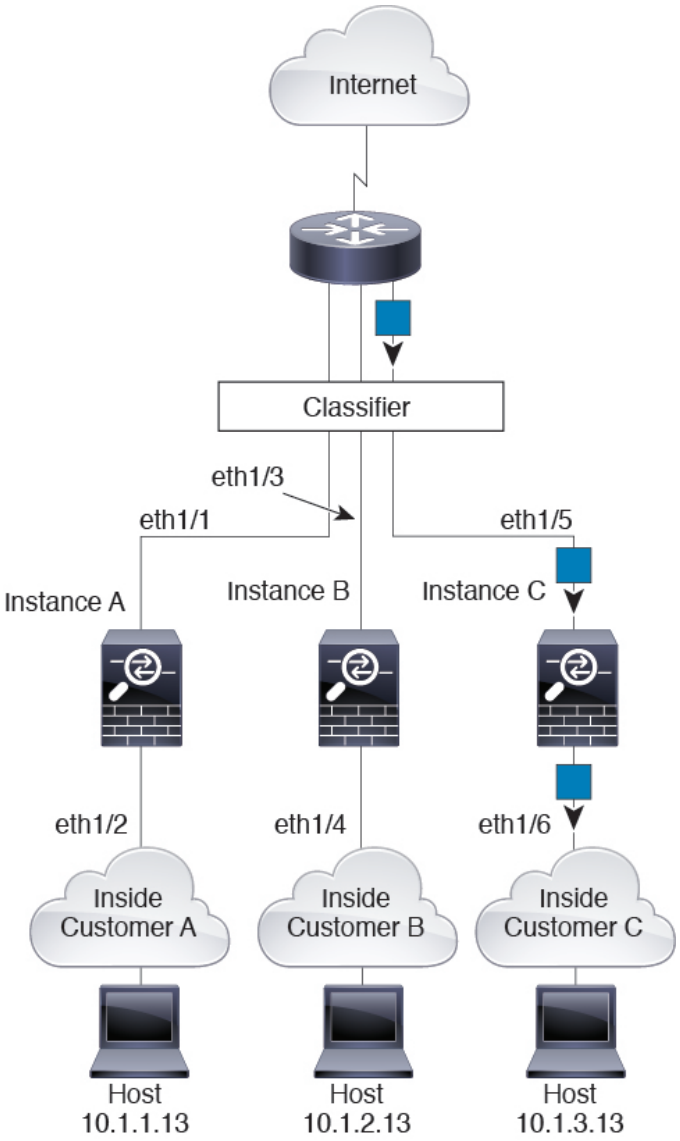
图 *8:* 透明防火墙实例



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

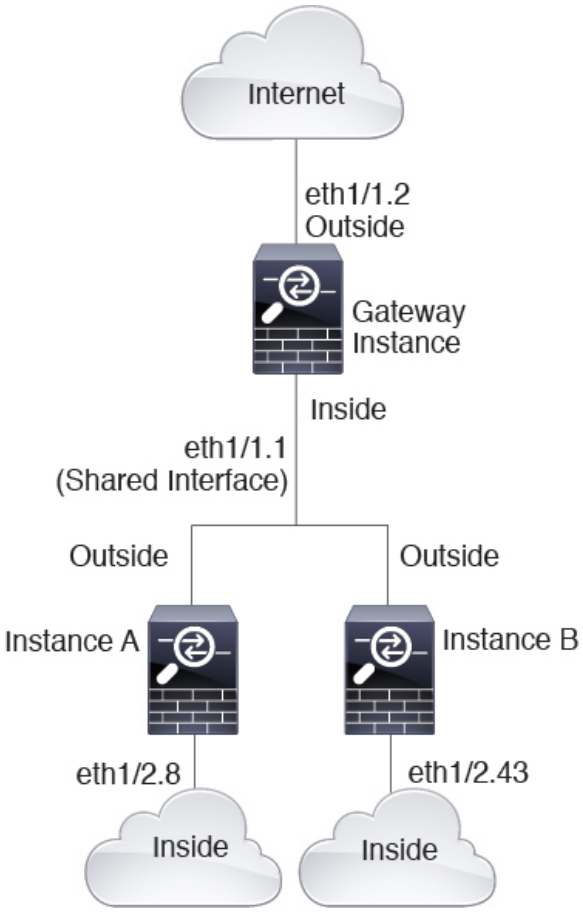


级联容器实例

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



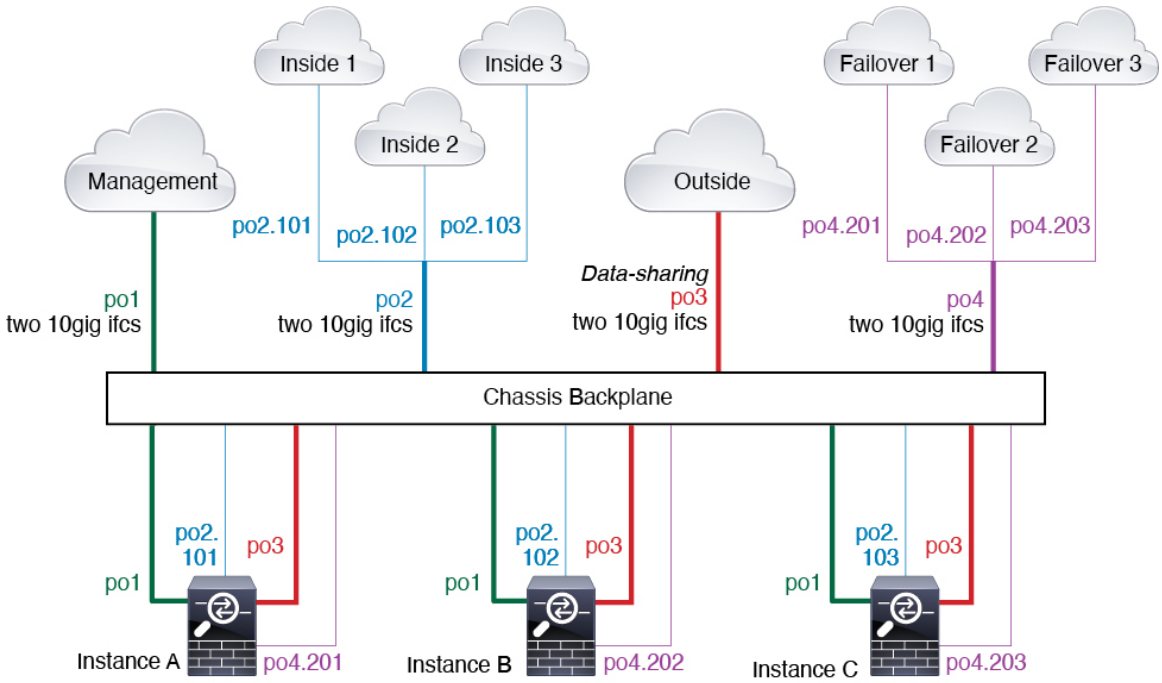
注释 请勿使用具有高可用性的级联实例（使用共享接口）。发生故障转移且备用设备重新加入后，MAC 地址可能会暂时重叠并导致中断。您应改为为网关实例和内部实例使用唯一接口，使用外部交换机在实例之间传递流量。

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 - 所有实例都使用端口通道 1 接口（管理类型）。此 EtherChannel 包括两个万兆以太网接口。在每个应用内，该接口都使用同一管理网络上的唯一 IP 地址。
- 内部 - 每个实例使用端口通道 2 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 3 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 4 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。



容器实例接口的自动 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

容器实例资源管理

要指定每个容器实例的资源使用情况，请在FXOS中创建一个或多个资源配置文件。部署逻辑设备/应用实例时，请指定想要使用的资源配置文件。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。要查看每个型号的可用资源，请参阅容器实例的要求和前提条件，第 30 页。要添加资源配置文件，请参阅为容器实例添加资源配置文件，第 43 页。

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 会话数和 TLS 代理会话数）是为了得出本地实例的内存和 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% 核心的容器实例，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，但容器实例可用的吞吐量可能低于本地实例可用的吞吐量。

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。

容器实例与高可用性

您可以在 2 个独立机箱上使用容器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。请注意，不得在FXOS中配置高可用性；在应用管理器中配置每个高可用性对。

有关详细要求，请参阅高可用性的要求和前提条件，第 31 页和添加高可用性对，第 49 页。

容器实例和集群

您可以每个安全模块/引擎各使用一个容器实例创建容器实例集群。有关详细要求，请参阅集群要求和前提条件，第 31 页。

容器实例的许可证

所有许可证按每个引擎/机箱（对于Firepower 4100）或每个安全模块（对于Firepower 9300）予以使用，而不是按每个容器实例使用。请查看以下详细信息：

- 基础版 许可证自动分配：每个 安全模块/引擎一个。
- 功能许可证手动分配到每个实例；但每个 安全模块/引擎每个功能只能使用一个许可证。例如，对于具有 3 个安全模块的 Firepower 9300，每个模块只需要一个 URL 过滤 许可证，总共需要 3 个许可证，而无须考虑正在使用的实例数。

例如：

表 *6: Firepower 9300* 上容器实例的许可证使用情况示例

Firepower 9300	实例	许可证
安全模块 1	实例 1	基础版、 URL 过滤、 恶意软件防御
	实例 2	基础版、 URL 过滤
	实例 3	基础版、 URL 过滤
安全模块 2	实例 4	基础版、 IPS
	实例 5	基础版、 URL 过滤、 恶意软件防御、 IPS
安全模块 3	实例 6	基础版、 恶意软件防御、 IPS
	实例 7	基础版、 IPS

表 *7:* 许可证总数

基础版	URL 过滤	恶意软件防御	IPS
3	2	3	2

逻辑设备的要求和前提条件

有关要求和前提条件，请参阅以下章节。

硬件和软件组合的要求与前提条件

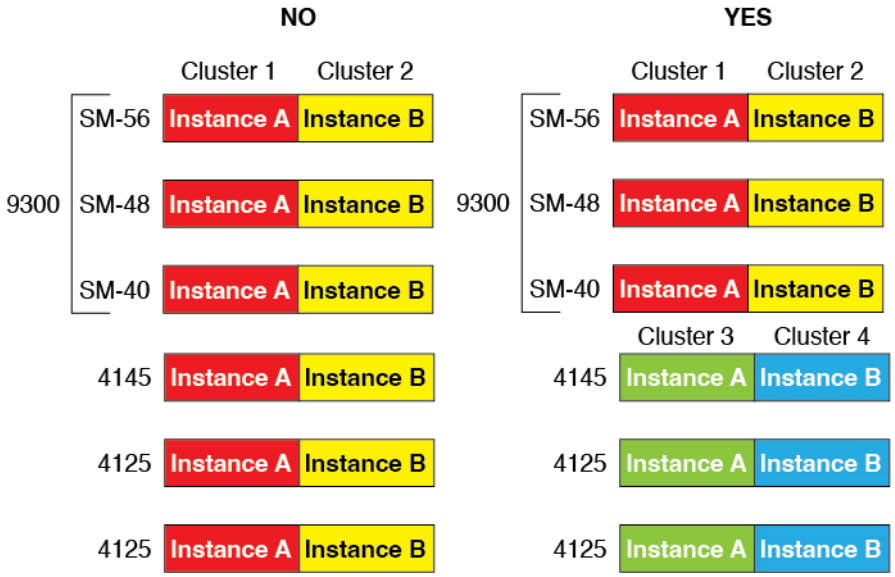
Firepower 4100/9300支持多种型号、安全模块、应用类型以及高可用性和可扩展性功能。请参阅以下要求，了解允许的组合。

Firepower 9300 的要求

Firepower 9300 包括 3 个安全模块插槽和多种类型的安全模块。请参阅以下要求：

- 安全模块类型 - 您可以在 Firepower 9300 中安装不同类型的模块。例如，您可以将 SM-48 作为模块 1、SM-40 作为模块 2、SM-56 作为模块 3 安装。
- 本地实例 集群 - 集群中的所有安全模块（无论是机箱内还是机箱间）都必须为同一类型。您可以在各机箱中安装不同数量的安全模块，但机箱中存在的所有模块（包括任何空插槽）必须属于集群。例如，您可以在机箱 1 中安装 2 个 SM-40，在机箱 2 中安装 3 个 SM-40。 如果在同一机箱中安装了 1 个 SM-48 和 2 个 SM-40，则无法使用集群。

- 容器实例集群 - 您可以使用不同型号类型上的实例创建集群。例如，您可以使用 Firepower 9300 SM-56、SM-48 和 SM-40 上的实例创建集群。但是，不能在同一个集群中混合使用 Firepower 9300 和 Firepower 4100。

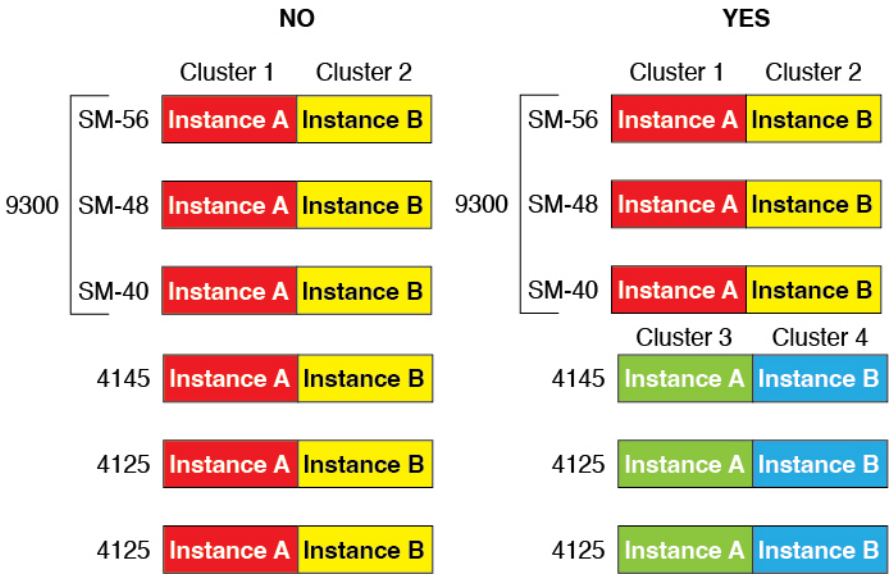


- 高可用性 - 仅在 Firepower 9300 上的同类模块间支持高可用性。 但是，这两个机箱可以包含混合模块。例如，每个机箱都设有 SM-40、SM-48 和 SM-56。可以在 SM-40 模块之间、SM-48 模块之间和 SM-56 模块之间创建高可用性对。
- ASA 和 Firewall Threat Defense 应用类型-您可以在机箱中的独立模块上安装不同类型的应用。例如，您可以在模块 1 和模块 2 上安装 ASA，在模块 3 上安装 Firewall Threat Defense 。
- ASA 或 Firewall Threat Defense 版本 - 您可以在单独的模块上运行不同版本的应用实例类型，或在同一模块上运行单独的容器实例。例如，您可以在模块 1 上安装 Firewall Threat Defense 6.3，在模块 2 上安装 Firewall Threat Defense 6.4，在模块 3 上安装 Firewall Threat Defense 6.5。

Firepower 4100 的要求

Firepower 4100 有多个型号。请参阅以下要求：

- 本地和容器实例 - 在 Firepower 4100 上安装容器实例时，该设备只能支持其他容器实例。本地实例将使用设备的所有资源，因此只能在设备上安装一个本地实例。
- 本地实例 集群 - 集群内的所有机箱都必须为同一型号。
- 容器实例集群 - 您可以使用不同型号类型上的实例创建集群。例如，您可以使用 Firepower 4145 和 4125 上的实例创建集群。但是，不能在同一个集群中混合使用 Firepower 9300 和 Firepower 4100。



- 高可用性 - 仅在同类模块间支持高可用性。
- ASA 和 Firewall Threat Defense 应用类型 - Firepower 4100 只能运行一种应用类型。
- Firewall Threat Defense 容器实例版本 - 您可以在同一模块上将不同版本的 Firewall Threat Defense 作为单独的容器实例运行。

容器实例的要求和前提条件

有关多实例的高可用性或集群要求的信息，请参阅高可用性的要求和前提条件，第 31 页和集群要求和前提条件，第 31 页。

受支持应用类型

- 使用 防火墙管理中心 的 Firewall Threat Defense

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。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 *8:* 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	可用 RAM	可用磁盘空间
Firepower 4112	3	22	78 GB	308 GB
Firepower 4115	7	46	162 GB	308 GB
Firepower 4125	10	62	162 GB	644 GB

型号	最大容器实例数	可用 CPU 核心	可用 RAM	可用磁盘空间
Firepower 4140	7	70	222 GB	311.8 GB
Firepower 4145	14	86	344 GB	608 GB
Firepower 9300 SM-40 安全模块	13	78	334 GB	1359 GB
Firepower 9300 SM-48 安全模块	15	94	334 GB	1341 GB
Firepower 9300 SM-56 安全模块	18	110	334 GB	1314 GB

防火墙管理中心 要求

对于在 Firepower 4100 机箱或 Firepower 9300 模块上的所有情况下，由于许可实施，您必须使用相同 防火墙管理中心 。

高可用性的要求和前提条件

- 高可用性故障转移配置中的两个设备必须：
  - 位于单独的机箱上；不支持 Firepower 9300 的机箱内高可用性。
  - 型号相同。
  - 将同一接口分配至高可用性逻辑设备。
  - 拥有相同数量和类型的接口。启用高可用性之前，所有接口必须在 FXOS 中进行相同的预配置。
- 仅 Firepower 9300 上同种类型模块之间支持高可用性；但是两个机箱可以包含混合模块。例如，每个机箱都设有 SM-56、SM-48 和 SM-40。可以在 SM-56 模块之间、SM-48 模块之间和 SM-40 模块之间创建高可用性对。
- 对于容器实例，每个单元必须使用相同的资源配置文件属性。
- 对于容器实例：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。
- 有关其他高可用性系统要求，请参阅 系统要求一章。

集群要求和前提条件

集群型号支持

Firewall Threat Defense 在以下型号上支持集群：

- Firepower 9300-您可以在集群中包含最多 16 个节点。例如，您可以在 16 个机箱中使用 1 个模块，或者在 8 个机箱中使用 2 个模块，也可以使用最多提供 16 个模块的任意组合。支持多个机箱的集群，以及与一个机箱内的安全模块隔离的集群。
- Firepower 4100-使用多机箱集群时，最多支持 16 个节点。

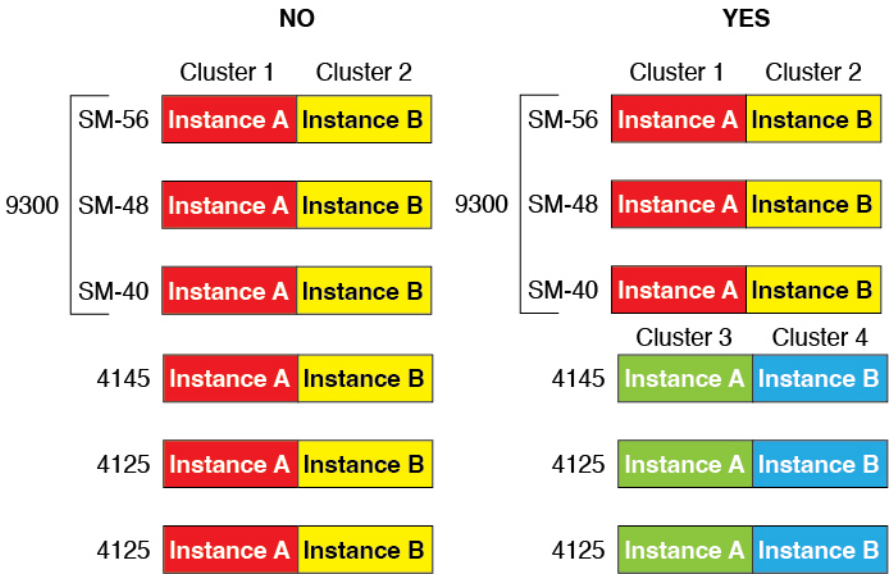
用户角色

- 管理员
- 访问管理员
- 网络管理员

集群硬件和软件要求

集群中的所有机箱：

- 本地实例集群 -对于 Firepower 4100：所有机箱必须为同一型号。对于 Firepower 9300：所有安全模块必须为同一类型。例如，如果使用集群，则Firepower 9300 中的所有模块都必须是 SM-40s。您可以在各机箱中安装不同数量的安全模块，但机箱中存在的所有模块（包括任何空插槽）必须属于集群。
- 容器实例集群 - 建议您为每个集群实例使用相同的安全模块或机箱模型。但是，如果需要，您可以在同一集群中的不同 Firepower 9300 安全模块类型或 Firepower 4100 型号上混合和匹配容器实例。不能在同一个集群中混合使用 Firepower 9300 和 Firepower 4100。例如，您可以使用 Firepower 9300 SM-56、SM-48 和 SM-40 上的实例创建集群。或者，您可以在 Firepower 4145 和 4125 上创建集群。



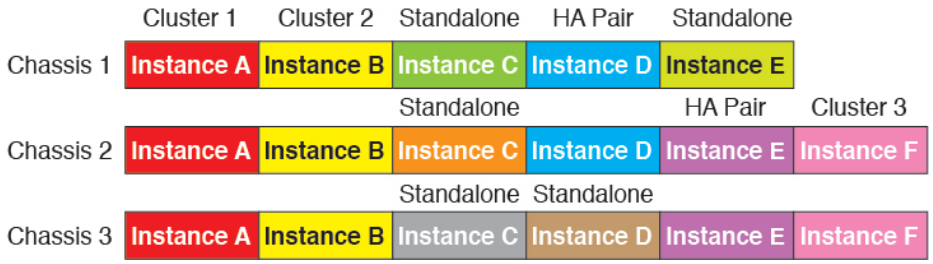
- 除进行映像升级外，必须运行完全相同的 FXOS 和应用软件。不匹配的软件版本可能会导致性能不佳，因此请务必在同一维护窗口中升级所有节点。

- 对于分配给集群的接口，必须采用相同的接口配置，例如：相同的管理接口、EtherChannel、主用接口、速度和复用等。您可在机箱中使用不同的网络模块类型，但必须满足以下条件：对于相同接口 ID，容量必须匹配，且接口可成功捆绑于同一跨区以太网通道中。请注意，所有数据接口必须是具有多个机箱的集群中的 EtherChannel。如果您要在启用集群（例如，通过添加或删除接口模块，或配置 Etherchannel）后更改 FXOS 中的接口，则请对每个机箱执行相同更改，从数据节点开始，到控制节点结束。
- 必须使用同一台 NTP 服务器。 对于 防火墙威胁防御， 防火墙管理中心 必须使用同一台 NTP 服务器。请勿手动设置时间。

多实例集群要求

- 无内部安全模块/引擎集群 - 对于给定集群，只能在每个安全模块/引擎中使用单个容器实例。如果 2 个容器实例在同一模块上运行，则不能将其添加到同一集群。

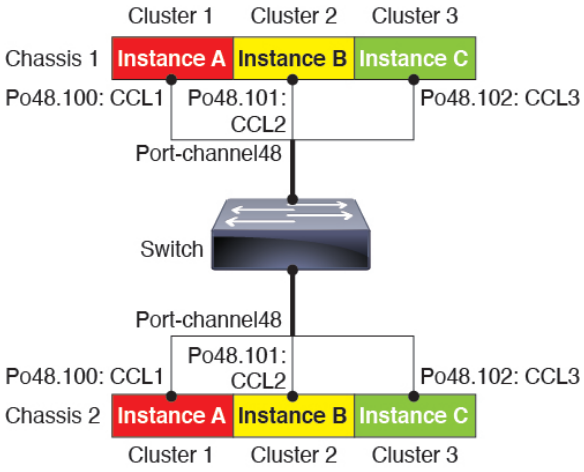
- 混合和匹配集群和独立实例 - 并非安全模块/引擎上的所有容器实例都需要属于集群。可以将某些实例用作独立节点或高可用性节点。还可以在同一安全模块/引擎上使用单独的实例来创建多个集群。



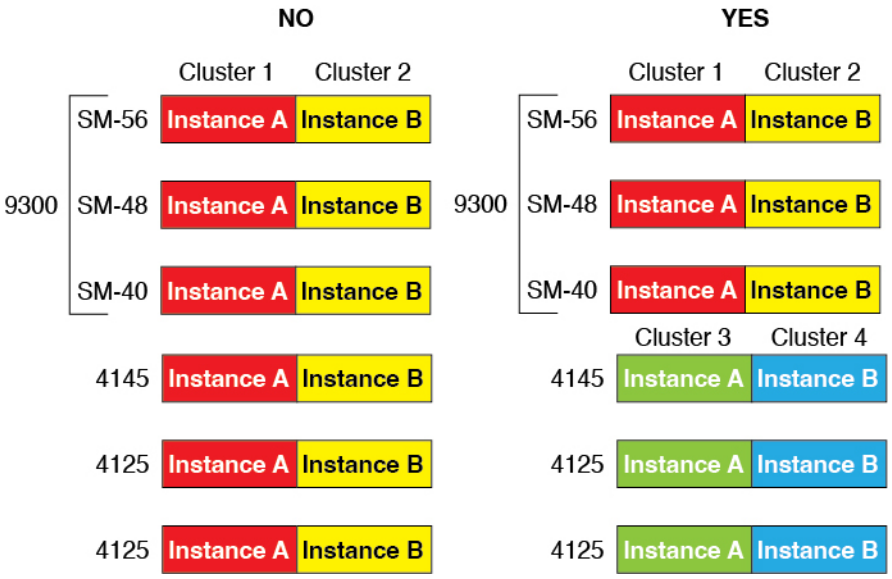
- Firepower 9300 中的所有 3 个模块都必须属于集群 - 对于 Firepower 9300，集群要求所有 3 个模块上都有一个容器实例。例如，不能使用模块 1 和 2 上的实例来创建集群，然后在模块 3 中使用本地实例。

- 匹配资源配置文件 - 建议集群中的每个节点都使用相同的资源配置文件属性；但是，在将集群节点更改为使用其他资源配置文件或使用不同型号时，允许使用不匹配的资源。

- 专用集群控制链路 - 对于具有多个机箱的集群，每个集群都需要专用的集群控制链路。例如，每个集群可以在同一集群类型 EtherChannel 上使用单独的子接口，也可以使用单独的 Etherchannel。



- 无共享接口 - 集群不支持共享类型接口。但是，多个集群可以使用相同的管理接口和事件接口。
- 无子接口 - 多实例集群无法使用 FXOS 定义的 VLAN 子接口。集群控制链路例外，它可以使用集群 EtherChannel 的子接口。
- 混合机箱型号 - 建议您为每个集群实例使用相同的安全模块或机箱模型。但是，如果需要，您可以在同一集群中的不同 Firepower 9300 安全模块类型或 Firepower 4100 型号上混合和匹配容器实例。不能在同一个集群中混合使用 Firepower 9300 和 Firepower 4100。例如，您可以使用 Firepower 9300 SM-56、SM-48 和 SM-40 上的实例创建集群。或者，您可以在 Firepower 4145 和 4125 上创建集群。



- 最多 6 个节点 - 在一个集群中最多可以使用六个容器实例。

交换机要求

- 请务必先完成交换机配置并将机箱中的所有 EtherChannel 成功连接至交换机后，再在 Firepower 4100/9300 机箱 上配置集群。
- 有关受支持的交换机的特性，请参阅思科 FXOS 兼容性。

逻辑设备的准则和限制

有关准则和限制，请参阅以下章节。

接口的准则和限制

VLAN 子接口

- 本文档仅讨论 *FXOS* VLAN 子接口。您还可以在 Firewall Threat Defense 应用内单独创建子接口。有关详细信息，请参阅FXOS 接口与应用接口，第 4 页。
- 子接口（和父接口）仅可分配至容器实例。

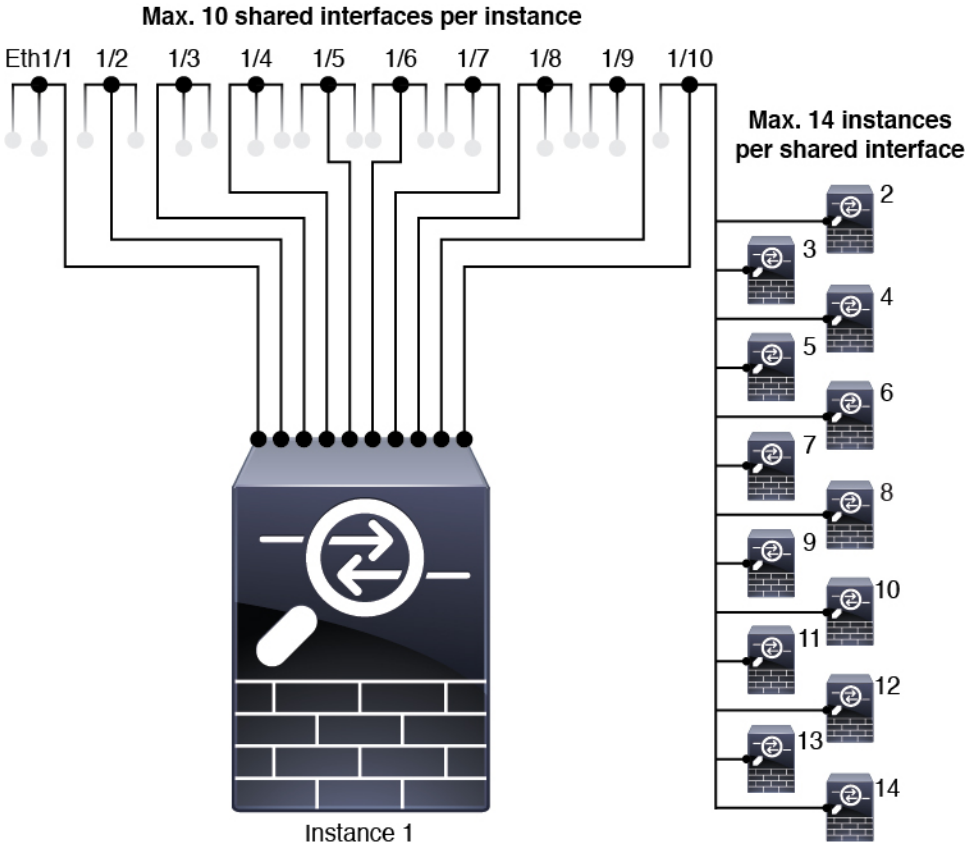
注释 如果将父接口分配至容器实例，该接口将仅传递未标记（非 VLAN）流量。除非您想要传递未标记流量，否则不予分配父接口。对于集群类型接口，不得使用父接口。

- 子接口在数据或数据共享型接口以及集群类型接口上受支持。如果向某个集群接口添加子接口，则不能将该接口用于本地集群。
- 对于多实例集群，数据接口上不支持 FXOS 子接口。但是，集群控制链路支持子接口，因此可以将专用 EtherChannel 或 EtherChannel 子接口用于集群控制链路。请注意，数据接口支持 应用定义的子接口。
- 最多可以创建 500 个 VLAN ID。
- 请参阅逻辑设备应用中的以下限制；规划接口分配时，请谨记这些限制。
  - 不得将子接口用于 Firewall Threat Defense 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。

数据共享接口

- 不得结合使用数据共享接口和本地实例。
- 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。



- 不得在集群中使用数据共享接口。
- 请参阅逻辑设备应用中的以下限制；规划接口分配时，请谨记这些限制。
  - 不得结合使用数据共享接口和透明防火墙模式设备。
  - 不得结合数据共享接口和 Firewall Threat Defense 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。

FTD 的内联集 Firewall Threat Defense

- 支持物理接口（常规端口和分支端口）和 Etherchannel。 不支持子接口。
- 支持链路状态传播。
- 请勿为同一内联集启用 硬件旁路 和传播链路状态。

硬件旁路

- 支持 Firewall Threat Defense；可以将它们用作 ASA 的常规接口。

- Firewall Threat Defense仅支持包含内联集的 硬件旁路。
- 不可为分支端口配置具有硬件旁路功能的接口。
- 不得包含 EtherChannel 中的硬件旁路接口包含在并将它们用于硬件旁路；可以将它们用作 EtherChannel 中的常规接口。
- 硬件旁路不支持高可用性。
- 请勿为同一内联集启用 硬件旁路 和传播链路状态。

默认 MAC 地址

对于本地实例：

默认 MAC 地址分配取决于接口类型。

- 物理接口 - 物理接口使用已刻录的 MAC 地址。
- EtherChannel - 对于 EtherChannel，属于通道组的所有接口共用同一个 MAC 地址。此功能使 EtherChannel 对网络应用和用户透明，因为他们只看到一个逻辑连接；而不知道各个链路。端口通道接口使用来自池中的唯一 MAC 地址；接口成员身份不影响 MAC 地址。

对于容器实例：

- 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。请参阅容器实例接口的自动 MAC 地址，第 26 页。

一般准则和限制

防火墙模式

您可以在 防火墙威胁防御 的引导程序配置中将防火墙模式设置为路由或透明模式。

高可用性

- 在应用配置中配置高可用性。
- 可以将任何数据接口用作故障转移和状态链路。 不支持数据共享接口。

多实例

- 包含容器实例的多实例功能仅适用于使用 防火墙管理中心 的 防火墙威胁防御。
- 对于 防火墙威胁防御 容器实例，单个 防火墙管理中心必须管理安全模块/引擎上的所有实例。
- 对于 防火墙威胁防御 容器实例，不支持以下功能：
  - Radware DefensePro 链路修饰器

- 防火墙管理中心 UCAPL/CC 模式
- 到硬件的数据流分流

配置接口

默认情况下，物理接口处于禁用状态。可以启用接口，添加 Etherchannel，添加 VLAN 子接口，编辑接口属性。

启用或禁用接口

可以将每个接口的**管理状态**更改为启用或禁用。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 选择**接口 (Interfaces)** 打开接口页面。

“接口 (Interfaces)”页面顶部显示当前已安装的接口的直观展示图，在下表中提供已安装接口列表。

步骤 2 要启用接口，请点击已禁用**滑块已禁用**（  ），使其更改为已启用**滑块已启用**（  ）。

点击**是**，确认更改。以直观展示图表现的对应接口从灰色变为绿色。

步骤 3 要禁用接口，请点击已启用**滑块已启用**（  ），使其更改为已禁用**滑块已禁用**（  ）。

点击**是**，确认更改。以直观展示图表现的对应接口从绿色变为灰色。

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。要使用某一接口，必须在 FXOS 中以物理方式启用它，并在应用中以逻辑方式启用它。

注释

- 对于 QSFPH40G-CUxM，默认情况下自动协商会始终处于启用状态，并且您无法将其禁用。
- 如果使用其他 SFP 模块替换端口上的 SFP，则该接口的速度、双工和自动协商不会自动更新。您必须手动重新配置该接口。

开始之前

- 不能单独修改已经是 EtherChannel 成员的接口。务必在将接口添加到 EtherChannel 之前为其配置设置。

过程

步骤 1 选择**接口 (Interfaces)** 打开“接口”(Interfaces) 页面。

所有接口页面顶部显示当前已安装的接口的直观展示图，在下表中提供已安装接口列表。

步骤 2 在您要编辑的接口所对应的行中点击**编辑 (Edit)**，可打开**编辑接口 (Edit Interface)** 对话框。

步骤 3 要启用接口，请选中**启用**复选框。要禁用接口，请取消选中**启用**复选框。

步骤 4 选择接口**类型**：

有关接口类型使用的详细信息，请参阅接口类型，第 2 页。

- **数据**
- **数据共享** - 仅用于容器实例。
- **管理**
- **Firepower 事件** - 仅用于 Firewall Threat Defense 。
- **集群** - 请勿选择**集群**类型；默认情况下，系统会自动在端口通道 48 上创建集群控制链路。

步骤 5 （可选） 从**速度 (Speed)** 下拉列表中选择接口的速度。

步骤 6 （可选） 如果您的接口支持**自动协商**，请点击**是 (Yes)** 或**否 (No)** 单选按钮。

如果通过 50G 电缆连接到端口的对等交换机不支持自动协商，请确保同时在交换机和平台接口上禁用自动协商。例如，N9K-C93400LD-H1 不支持在 50G 电缆上进行自动协商。因此，要连接端口，必须在平台和交换机上禁用默认自动协商。

步骤 7 （可选） 从**双工 (Duplex)** 下拉列表中选择接口双工。

步骤 8 （可选） 明确配置**防反跳时间 (ms)**。输入 0-15000 毫秒之间的值。

注释
不支持在 1G 接口上配置防反跳时间。

步骤 9 点击**确定**。

添加 EtherChannel（端口通道）

EtherChannel（也称为端口通道）最多可以包含 16 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。不能通过在大容量接口上将速度设置为较低值来混合接口容量（例如 1GB 和 10GB 接口）。链路聚合控制协议 (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。

您可以将 EtherChannel 中的每个物理数据或数据共享接口配置为：

- Active - 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。

非数据接口仅支持主用模式。

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。

Firepower 4100/9300 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。EtherChannel 在以下情况下将退出**挂起**状态：

- 将 EtherChannel 添加为独立逻辑设备的数据或管理端口
- 将 EtherChannel 添加为属于集群一部分的逻辑设备的管理接口或集群控制链路
- 将 EtherChannel 添加为属于集群一部分的逻辑设备的数据端口，并且至少有一个单元已加入该集群

请注意，EtherChannel 在您将它分配到逻辑设备前不会正常工作。如果从逻辑设备移除 EtherChannel 或删除逻辑设备，EtherChannel 将恢复为**挂起**或**关闭**状态。

过程

步骤 1 选择**接口 (Interfaces)** 打开“接口”(Interfaces) 页面。

所有接口页面顶部显示当前已安装的接口的直观展示图，在下表中提供已安装接口列表。

步骤 2 点击接口表上方的**添加端口通道 (Add Port Channel)**，可打开**添加端口通道 (Add Port Channel)** 对话框。

步骤 3 在**端口通道 ID (Port Channel ID)** 字段中输入端口通道 ID。有效值介于 1 与 47 之间。

部署集群逻辑设备时，端口通道 48 为集群控制链路预留。如果不想将端口通道 48 用于集群控制链路，可以将其删除并为集群类型 EtherChannel 配置不同的 ID。您可以添加多个集群类型 Etherchannel，

并添加 VLAN 子接口以与多实例集群结合使用。对于机箱内集群，请不要将任何接口分配给集群 EtherChannel。

步骤 4 要启用端口通道，请选中**启用**复选框。要禁用端口通道，请取消选中**启用**复选框。

步骤 5 选择接口**类型**：

有关接口类型使用的详细信息，请参阅接口类型，第 2 页。

- **数据**
- **数据共享** - 仅用于容器实例。
- **管理**
- **Firepower 事件** - 仅用于 Firewall Threat Defense 。
- **集群**

步骤 6 从下拉列表设置成员接口要求的**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。

步骤 7 对于数据或数据共享接口，选择 LACP 端口通道**模式**、**主用**或**保持**。

对于非数据或数据共享接口，模式始终是主用模式。

步骤 8 为成员接口、**全双工**或**半双工**设置所需的**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。

步骤 9 要将接口添加到端口通道，请在**可用接口 (Available Interface)** 列表中选择该接口，点击**添加接口 (Add Interface)**，将接口移动至“成员 ID”列表。

您最多可以添加相同介质类型和容量的16个成员接口。成员接口必须设置为相同的速度和双工，并且必须与您为此端口通道配置的速度和双工相匹配。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。不能通过在大容量接口上将速度设置为较低值来混合接口容量（例如 1GB 和 10GB 接口）。

提示
一次可添加多个接口。要选择多个独立接口，请点击所需的接口，同时按住 **Ctrl** 键。要选择一个接口范围，请选择范围中的第一个接口，然后，在按住 **Shift** 键的同时，点击选择范围中的最后一个接口。

步骤 10 要从端口通道删除接口，请点击“成员 ID”(Member ID) 列表中接口右侧的**删除 (Delete)** 按钮。

步骤 11 点击**确定**。

为容器实例添加 VLAN 子接口

您可以向机箱添加 250 至 500 个 VLAN 子接口，具体取决于网络部署。您最多可以将 500 个子接口连接到您的机箱。

对于多实例集群，只能将子接口添加到集群类型接口；不支持数据接口上的子接口。

每个接口的 VLAN ID 都必须具有唯一性，并且在容器实例内，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 分配至不同的容器实例，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。

本文档仅讨论 *FXOS* VLAN 子接口。您还可以在 Firewall Threat Defense 应用内单独创建子接口。有关何时使用 FXOS 子接口与应用子接口的详细信息，请参阅FXOS 接口与应用接口，第 4 页。

过程

步骤 1 选择**接口 (Interfaces)**打开**所有接口 (All Interfaces)**选项卡。

页面顶部的**所有接口 (All Interfaces)** 选项卡显示当前已安装的接口的直观展示图，并在下表中提供已安装接口列表。

步骤 2 点击**添加新 (Add New)** > **子接口 (Subinterface)**打开**添加子接口 (Add Subinterface)** 对话框。

步骤 3 选择接口**类型**：

有关接口类型使用的详细信息，请参阅接口类型，第 2 页。

- **数据**
- **数据共享**
- **集群** - 如果向某个集群接口添加子接口，则不能将此接口用于本地集群。

对于数据和数据共享接口：此类型独立于父接口类型；例如，您可以设数据共享父接口和数据子接口。

步骤 4 从下拉列表选择父**接口**。

不得将子接口添加到当前已分配至逻辑设备的物理接口。如果系统已分配父接口的其他子接口，只要未分配此父接口，您就可以添加新的子接口。

步骤 5 输入一个介于 1 和 4294967295 之间的**子接口 ID**。

此 ID 将附加到父接口 ID，作为 *interface_id.subinterface_id*。例如，如果您将子接口添加到 ID 为 100 的以太网接口 1/1，则子接口 ID 将为：以太网接口 1/1.100。尽管可以出于方便目的将此 ID 和 VLAN ID 设置为相互匹配，但两者始终不同。

步骤 6 设置介于 1 和 4095 之间的 **VLAN ID** 。

步骤 7 点击**确定**。

展开父接口查看其项下所有子接口。

配置逻辑设备

在 Firepower 4100/9300上添加独立逻辑设备或高可用性对。

有关集群，请参阅用于 Firepower 4100/9300 的集群。

为容器实例添加资源配置文件

要指定每个容器实例的资源使用情况，请创建一个或多个资源配置文件。部署逻辑设备/应用实例时，请指定想要使用的资源配置文件。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。

- 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安全模块/机箱型号，请参阅容器实例的要求和前提条件，第 30 页。

机箱包括一个命名为 "Default-Small" 的默认资源配置文件，此文件包括最小核心数。您可以更改此配置文件定义，甚至可在未使用情况下将其删除。请注意，此配置文件在机箱重新加载且系统上不存在任何其他配置文件时创建而成。

在分配资源配置文件后更改资源配置文件会造成中断。请参阅以下准则：

- 如果当前正在使用，则无法更改资源配置文件设置。必须禁用使用此文件的任何实例，然后更改资源配置文件，最后重新启用该实例。
- 如果在将 防火墙威胁防御 实例添加到 防火墙管理中心 后更改资源配置文件设置，稍后应在设备设备管理设备系统清单对话框上更新每个设备的清单。防火墙管理中心选择 **设备** > **设备管理**，点击**编辑** (✎)实例的，然后点击**刷新** (↻)**设备** > **清单详细信息**区域。
- 如果将其他配置文件分配给实例，它会重新启动。
- 如果将不同的配置文件分配给已建立的高可用性对中的实例，这要求两台设备上的配置文件相同，则必须：
  1. 中断高可用性。
  2. 将新配置文件分配给两台设备。
  3. 重新建立高可用性。

- 如果将不同的配置文件分配给已建立的集群中的实例，则允许不匹配的配置文件，则首先在数据节点上应用新的配置文件；全部恢复后，您可以将新的配置文件应用到控制节点。

过程

步骤 1 选择**平台设置 (Platform Settings)** > **资源配置文件 (Resource Profiles)**，然后点击**添加 (Add)**。

系统将显示**添加资源配置文件**对话框。

步骤 2 设置以下参数。

- **Name** - 设置介于 1 和 64 个字符之间的配置文件名称。请注意，此配置文件名称添加后无法更改。
- **Description** - 设置最多 510 个字符的配置文件说明。
- **Number of Cores** - 设置介于 6 和最大值之间的配置文件核心数（偶数），具体取决于机箱。

步骤 3 点击**确定**。

为 防火墙管理中心

独立逻辑设备可单独使用，也可在高可用性对中使用。在具有多个安全模块的 Firepower 9300 上，可以配置集群或独立设备。集群必须使用所有模块，因此无法将双模块集群和独立设备进行混用和搭配。

可以在某些模块上使用本地实例，在其他模块上使用容器实例。

开始之前

- 从 Cisco.com 下载要用于逻辑设备的应用映像，然后将映像上传到 Firepower 4100/9300。

注释 对于 Firepower 9300，可以在机箱中的独立模块上安装不同类型的应用（ASA 和 Firewall Threat Defense）。还可以在独立模块上运行一种应用实例的不同版本。

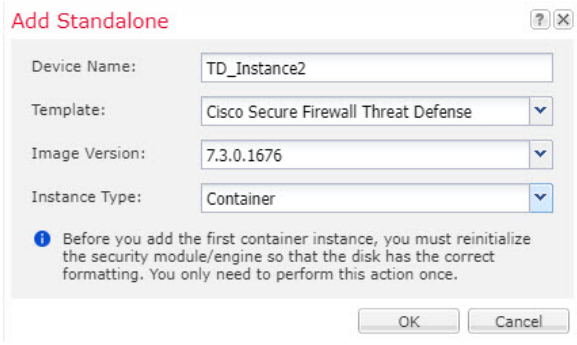
- 配置逻辑设备要使用的管理接口。管理接口是必需的。请注意，此管理接口不同于仅用于机箱管理的机箱管理端口 （并且在**接口**选项卡的顶部显示为 **MGMT**）。
- 您可以稍后从数据接口启用管理；但必须将管理接口分配给逻辑设备，即使您不打算在启用数据管理后使用该接口。有关详细信息，请参阅 FTD 命令参考中的 **configure network management-data-interface** 命令。

- 您还必须至少配置一个数据类型的接口。或者，您也可以创建Firepower事件接口，传输所有事件流量（例如 Web 事件）。有关详细信息，请参阅接口类型，第 2 页。
- 对于容器实例，如果您不想使用默认配置文件，则请根据为容器实例添加资源配置文件，第43页添加资源配置文件。
- 对于容器实例，在首次安装容器实例之前，必须重新初始化安全模块/引擎，以保证磁盘具有正确的格式。选择**安全模块**或**安全引擎**，然后点击**重新初始化图标**。首先删除现有逻辑设备，然后将其重新安装为新设备，这会丢失任何本地应用配置。如果要使用容器实例替换本地实例，则在任何情况下都需要删除本地实例。无法自动将本地实例迁移到容器实例。
- 收集以下信息：
  - 此设备的接口 ID
  - 管理接口 IP 地址和网络掩码
  - 网关 IP 地址
  - 您选择的防火墙管理中心 IP 地址和/或 NAT ID
  - DNS 服务器 IP 地址
  - 防火墙威胁防御 主机名和域名

过程

步骤 1 选择**逻辑设备**。

步骤 2 点击**添加** > **独立设备**，并设置以下参数：



a) 提供**设备名称**。

此名称由机箱管理引擎用于配置管理设置和分配接口；它不是在应用配置中使用的设备名称。

注释
添加逻辑设备后，无法更改此名称。

b) 对于**模板**，请选择 **Cisco Firepower Threat Defense**。

c) 选择**映像版本**。

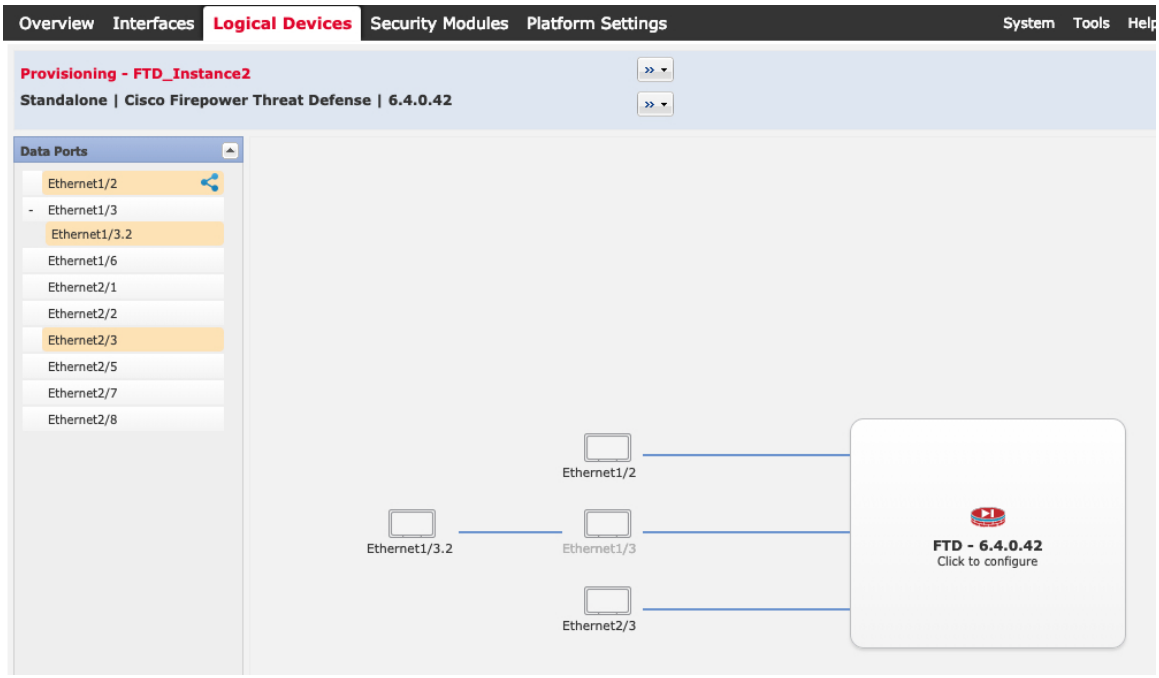
d) 选择**实例类型：容器**或**本地**。

本地实例使用安全模块/引擎的所有资源（CPU、RAM和磁盘空间），因此仅可安装一个本地实例。容器实例使用部分安全模块/引擎资源，因此可以安装多个容器实例。

e) 点击**确定**。

屏幕会显示调配 - 设备名称窗口。

步骤 3 展开**数据端口 (Data Ports)** 区域，然后点击要分配给设备的每个接口。



您仅可分配先前在接口 (Interfaces) 页面上启用的数据**和数据共享**接口。稍后您需要在 防火墙管理中心 中启用和配置这些接口，包括设置 IP 地址。

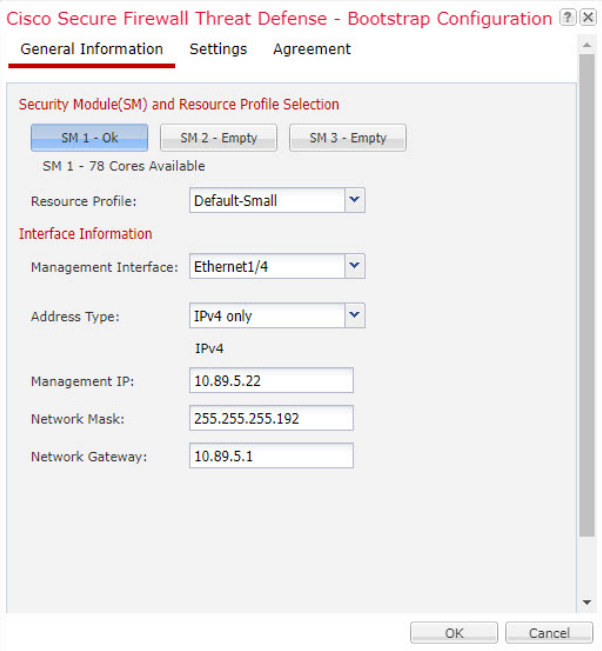
仅可向一个容器实例分配最多 10 个数据共享接口。此外，可以将每个数据共享接口分配至最多 14 个容器实例。数据共享接口以共享图标（ ） 表示。

具有硬件旁路功能的端口使用以下图标显示： 。对于某些接口模块，仅可启用用于内联集接口的硬件旁路功能（请参阅 防火墙管理中心配置指南）。硬件绕行确保流量在断电期间继续在接口对之间流动。在软件或硬件发生故障时，此功能可用于维持网络连接性。如果您未同时分配一个硬件旁路对中的两个接口，则会收到一条警告消息，确认您是故意这样分配。您不需要使用硬件旁路功能，因此如果您愿意，可以分配单个接口。

步骤 4 点击屏幕中心的设备图标。

系统将显示对话框，可以在该对话框中配置初始引导程序设置。这些设置仅用于仅初始部署或灾难恢复。为了实现正常运行，稍后可以更改应用 CLI 配置中的大多数值。

步骤 5 在**一般信息 (General Information)** 页面上，完成下列操作：



a) （对于 Firepower 9300）在**安全模块选择**下，点击您想用于此逻辑设备的安全模块。

b) 对于容器实例，指定**资源配置文件**。

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。

注释
如果稍后将不同的配置文件分配给已建立的高可用性对中的实例，这要求两台设备上的配置文件相同，则必须：

1. 中断高可用性。
2. 将新配置文件分配给两台设备。
3. 重新建立高可用性。

c) 选择**管理接口**。

此接口用于管理逻辑设备。此接口独立于机箱管理端口。

d) 选择管理接口**地址类型**：**仅 IPv4**、**仅 IPv6** 或 **IPv4 和 IPv6**。

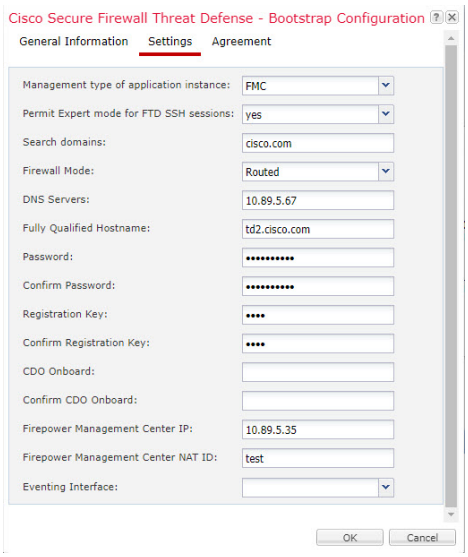
e) 配置**管理 IP** 地址。

设置用于此接口的唯一 IP 地址。

f) 输入**网络掩码**或**前缀长度**。

g) 输入**网络网关**地址。

步骤 6 在**设置**选项卡上，完成下列操作：



a) 对于本地实例，在**应用实例的管理类型**下拉列表中，选择 **FMC**。

本地实例还支持 防火墙设备管理器 作为管理器。部署逻辑设备后，无法更改管理器类型。

b) 输入管理 防火墙管理中心 的 **Firepower 管理中心 IP**。如果您不知道 防火墙管理中心 IP 地址，请将此字段留空，并在 **Firepower 管理中心 NAT ID (Firepower Management Center NAT ID)** 字段中输入口令。

c) 对于容器实例，选择**是否允许 FTD SSH 会话专家模式：是** 或**否**。专家模式提供 防火墙威胁防御 shell 访问权限以确保实现高级故障排除。

对于此选项，如果您选择**是**，拥有直接从 SSH 会话访问容器实例的权限的用户可以输入专家模式。如果您选择**否**，只有拥有从 FXOS CLI 访问容器实例的权限的用户可以输入专家模式。我们建议选择**否**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 防火墙威胁防御 CLI 中使用 **expert** 命令。

d) 输入逗号分隔列表形式的**搜索域**。

e) 选择**防火墙模式：透明**或**路由式**。

在路由模式中，防火墙威胁防御被视为网络中的路由器跃点。要在其间路由的每个接口都位于不同的子网上。另一方面，透明防火墙是一个第 2 层防火墙，充当“线缆中的块”或“隐蔽的防火墙”，不被视为是到所连接设备的路由器跃点。

系统仅在初始部署时设置防火墙模式。如果您重新应用引导程序设置，则不会使用此设置。

f) 输入逗号分隔列表形式的 **DNS 服务器**。

例如，如果指定 防火墙管理中心 主机名，则 防火墙威胁防御 使用 DNS。

g) 输入 防火墙威胁防御 的**完全限定主机名**。

h) 输入注册期间要在防火墙管理中心和设备之间共享的**注册密钥**。

可以为此密钥选择介于 1 至 37 个字符之间的任何文本字符串；添加防火墙威胁防御时，需要在防火墙管理中心上输入相同的密钥。

i) 输入供防火墙威胁防御管理员用户用于 CLI 访问的**密码**。

j) 选择应该发送事件的**事件接口**。如果未指定，系统将使用管理接口。

此接口必须定义为 Firepower 事件接口。

k) 对于容器实例，请将**硬件加密**设置为**已启用**或**已禁用**。

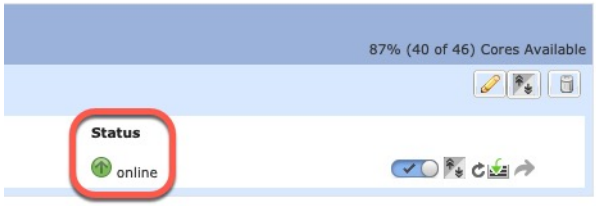
此设置在硬件中启用 TLS 加密加速，并提高某些类型流量的性能。默认情况下启用此功能。您最多可以为每个安全模块的 16 个实例启用 TLS 加密加速。始终为本地实例启用此功能。要查看分配给该实例的硬件加密资源百分比，请输入 **show hw-crypto** 命令。

步骤 7 在**协议**选项卡上，阅读并接受最终用户许可协议 (EULA)。

步骤 8 点击**确定 (OK)** 关闭配置对话框。

步骤 9 点击**保存 (Save)**。

机箱通过下载指定软件版本，并将引导程序配置和管理接口设置推送至应用实例来部署逻辑设备。在**逻辑设备 (Logical Devices)** 页面中，查看新逻辑设备的状态。当逻辑设备将其**状态**显示为**在线**时，可以开始在应用中配置安全策略。



步骤 10 请参阅 防火墙管理中心 配置指南，将 防火墙威胁防御 添加为托管设备，并开始配置安全策略。

添加高可用性对

Firewall Threat Defense 高可用性（也称为故障转移）是在应用中配置，而不是在 FXOS 中配置。但为了让您的机箱做好配置高可用性的准备，请参阅以下步骤。

开始之前

请参阅高可用性的要求和前提条件，第 31 页。

过程

步骤 1 将相同的接口分配给各个逻辑设备。

步骤 2 为故障转移和状态链路分配 1 个或 2 个数据接口。

这些接口用于交换 2 个机箱之间的高可用性流量。我们建议您将一个 10 GB 数据接口用于组合的故障转移和状态链路。如果您有可用的接口，可以使用单独的故障转移和状态链路；状态链路需要的带宽最多。不能将管理类型的接口用于故障转移或状态链路。我们建议您在机箱之间使用一个交换机，并且不将同一网段中的其他任何设备作为故障转移接口。

对于容器实例，故障转移链路不支持数据共享接口。我们建议您在父接口或 EtherChannel 上创建子接口，并为每个实例分配子接口以用作故障转移链路。请注意，您必须将同一父接口上的所有子接口用作故障转移链路。不得将一个子接口用作故障转移链路，然后将其他子接口（或父接口）用作常规数据接口。

步骤 3 在逻辑设备上启用高可用性。请参阅设备的高可用性。

步骤 4 如果您在启用高可用性后需要更改接口，请先在备用设备上执行更改，然后再在主用设备上执行更改。

更改Firewall Threat Defense逻辑设备上的接口

可以在 Firewall Threat Defense 逻辑设备上分配或取消分配接口，或者替换管理接口。然后，您可以在 防火墙管理中心 中同步接口配置。

添加新接口或删除未使用接口对 Firewall Threat Defense 配置的影响最小。但是，删除安全策略中使用的接口会影响配置。可以直接在 Firewall Threat Defense 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。引用安全区的策略不受影响。还可以编辑已分配的 EtherChannel 的成员关系，而不影响逻辑设备或要求在 防火墙管理中心 上进行同步。

删除接口将删除与该接口相关的任何配置。

开始之前

- 根据配置物理接口，第 38 页和添加 EtherChannel（端口通道），第 39 页配置您的接口，并添加任何 EtherChannel。
- 如果您要将已分配的接口添加到 EtherChannel（例如，默认情况下将所有接口分配给集群），则需要先从逻辑设备取消分配接口，然后再将该接口添加到EtherChannel。对于新的EtherChannel，您可以随后将 EtherChannel 分配到设备。
- 如果要将管理或事件接口替换为管理 EtherChannel，则需要创建至少具有 1 个取消分配数据成员接口的 EtherChannel，然后将当前管理接口替换为 EtherChannel。Firewall Threat Defense 重新启动（管理接口更改导致重新启动），并且在防火墙管理中心中同步配置后，还可以将（目前取消分配的）管理接口添加到 EtherChannel。
- 对于集群或高可用性，请确保在所有设备上添加或删除该接口，然后在防火墙管理中心中同步配置。我们建议先在数据/备用设备上更改接口，然后再在控制/主用设备上更改接口。请注意，新的接口在管理权限关闭的状态下添加，因此，它们不会影响接口监控。

- 在多实例模式下，要更改具有相同 vlan 标记的另一个子接口的子接口，必须先删除该接口的所有配置（包括 nameif config），然后从 防火墙机箱管理器取消分配该接口。取消分配后，添加新接口，然后使用 防火墙管理中心中的同步接口。

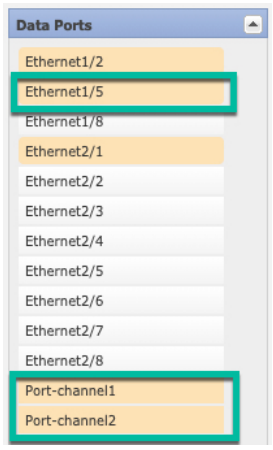
过程

步骤 1 在 防火墙机箱管理器中，选择**逻辑设备**。

步骤 2 点击右上角的**编辑**图标以编辑逻辑设备。

步骤 3 通过在**数据端口**区域中选择新的数据接口来分配该接口。

请勿删除任何接口。



步骤 4 替换管理或事件接口：

对于这些类型的接口，在您保存更改后，设备会重新启动。

a) 点击页面中心的设备图标。
b) 在**常规**或**集群信息**选项卡上，从下拉列表中选择新的**管理接口**。
c) 在**设置**选项卡上，从下拉列表中选择新的**事件接口**。
d) 点击**确定**。

如果更改管理接口的 IP 地址，则还必须更改 防火墙管理中心中设备的 IP 地址：转到**设备** > **设备管理** > **设备/集群**。在**管理**区域中，设置 IP 地址以匹配引导程序配置地址。

步骤 5 点击**保存**。

步骤 6 同步 防火墙管理中心 中的接口。

a) 登录至防火墙管理中心。
b) 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并点击 Firewall Threat Defense 设备的**编辑**（）。系统默认选择**接口 (Interfaces)** 页面。
c) 点击**接口 (Interfaces)** 页面左上方的**同步设备 (Sync Device)** 按钮。
d) 检测到更改后，可以在**接口 (Interfaces)** 页面上看到红色横幅，表明接口配置已发生更改。点击**点击了解详细信息**链接以查看接口更改。

e) 如果计划删除接口，请手动将任何接口配置从旧接口传输至新接口。

由于尚未删除任何接口，因此可以引用现有配置。在删除旧接口并重新运行验证后，将有额外的机会来修复配置。验证将显示仍在使用旧接口的所有位置。

f) 点击**验证更改 (Validate Changes)** 以确保策略在接口更改后仍有效。

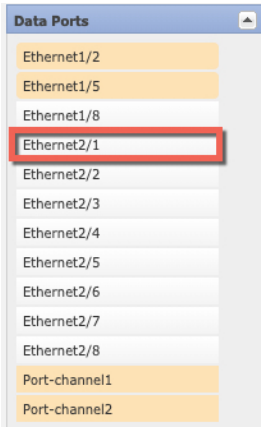
如出现任何错误，则需要更改配置并重新运行验证。

g) 点击**保存 (Save)**。

h) 依次点击**部署** > **部署**。

i) 选择设备然后点击**部署**，以将策略部署到所分配的设备。在部署更改之后，更改才生效。

步骤 7 在 防火墙机箱管理器 中，通过在**数据端口 (Data Ports)** 区域中取消选择数据接口来取消分配该接口。



步骤 8 点击**保存**。

步骤 9 再次在 防火墙管理中心 中同步接口。

连接到应用控制台

使用以下程序连接至应用的控制台。

过程

步骤 1 使用控制台连接或 Telnet 连接来连接至模块 CLI。

connect module *slot_number* {**console** | **telnet**}

要连接至不支持多个安全模块的设备的安全引擎，请使用 **1** 作为 *slot_number*。

使用 Telnet 连接的优点在于，您可以同时对模块开展多个会话，并且连接速度更快。

示例：

```
Firepower# 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

Firepower-module1>
```

步骤 2 连接到应用控制台。

connect ftd *name*

要查看实例名称，请输入不含名称的命令。

示例：

```
Firepower-module1> connect ftd ftd1
Connecting to ftd(ftd-native) console... enter exit to return to bootCLI
[...]
>
```

步骤 3 退出应用控制台到 FXOS 模块 CLI。

- Firewall Threat Defense - 输入 **exit**

步骤 4 返回 FXOS CLI 的管理引擎层。

退出控制台：

a) 输入 **~**

您将退出至 Telnet 应用。

b) 要退出 Telnet 应用，请输入：

telnet>**quit**

退出 Telnet 会话：

a) 输入 **Ctrl-],**。

逻辑设备的历史记录

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
Firewall Threat Defense 运行链路状态与物理链路状态之间的同步	6.7	任意	机箱现在可以将 Firewall Threat Defense 运行链路状态与数据接口的物理链路状态同步。目前，只要 FXOS 管理状态为“运行”且物理链路状态为“运行”，接口将处于“运行”状态，而不考虑 Firewall Threat Defense 应用接口管理状态。如果没有从 Firewall Threat Defense同步，数据接口可能在 Firewall Threat Defense 应用完全上线之前处于“Up”物理状态，或者在您启动 Firewall Threat Defense 关闭后的一段时间内保持 “Up”状态。对于内联集，此状态不匹配可能会导致数据包丢失，因为外部路由器可能会在 Firewall Threat Defense 可以处理流量之前开始向 Firewall Threat Defense 发送流量。该功能默认为禁用状态并可在 FXOS 中按逻辑设备逐一启用。 **注释** 集群、容器实例或具有 Radware vDP 修饰器的 Firewall Threat Defense 不支持此功能。此外，ASA 也不支持此功能。 新增/修改的 Firepower 机箱管理器屏幕：**逻辑设备** > **启用链路状态** 新增/修改的 FXOS 命令：**set link-state-sync enabled**、**show interface expand detail**
对容器实例使用防火墙管理中心 的 Firewall Threat Defense 配置备份和恢复	6.7	任意	您现在可以在 Firewall Threat Defense 容器实例上使用 防火墙管理中心 备份/恢复工具。 新增/修改的 防火墙管理中心 屏幕：**系统** > **工具** > **备份/恢复** > **托管设备备份** 新增/修改的 Firewall Threat Defense CLI 命令：**restore** 支持的平台：Firepower 4100/9300 **注释** 需要 FXOS 2.9。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
支持集群类型接口上的VLAN子接口（仅限多实例使用）	6.6	任意	要与多实例集群配合使用，您现在可以在集群类型接口上创建VLAN子接口。由于每个集群都需要唯一的集群控制链路，因此VLAN子接口提供了一种可满足此要求的简单方法。您也可以为每个集群分配专用的EtherChannel。现在允许多个集群接口。 新增/修改的 Firepower 机箱管理器菜单项： **接口** > **所有接口** > **新增**下拉菜单**子接口** > **类型**字段 新增/修改的 FXOS 命令：**set port-type cluster** **注释** 需要 FXOS 2.8.1。
Firepower 4112 上的 Firewall Threat Defense	6.6	任意	我们推出了 Firepower 4112。 **注释** 需要 FXOS 2.8.1。
多个容器实例的TLS加密加速	6.5	任意	现在，在Firepower 4100/9300 机箱上的多个容器实例（最多16个）上支持 TLS 加密加速。以前，每个模块/安全引擎只能为一个容器实例启用 TLS 加密加速。 新实例默认启用此功能。但是，升级不会在现有实例上启用加速。相反，请依次使用 **enter hw-crypto** 和 **set admin-state enabled** FXOS 命令。 新增/修改的 Firepower 机箱管理器菜单项： **逻辑设备** > **添加设备** > **设置** > **硬件加密**下拉菜单 **注释** 需要 FXOS 2.7.1。
Firewall Threat Defense（位于 Firepower 4115、4125 和 4145 上）	6.4	任意	我们推出了 Firepower 4115、4125 和 4145。 **注释** 需要 FXOS 2.6.1.157。
Firepower 9300 SM-40、SM-48 和 SM-56 支持	6.4	任意	引入了以下三个安全模块：SM-40、SM-48 和 SM-56。 **注释** 需要 FXOS 2.6.1.157。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
支持在同一个Firepower 9300 上使用独立的 ASA 和 Firewall Threat Defense 模块	6.4	任意	您现在可以在同一个 Firepower 9300 上同时部署 ASA 和 Firewall Threat Defense 逻辑设备。 注释 需要 FXOS 2.6.1.157。
支持将SSL硬件加速用于模块/安全引擎上的一个 Firewall Threat Defense 容器实例	6.4	任意	您现在可以启用用于模块/安全引擎上的一个容器实例的SSL硬件加速。SSL 硬件加速禁用于其他容器实例，但启用于本地实例。 新增/修改的 FXOS 命令：**config hwCrypto enable** 未修改任何屏幕。 注释 需要 FXOS 2.6.1.157。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
Firepower 4100/9300 上 Firewall Threat Defense 的多实例功能	6.3	任意	您现在可以在单个安全引擎/模块上部署多个逻辑设备，每台逻辑设备都设 Firewall Threat Defense 容器实例。以前，您仅可部署单个本地应用实例。 要确保灵活使用物理接口，可以在 FXOS 中创建 VLAN 子接口，还可以在多个实例之间共享接口。资源管理允许您自定义每个实例的性能。 您可以使用在 2 个独立机箱上使用一个容器实例的高可用性。不支持集群。 注释 尽管实现方式不同，但多实例功能与 ASA 多情景模式类似。Firewall Threat Defense 的多情景模式不可用。 新增/修改的 防火墙管理中心菜单项： • **设备** > **设备管理** > **编辑**图标**接口**选项卡 新增/修改的 Firepower 机箱管理器菜单项： • **概述** > **设备** • **接口** > **所有接口** > **新增**下拉菜单**子接口** • **接口** > **所有接口** > **类型** • **逻辑设备** > **添加设备** • **平台设置** > **Mac 池** • **平台设置** > **资源配置文件** 新增/修改的 FXOS 命令：**connect ftd** *name*、**connect module telnet**、**create bootstrap-key PERMIT_EXPERT_MODE**、**create resource-profile**、**create subinterface**、**scope auto-macpool**、**set cpu-core-count**、**set deploy-type**、**set port-type data-sharing**、**set prefix**、**set resource-profile-name**、**set vlan**、**scope app-instance ftd** *name*、**show cgroups container**、**show interface**、**show mac-address**、**show subinterface**、**show tech-support module app-instance**、**show version** 支持的平台：Firepower 4100/9300

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
Firepower 4100/9300 的集群控制链路可自定义 IP 地址	6.3	任意	默认情况下， 集群控制链路使用 127.2.0.0/16 网络。现在，可以在 FXOS 中部署集群时设置网络。机箱根据机箱 ID 和插槽 ID 自动生成每个设备的集群控制链路接口 IP 地址：127.2.*chassis_id*.*slot_id*。但是，某些网络部署不允许 127.2.0.0/16 流量通过。因此，您现在可以为 FXOS 中的集群控制链路设置一个自定义的 /16 子网（环回 (127.0.0.0/8) 和组播 (224.0.0.0/4) 地址除外）。 新增/修改的 Firepower 机箱管理器菜单项： • **逻辑设备** > **添加设备** > **集群信息** > **CCL 子网 IP** 字段 新增/修改的 FXOS 命令：**set cluster-control-link network** 支持的平台：Firepower 4100/9300
支持保存模式下的数据 Etherchannel	6.3	任意	现在可以将数据和数据共享 Etherchannel 设置为“主用”LACP 模式或“保持”模式。其他类型 Etherchannel 仅支持“主用”模式。 新增/修改的 Firepower 机箱管理器菜单项： • **接口** > **所有接口** > **编辑端口通道** > **模式** 新增/修改的 FXOS 命令：**set port-channel-mode** 支持的平台：Firepower 4100/9300
支持 Firewall Threat Defense 内联集中的 Etherchannel	6.2	任意	现在可以使用 Firewall Threat Defense 内联集中的 EtherChannel。 支持的平台：Firepower 4100/9300
对 6 个 Firewall Threat Defense模块进行机箱间集群	6.2	任意	现在，您可以对 Firewall Threat Defense启用机箱间集群。在最多 6 个机箱中最多可以包含 6 个模块。 新增/修改的 Firepower 机箱管理器屏幕： • **逻辑设备** > **配置** 支持的平台：Firepower 4100/9300
Firepower 4100/9300 上对所支持网络模块的硬件旁路支持	6.1	任意	硬件绕行确保流量在断电期间继续在接口对之间流动。在软件或硬件发生故障时，此功能可用于维持网络连接性。 新增/修改的屏幕： • **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **编辑物理接口 (Edit Physical Interface)** 支持的平台：Firepower 4100/9300

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
内联集链路状态传播支持 Firewall Threat Defense	6.1	任意	当您在 Firewall Threat Defense 应用中配置内联集并启用链路状态传播时，Firewall Threat Defense 会向 FXOS 机箱发送内联集成员身份。链路状态传播意味着，当内联集的一个接口断开时，机箱将自动关闭内联接口对的第二个接口。 新增/修改的 FXOS 命令：**show fault |grep link-down**、**show interface detail** 支持的平台：Firepower 4100/9300
支持在 Firepower 9300 上的 Firewall Threat Defense 上执行机箱内集群	6.0.1	任意	Firepower 9300 支持使用 Firewall Threat Defense 应用执行机箱内集群。 新增/修改的 Firepower 机箱管理器菜单项： • **逻辑设备** > **配置** 新增/修改的 FXOS 命令：**enter mgmt-bootstrap ftd**、**enter bootstrap-key FIREPOWER_MANAGER_IP**、**enter bootstrap-key FIREWALL_MODE**、**enter bootstrap-key-secret REGISTRATION_KEY**、**enter bootstrap-key-secret PASSWORD**、**enter bootstrap-key FQDN**、**enter bootstrap-key DNS_SERVERS**、**enter bootstrap-key SEARCH_DOMAINS**、**enter ipv4 firepower**、**enter ipv6 firepower**、**set value**、**set gateway**、**set ip**、**accept-license-agreement** 支持的平台：Firepower 4100/9300

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。

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。

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。