



基本接口配置

本章介绍基本接口配置，包括以太网设置和巨帧配置。



注释 在多情景模式下，请在系统执行空间中完成本节所述的所有任务。要从情景更改到系统执行空间，请输入 **change to system** 命令。



注释 对于平台模式中的 和上的 Firepower 4100/9300 机箱Firepower 2100，您可以在 FXOS 操作系统中配置基本接口设置。有关详细信息，请参阅机箱的配置或快速入门指南。

- [关于基本接口配置，第 1 页](#)
- [基本接口配置的相关准则，第 3 页](#)
- [基本接口配置的默认设置，第 4 页](#)
- [启用物理接口和配置以太网参数，第 5 页](#)
- [启用巨帧支持（ASA Virtual、ISA 3000），第 8 页](#)
- [管理安全防火墙 3100/4200 的网络模块，第 9 页](#)
- [监控接口，第 13 页](#)
- [基本接口示例，第 14 页](#)
- [基本接口配置的历史记录，第 14 页](#)

关于基本接口配置

本节介绍接口功能与特殊接口。

Auto-MDI/MDIX 功能

对于 RJ-45 接口，默认的自动协商设置还包括 Auto-MDI/MDIX 功能。Auto-MDI/MDIX 在自动协商阶段检测直通电缆时执行内部交叉，从而消除交叉布线的需要。如要启用接口的 Auto-MDI/MDIX，必须将速度或双工设置为自动协商。如果将速度和双工明确设置为固定值，从而禁用了两种设置的

管理接口

自动协商，则 Auto-MDI/MDIX 也将被禁用。对于千兆以太网，当速度和双工被设置为 1000 和全值时，接口始终会自动协商；因此，Auto-MDI/MDIX 始终会启用，且您无法禁用它。

管理接口

管理接口是一个仅用于管理流量的独立接口，具体情况视型号而定。

管理接口概述

可以通过连接至以下接口来管理 ASA：

- 任何直通流量接口
- 专用的管理插槽/端口接口（如果适用于所用的型号）

您可以需要根据[管理访问](#)来配置对接口的管理访问权限。

管理插槽/端口接口

下表列出了每个型号的管理接口。

表 1: 每个型号的管理接口

| 型号 | Management 0/0 | Management 1/1 | 管理 1/2 | 可针对直通流量进行配置 | 允许子接口 |
|----------------------------|---------------------------------------|-----------------------|---------------|---|-------|
| Firepower 1000 | — | 是 | — | 是 | 是 |
| Firepower 2100 | — | 是 | — | — 请注意：技术上而言，您可以启用直通流量；但是，此接口的吞吐量不足以进行数据操作。 | 是 |
| Cisco Secure Firewall 3100 | — | 是 | — | 是 | 是 |
| Cisco Secure Firewall 4200 | — | 是 | 是 | 是 | 是 |
| Firepower 4100/9300 | 不适用 接口 ID 取决于分配给 ASA 逻辑设备的管理类型物理接口 | — | — | — | 是 |
| ISA 3000 | — | 是 | — | — | — |
| ASAv | 是 | — | — | 是 | — |

将任何接口用于管理专用流量

若想将任何接口（包括 EtherChannel 接口）用作管理专用接口，您只需将该接口配置为用于管理流量（请参阅 **management-only** 命令）。

透明模式下的管理接口

在透明防火墙模式下，除了允许的最大数量的直通流量接口，您还可以将管理接口（物理接口、子接口[如果所用的型号支持]用作单独的仅管理接口。

您不能将任何其他接口类型用作管理接口。

对于 Firepower 4100/9300 机箱，管理接口 ID 取决于分配给 ASA 逻辑设备的管理类型接口。



注释 管理接口不属于普通网桥组的一部分。请注意，出于操作目的，管理接口属于不可配置网桥组的一部分。

仅管理 流量

管理接口仅适用于传入和传出设备的流量，不能通过流量。在任何情况下，网桥组都无法与任何其他网桥组通信，因此即使管理接口支持直通流量，管理接口也无法路由到网桥组，反之亦然。

共享 MAC 地址表和交换机连接

在透明防火墙模式下，管理接口以与数据接口相同的方式更新 MAC 地址表；因此不应将管理和数据接口连接到同一个交换机，除非将其中一个交换机端口配置为路由端口（默认情况下，Catalyst 交换机在所有的 VLAN 交换机端口上共享一个 MAC 地址）。否则，如果流量从物理连接的交换机到达管理接口，那么 ASA 会更新 MAC 地址表，以使用管理接口而非数据接口访问交换机。此操作会导致流量临时中断；出于安全考虑，ASA 在至少 30 秒的时间内不会为了从交换机传输至数据接口的数据包而再次更新 MAC 地址表。

多情景模式

在多情景模式下，您无法跨情景共享任何接口，包括管理接口。要为每个情景提供管理，您可以创建管理接口的子接口，然后向每个情景分配管理子接口。一些型号不允许管理接口上有子接口，因此这些型号需要为了针对每个情景进行管理，您必须连接到数据接口。对于 Firepower 4100/9300 机箱，管理接口及其子接口不会被识别为情景中允许的特殊管理接口；您必须在这种情况下将管理子接口视为数据接口，并将其添加到 BVI。

基本接口配置的相关准则

透明防火墙模式

对于多情景透明模式，每个情景必须使用不同的接口；您不能在情景之间共享一个接口。

■ 基本接口配置的默认设置

故障转移

您不能与数据接口共享一个故障转移接口或状态接口。

其他准则

有些管理相关服务在启用非管理接口和ASA实现“系统就绪”状态之前不可用。在“系统就绪”状态下，ASA会生成以下系统日志消息：

```
%ASA-6-199002: Startup completed. Beginning operation.
```

基本接口配置的默认设置

本节列出了接口的默认设置（如果没有出厂默认配置）。

接口的默认状态

接口的默认状态取决于类型和情景模式。

在多情景模式下，默认启用所有已分配的接口，而不考虑接口在系统执行空间中的状态。但是，要使流量通过该接口，还必须在系统执行空间中启用该接口。如果您在系统执行空间中关闭了一个接口，则该接口在所有共享它的情景中都会关闭。

在单模式下或在系统执行空间中，接口具有以下默认状态：

- 物理接口 - 已禁用。
- VLAN 子接口 - 已启用。但是，要使流量通过子接口，还必须启用物理接口。
- VXLAN VNI 接口 - 已启用。
- EtherChannel port-channel 接口 (ISA 3000) - 已启用。但是，要使流量通过 EtherChannel 接口，还必须启用通道组物理接口。
- EtherChannel port-channel 接口 (其他型号) - 已禁用。



注释 对于 Firepower 4100/9300，您可以出于管理需要同时启用和禁用机箱和 ASA 上的接口。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 ASA 之间可能出现不匹配的情况。

默认速度和双工

- 默认情况下，铜缆 (RJ-45) 接口的速度和双工设置为自动协商。

默认连接器类型

有些型号包含两个连接器类型：铜缆 RJ-45 和光纤 SFP。RJ-45 是默认接口。您可以将 ASA 配置为使用光纤 SFP 连接器。

默认 MAC 地址

默认情况下，物理接口使用烧录 MAC 地址，物理接口的所有子接口均使用相同的烧录 MAC 地址。

启用物理接口和配置以太网参数

本节介绍如何执行以下操作：

- 启用物理接口
- 设置特定的速度和双工（如有）
- 启用暂停帧以进行流量控制
- (Cisco Secure Firewall 3100/4200) 设置前向纠错

此过程仅涵盖一小部分接口设置。此时不能设置其他参数。例如，不能命名要用作 EtherChannel 接口一部分的接口。具体的接口选项因您的设备型号和接口类型而异。



注释 对于 Firepower 4100/9300，可在 FXOS 中配置基本接口设置。



注释 有关 Firepower 1010 交换机端口，请参阅 200。[Firepower 1010 交换机端口的基本接口配置](#)

开始之前

对于多情景模式，请在系统执行空间中完成本程序。要从情景更改到系统执行空间，请输入 **changeto system** 命令。

过程

步骤 1 指定要配置的接口：

interface physical_interface

示例：

```
ciscoasa(config)# interface gigabitethernet 0/0
```

physical_interface ID 包含类型、插槽和端口号，格式为 type[slot/]port。

启用物理接口和配置以太网参数

物理接口类型包括:

- 以太网
gigabitethernet
- **tengigabitethernet**
- **management**

依次输入类型和插槽/端口，例如 **gigabitethernet0/1**。类型与插槽/端口之间的空格是可选的。

步骤 2 (可选) 设置速度 (因型号而异)。

speed {auto | speed | nonegotiate | sfp-detect}

示例:

```
ciscoasa(config-if)# speed 100
```

对于 Firepower 1100 和 2100 光纤接口，**speed nonegotiate** 会将速度设置为 1000 Mbps，并禁用流量控制参数和远程故障信息的链路协商。对于其他型号，请使用 **negotiate-auto** 命令。

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。**sfp-detect** 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 3 Set auto-negotiation.

negotiate-auto

自动协商与速度分开设置。

示例:

```
ciscoasa(config-if)# negotiate-auto
```

步骤 4 (可选) 设置双工。

duplex {auto | full | half}

SFP 接口仅支持全复用。

示例:

```
ciscoasa(config-if)# duplex full
```

步骤 5 (可选) (Cisco Secure Firewall 3100/4200) 对于 25 Gbps 及更高的接口，请设置前向纠错 (FEC)。

fec {auto | cl108-rs | cl74-fc | cl91-rs | disable}

对于 EtherChannel 成员接口，必须先配置 FEC，然后才能将其添加到 EtherChannel。使用 **自动** 时选择的设置取决于收发器类型，以及接口是固定接口（内置）还是在网络模块上。

注释

- 如果从 EtherChannel 中删除接口，则在重新启动 ASA 后，FEC 和自动协商配置将更改。您需要再次手动配置 FEC 和自动协商，因为这是预期行为。
- 如果连接到 EtherChannel 成员接口的对等交换机不支持 FEC 模式的 **自动** 设置，您必须根据下表在平台和接口的交换机上手动配置 FEC 模式，以接通链路。例如，当连接到 25 Gbps 接口时，N9K-C93400LD-H1 不支持 FEC 模式的 **自动** 设置。

表 2: 用于自动设置的默认 FEC

| 收发器类型 | 固定端口默认 FEC (以太网 1/9 至 1/16) | 网络模块默认 FEC |
|--------------|-----------------------------|------------|
| 25G-SR | cl108-rs | cl108-rs |
| 25G-LR | cl108-rs | cl108-rs |
| 10/25G-CSR | cl108-rs | cl74-fc |
| 25G-AOCxM | cl74-fc | cl74-fc |
| 25G-CU2.5/3M | 自动协商 | 自动协商 |
| 25G-CU4/5M | 自动协商 | 自动协商 |
| 25/50/100G | cl91-rs | cl91-rs |

步骤 6 (可选) (ASA 硬件) 在千兆位及更高版本的接口上启用暂停 (XOFF) 帧以进行流量控制:

flowcontrol send on

示例:

```
ciscoasa(config-if)# flowcontrol send on
```

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 ASA 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

ASA 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。

启用巨帧支持 (ASA Virtual、ISA 3000)

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 7 启用接口:

no shutdown

示例:

```
ciscoasa(config-if)# no shutdown
```

要显示接口，请输入 **shutdown** 命令。如果输入 **shutdown** 命令，则还可关闭所有子接口。如果您在系统执行空间中关闭了一个接口，则该接口在所有共享它的情景中都会关闭。

启用巨帧支持 (ASA Virtual、ISA 3000)

巨型帧是指大于标准最大值 1518 字节（包括第 2 层报头和 VLAN 报头）的以太网数据包，最大为 9216 字节。您可以通过增加用于处理以太网帧的内存量对所有接口启用巨型帧支持。为巨型帧分配较多内存可能会有碍于最大限度地利用其他功能（例如 ACL）。请注意，ASA MTU 设置的负载大小不包括第 2 层（14 字节）和 VLAN 报头（4 字节），因此最大 MTU 是 9198，具体取决于您的型号。

此程序仅适用于 ISA 3000 和 ASA Virtual。其他型号默认支持巨型帧。

RAM 小于 8GB 的 ASAv5 和 ASAv10 不支持巨型帧。

开始之前

- 在多情景模式下，请在系统执行空间中设置此选项。
- 此设置的更改要求您重新加载 ASA。
- 确保要将需要传送巨型帧的每个接口的 MTU 设置为大于默认值 1500 的值；例如使用 **mtu** 命令将该值设置为 9198。在多情景模式下，请在每个情景中设置 MTU。
- 请务必调整 TCP MSS，以对非 IPsec 流量禁用此功能（使用 **sysopt connection tcpmss 0** 命令），或者根据 MTU 增加 TCP MSS 的值。

过程

启用巨型帧支持:

jumbo-frame reservation

示例

以下示例将启用巨型帧预留、保存配置并重新加载 ASA:

```
ciscoasa(config)# jumbo-frame reservation
WARNING: this command will take effect after the running-config is saved
and the system has been rebooted. Command accepted.

ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: 718e3706 4edb11ea 69af58d0 0a6b7cb5

70291 bytes copied in 3.710 secs (23430 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm] Y
```

管理安全防火墙 3100/4200 的网络模块

如果在首次打开防火墙之前安装网络模块，则无需执行任何操作；网络模块已启用并可供使用。

如果您需要在初始启动后更改网络模块安装，请参阅以下程序。

配置分支端口

您可以为每个 40GB 或更高的接口配置更小的分支端口。此程序介绍如何断开和重新加入端口。此程序介绍如何断开和重新加入端口。分支端口可以像任何其他物理以太网端口一样使用，包括添加到 EtherChannel。例如，可以从 40GB 接口划分为四个 10GB 端口。端口的确切大小和数量取决于型号。

如果一个接口已经在您的配置中使用，那么您必须手动删除与不再存在的接口相关的任何配置。

开始之前

- 您必须使用受支持的分支电缆。有关详细信息，请参阅硬件安装指南。
- 对于集群或故障转移，请确保集群/故障转移链路未使用父接口（用于分支）或子接口（用于重新加入）；如果该接口正用于集群/故障转移链路，则无法对其进行更改。

过程

步骤 1 从 40GB 或更高的接口分支出端口。

breakout slot port

例如，要断开 Ethernet2/1 40GB 接口，应为插槽指定 2，为端口指定 1。子接口将被标识为 Ethernet2/1/1、Ethernet2/1/2、Ethernet2/1/3 和 Ethernet2/1/4。

增加网络模块

对于集群或故障转移，请在控制节点/主用设备上执行此步骤；接口更改将复制到其他节点。

示例：

```
ciscoasa(config)# breakout 2 1
ciscoasa(config)# breakout 2 2
ciscoasa(config)# breakout 2 3
ciscoasa(config)# breakout 2 4
```

步骤 2 重新加入分支端口以恢复接口。

no breakout slot port

对于集群或故障转移，请在控制节点/主用设备上执行此步骤；模块状态被复制到其他节点。

您必须重新加入该接口的所有子端口。

示例：

```
ciscoasa(config)# no breakout 2 1
```

增加网络模块

要在初始启动后将网络模块添加到防火墙，请执行以下步骤。添加新模块需要重新加载。对于集群或故障转移，不支持零停机时间，因此请确保在维护窗口期间执行此程序。

过程

步骤 1 根据硬件安装指南安装网络模块。您可以在防火墙打开时安装网络模块。

对于集群或故障转移，请在所有节点上安装网络模块。

步骤 2 重新加载防火墙；请参阅 [重新加载 ASA](#)。

对于集群或故障转移，请重新加载所有节点。由于具有不同网络模块的节点无法加入集群/故障转移对，因此您需要使用新模块重新加载所有节点，然后它们才能重组集群/故障转移对。

步骤 3 启用网络模块。

no netmod 2 disable

对于集群或故障转移，请在控制节点/主用设备上执行此步骤；模块状态被复制到其他节点。

示例：

```
ciscoasa(config)# no netmod 2 disable
```

热插拔网络模块

您可以将网络模块热插拔为相同类型的新模块，而无需重新加载。但是，您必须关闭当前模块才能安全地将其删除。此程序介绍如何关闭旧模块、安装新模块以及如何启用它。

对于集群或故障转移，如果集群控制链路/故障转移链路在模块上，则不能禁用该模块。

过程

步骤 1 对于集群或故障转移，请执行以下步骤。

- 集群- 确保要执行热插拔的设备是数据节点（请参阅[更改控制节点](#)）；然后中断节点，使其不再位于集群中。请参阅[成为非活动节点](#)或[停用节点](#)。

如果集群控制链路在网络模块上，则必须离开集群。请参阅[离开集群](#)。不允许禁用具有主动集群控制链路的网络模块。

- 故障转移-请确保要执行热插拔的设备是备用节点。请参阅[强制故障转移](#)。

如果故障转移链路位于网络模块上，则必须禁用故障转移。请参阅[禁用故障转移](#)。不允许禁用具有主动故障转移链路的网络模块。

步骤 2 禁用网络模块。

netmod 2 disable

示例：

```
ciscoasa(config)# netmod 2 disable
```

步骤 3 根据硬件安装指南更换网络模块。您可以在防火墙通电时更换网络模块。

步骤 4 启用网络模块。

no netmod 2 disable

示例：

```
ciscoasa(config)# no netmod 2 disable
```

步骤 5 对于集群或故障转移，请执行以下步骤。

- 集群 (**Clustering**) - 将节点添加回集群。请参阅[重新加入集群](#)。
- 故障转移- 如果禁用故障转移，则重新进行故障转移。

将网络模块更换为其他类型

将网络模块更换为其他类型

如果您更换了其他类型的网络模块，则需要重新加载。如果新模块的接口少于旧模块，则必须手动删除与不再存在的接口相关的任何配置。对于集群或故障转移，不支持零停机时间，因此请确保在维护窗口期间执行此程序。

过程

步骤 1 禁用网络模块。

netmod 2 disable

对于集群或故障转移，请在控制节点/主用设备上执行此步骤；模块状态被复制到其他节点。不保存配置；重新加载时，系统将使用保存的配置启用该模块。

示例：

```
ciscoasa(config)# netmod 2 disable
```

步骤 2 根据硬件安装指南更换网络模块。您可以在防火墙通电时更换网络模块。

对于集群或故障转移，请在所有节点上安装网络模块。

步骤 3 重新加载防火墙；请参阅 [重新加载 ASA](#)。

对于集群或故障转移，请重新加载所有节点。由于具有不同网络模块的节点无法加入集群/故障转移对，因此您需要使用新模块重新加载所有节点，然后它们才能重组集群/故障转移对。

步骤 4 如果在重新加载之前保存了配置，则必须重新启用该模块。

拆卸网络模块

如果要永久删除网络模块，请执行以下步骤。拆卸网络模块需要重新加载。对于集群或故障转移，不支持零停机时间，因此请确保在维护窗口期间执行此程序。

开始之前

对于集群或故障转移，请确保集群/故障转移链路不在网络模块上；在这种情况下，您无法删除该模块。

过程

步骤 1 禁用网络模块并保存配置。

netmod 2 disable

write memory

对于集群或故障转移，请在控制节点/主用设备上执行此步骤；模块状态被复制到其他节点。

示例：

```
ciscoasa(config)# netmod 2 disable  
ciscoasa(config)# write memory
```

步骤 2 根据硬件安装指南删除网络模块。您可以在防火墙通电时删除网络模块。

对于集群或故障转移，请删除所有节点上的网络模块。

步骤 3 重新加载防火墙；请参阅 [重新加载 ASA](#)。

对于集群或故障转移，请重新加载所有节点。由于具有不同网络模块的节点无法加入集群/故障转移对，因此您需要重新加载不含该模块的所有节点，然后它们才能重组集群/故障转移对。

监控接口

请参阅以下命令。



注释 对于 Firepower 和 Cisco Secure Firewall 模型，某些统计信息未使用 ASA 命令显示。您必须使用 FXOS 命令查看更详细的接口统计信息。

- /eth-uplink/fabric# **show interface**
- /eth-uplink/fabric# **show port-channel**
- /eth-uplink/fabric/interface# **show stats**

对于平台模式下的 Firepower 2100，另请参阅以下 FXOS connect local-mgmt 命令：

- (local-mgmt)# **show portmanager counters**
- (local-mgmt)# **show lacp**
- (local-mgmt)# **show portchannel**

有关详细信息，请参阅 [FXOS 故障排除指南](#)。

• **show interface**

显示接口统计信息。

• **show interface ip brief**

显示接口的 IP 地址和状态。

■ 基本接口示例

基本接口示例

请参阅以下配置示例。

物理接口参数示例

以下示例在单模式下配置物理接口的参数：

```
interface gigabitethernet 0/1
speed 1000
duplex full
no shutdown
```

多情景模式示例

以下示例在多情景模式下配置用于系统配置的接口参数，并将千兆以太网 0/1.1 子接口分配到 contextA：

```
interface gigabitethernet 0/1
speed 1000
duplex full
no shutdown
interface gigabitethernet 0/1.1
vlan 101
context contextA
allocate-interface gigabitethernet 0/1.1
```

基本接口配置的历史记录

表 3: 接口的历史记录

| 功能名称 | 版本 | 功能信息 |
|--|-------------------|---|
| Cisco Secure Firewall 3100 固定端口上的默认前向纠错 (FEC) 从第 74 条 FC-FEC 更改为第 108 条 RS-FEC，适用于 25 GB+ SR、CSR 和 LR 收发器。 | 9.18(3) / 9.19(1) | 当您在 Cisco Secure Firewall 3100 固定端口上将 FEC 设置为自动时，对于 25 GB SR、CSR 和 LR 收发器，默认类型现在设置为 cl108-rs 而不是 cl74-fc。 新增/修改的命令： fec |
| 为 Cisco Secure Firewall 3100 暂停流量控制的帧 | 9.18(1) | 如果流量激增，数据包会在激增量超过 NIC 上的 FIFO 缓冲区的缓冲容量且接收环缓冲的情况下发生中断。启用暂停帧来进行流量控制可缓解此问题。 新增/修改的命令： flowcontrol send on |

| 功能名称 | 版本 | 功能信息 |
|---|---------------|---|
| Cisco Secure Firewall 3130 和 3140 的分支端口 | 9.18(1) | <p>您现在可以为 Cisco Secure Firewall 3130 和 3140 上的每个 40GB 接口配置四个 10GB 分支端口。</p> <p>新增/修改的命令: breakout</p> |
| 支持热插拔 Cisco Secure Firewall 3100 的网络模块 | 9.17(1) | <p>您可以在防火墙通电时在 Cisco Secure Firewall 3100 上添加或删除网络模块。要将某个模块替换为相同类型的另一个模块，则无需重新启动。初始启动后，添加模块、永久删除模块或用新类型替换模块都需要重新启动。</p> <p>新增/修改的命令: netmod</p> |
| 支持 Cisco Secure Firewall 3100 的前向纠错 | 9.17(1) | <p>Cisco Secure Firewall 3100 25 Gbps 接口支持前向纠错 (FEC)。FEC 默认为启用并会设为“自动” (Auto)。</p> <p>新增/修改的命令: fec</p> |
| 支持基于 SFP 为 Cisco Secure Firewall 3100 设置速度 | 9.17(1) | <p>Cisco Secure Firewall 3100 支持基于安装的 SFP 的接口速度检测。检测 SFP 默认为启用。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。</p> <p>新增/修改的命令: speed sfp-detect</p> |
| 可以为 1Gigabit 及更高版本的接口启用或禁用 Cisco Secure Firewall 3100 自动协商。 | 9.17(1) | <p>Cisco Secure Firewall 3100 自动协商功能可与千兆位及以上接口的速度分启用或禁用。</p> <p>新增/修改的命令: negotiation-auto</p> |
| 在 Firepower 1100 和 2100 的光纤接口上可禁用速度自动协商 | 9.14(1) | <p>现在，您可以配置 Firepower 1100 或 2100 光纤接口以禁用自动协商。对于 10GB 接口，您可以将速度配置为 1GB 而无需自动协商；无法对速度设置为 10GB 的接口禁用自动协商。</p> <p>新增/修改的命令: speed nonegotiate</p> |
| ASA Virtual 的管理 0/0 接口上提供通过流量支持 | 9.6(2) | <p>现在，您可以在 ASA Virtual 的管理 0/0 接口上允许通过流量。过去，仅 Microsoft Azure 上的 ASA Virtual 支持通过流量；现在所有 ASA Virtual 都支持通过流量。您可以选择将此接口配置为仅管理接口，但默认情况下，没有进行此配置。</p> <p>修改了以下命令: management-only</p> |
| 在千兆以太网接口上支持暂停帧以进行流量控制 | 8.2(5)/8.4(2) | <p>您现在可以在所有 ASA 型号的千兆以太网接口上启用暂停 (XOFF) 帧以进行流量控制。</p> <p>修改了以下命令: flowcontrol。</p> |
| 在 ASA 5580 的 10 千兆以太网接口上支持暂停帧以进行流量控制 | 8.2(2) | <p>您现在可以为流量控制启用暂停 (XOFF) 帧。</p> <p>ASA 5585-X 也支持此功能。</p> <p>引入了以下命令: flowcontrol。</p> |

■ 基本接口配置的历史记录

| 功能名称 | 版本 | 功能信息 |
|------------------------------|--------|--|
| 对 ASA 5580 的巨型数据包支持 | 8.1(1) | <p>ASA 5580 支持巨帧。巨帧是指大于标准最大字节数（1518 字节）的以太网数据包（包括第 2 层报头和 FCS），最大可达 9216 字节。您可以通过增加用于处理以太网帧的内存量对所有接口启用巨型帧支持。为巨型帧分配较多内存可能会有碍于最大限度地利用其他功能（例如 ACL）。</p> <p>ASA 5585-X 也支持此功能。</p> <p>引入了以下命令：jumbo-frame reservation。</p> |
| 对于 ASA 5510 增强型安全许可证的千兆以太网支持 | 7.2(3) | <p>现在，ASA 5510 通过增强型安全许可证为端口 0 和 1 提供 GE（千兆以太网）支持。如果从基础许可证升级至增强型安全许可证，则外部 Ethernet 0/0 和 Ethernet 0/1 端口的容量将从原始的 FE（快速以太网）(100 Mbps) 增加到 GE(1000 Mbps)。接口名称将仍为 Ethernet 0/0 和 Ethernet 0/1。使用 speed 命令可更改接口上的速度，使用 show interface 命令可查看为每个接口当前配置的速度。</p> |
| ASA 5510 上的基础许可证增加了接口数 | 7.2(2) | 对于 ASA 5510 上的基础许可证，最大接口数从 3 加管理接口数增加到无限个。 |

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。