高可用性（故障转移）

以下主题介绍如何配置和管理主用/备用设备故障转移，以实现 Firewall Threat Defense系统的高可用性。

关于高可用性（故障转移）

高可用性或故障转移设置可以将两台设备相关联，这样，当主设备发生故障时，辅助设备可以接管其任务。这有助于您在设备发生故障时保持网络运行。

配置高可用性需要两台相同的 Firewall Threat Defense设备，二者之间通过专用故障转移链路和（可选）状态链路彼此互连。这两台设备不断通过故障转移链路进行通信，以便确定每台设备的运行状态并同步已部署的配置更改。系统使用状态链路将连接状态信息传递到备用设备，因此如果发生故障转移，用户连接将得以保留。

这两台设备构成一对主用/备用设备，其中一台设备是主用设备并传递流量。备用设备不会主动传递流量，但会使配置和其他状态信息与主用设备同步。

系统会对主用设备的运行状况（硬件、接口、软件以及环境状态）进行监控，以便确定是否符合特定的故障转移条件。如果符合条件，主用设备将故障转移至备用设备，届时备用设备将变成主用设备。

主用/备用故障转移

主用/备用故障转移是一种高可用性配置

- 允许使用备用 Firewall Threat Defense 设备接管故障设备的功能，

- 当主用设备故障，备用设备将变为主用设备，以及
- 若故障为暂时性，故障设备恢复后可重新作为备用设备上线。

若故障非暂时性，必须更换故障设备。更换故障设备前，须先将备用设备设为主设备，以保留辅助设备的配置。

对于多情景模式，ASA 可以在整个设备（包括所有情景）上进行故障转移，但不能在单个情景上单独进行故障转移。

主/辅角色与主/备状态

主/辅角色和主/备状态是故障转移配置概念，

- 定义设备层级结构，在同时启动时主设备优先，
- 确定故障转移操作期间的 IP 地址和 MAC 地址使用模式，以及
- 在主/备故障转移配置中的配对设备之间确立流量传输职责。

主设备与辅设备的差异

在故障转移对中这两台设备之间的主要区别是哪台是主用设备，哪台是备用设备，即要使用哪些 IP 地址以及哪台设备积极传递流量。

但是，设备之间还存在一些取决于哪一设备为主设备（在配置中指定），哪一设备为辅助设备的差别：

- 如果两台设备同一时间启动（并且运行状况相同），则主设备总是会成为主用设备。
- 主设备 MAC 地址始终与主用 IP 地址相匹配。此规则的例外是，当辅助设备成为主用设备并且无法通过故障转移链路获取主设备 MAC 时。在这种情况下，会使用辅助设备的 MAC 地址。

启动时的主用设备确定

启动时主用设备判定是高可用性过程

- 若设备启动时检测到对等体已运行为主用，则该设备置为备用，
- 若设备启动未检测到对等体，则置为主用；
- 若两台设备同时启动，主设备置为主用，辅助设备置为备用。

故障转移事件

故障转移事件是指

- 触发主用/备用故障转移配置中的主用设备将控制权移交给备用设备
- 按设备级别发生，，以及
- 遵循特定故障转移策略以确定是否发生故障转移及各设备应采取的操作。

故障转移事件策略和操作

此表显示各故障事件的故障转移操作。对于每种故障事件，该表显示了故障转移策略（故障转移或禁用故障转移）、主用设备执行的操作、备用设备执行的操作，以及有关故障转移条件和操作的所有特别说明。

表 *1:* 故障转移事件

故障事件	策略	主用设备操作	备用设备操作	说明
主用设备发生故障（电源或硬件）	故障转移	不适用	成为主用设备 将主用设备标记为发生故障	在任何受监控接口或故障转移链路上，均未收到 Hello 消息。
以前的主用设备恢复	禁用故障转移	成为备用设备	无需操作	无。
备用设备发生故障（电源或硬件）	禁用故障转移	将备用设备标记为发生故障	不适用	备用设备被标记为发生故障后，主用设备不会尝试进行故障转移，即使超过接口故障阈值也是如此。
故障转移链路在运行过程中发生故障	禁用故障转移	将故障转移链路标记为发生故障	将故障转移链路标记为发生故障	您应尽快恢复故障转移链路，因为当故障转移链路发生故障时，设备无法故障转移到备用设备。
故障转移链路在启动时发生故障	禁用故障转移	成为主用设备 将故障转移链路标记为发生故障	成为主用设备 将故障转移链路标记为发生故障	如果故障转移链路在启动时发生故障，则两台设备都会成为主用设备。
状态链路发生故障	禁用故障转移	无需操作	无需操作	如果发生故障转移，状态信息会过时，而且会话会被终止。
主用设备上的接口故障超过阈值	故障转移	将主用设备标记为发生故障	成为主用设备	无。
备用设备上的接口故障超过阈值	禁用故障转移	无需操作	将备用设备标记为发生故障	备用设备被标记为发生故障后，主用设备不会尝试进行故障转移，即使超过接口故障阈值也是如此。

故障转移和状态故障转移链路

故障转移链路是两台设备之间的专用连接。状态故障转移链路也是专用连接，不过，您可以使用一个故障转移链路作为组合的故障转移/状态链路，也可以创建单独的专用状态链路。如果仅使用故障转移链路，状态信息也会通过该链路：状态故障转移功能不会受到影响。

默认情况下，故障转移和状态故障转移链路上的通信是纯文本通信（不加密）。为了增强安全性，您可以通过配置 IPsec 加密密钥对通信加密。

以下主题更加详细地介绍了这些接口，并就如何连接设备以获得最佳效果给出了建议。

故障转移链路

故障转移对中的两台设备会不断地通过故障转移链路进行通信，以确定每台设备的运行状态和同步配置更改。

以下信息将通过故障转移链路传输：

- 设备状态（主用或备用）。
- Hello 消息 (keep-alives)。
- 网络链路状态。
- MAC 地址交换。
- 配置复制和同步。
- 系统数据库更新，包括 VDB 和规则，但不包括地理位置和安全智能数据库。每个系统会单独下载地理位置和安全智能更新。如果您创建更新计划，这些更新应保持同步。但是，如果您在主用设备上执行手动地理位置或安全智能更新，那么也应在备用设备上执行同样的操作。

注释 事件、报告和审核日志数据不会同步。事件查看器和控制面板仅显示与特定设备相关的数据。此外，部署历史记录、任务历史记录和其他审核日志事件不会同步。

状态故障转移链路

系统使用状态链路将连接状态信息传送到备用设备。此信息可在发生故障转移时帮助备用设备保留现有连接。

对故障转移和状态故障转移链路使用一条链路能够最大程度地节省接口。但是，如果您有一个大型配置和高流量网络，必须考虑对状态链路和故障转移链路使用专用接口。

用于故障转移和状态链路的接口

可以使用未使用但已启用的数据接口（物理接口或 EtherChannel 接口）作为故障转移链路；但无法指定当前配置了名称的接口。故障转移链路接口不会配置为常规网络接口；该接口仅会因为故障转移而存在。该接口只能用于故障转移链路（还用于状态链路）。您不能使用管理接口、子接口、VLAN 接口或交换机端口作为故障转移接口。

Firewall Threat Defense 设备用户数据和故障转移链路之间共享接口。

请参阅下列有关调整故障转移和状态链路大小的准则：

- Firepower 4100/9300 - 我们建议您将一个 10 GB 的数据接口用于组合的故障转移和状态链路。
- 所有其他型号 - 1 GB 接口对于组合的故障转移和状态链路而言已足够大。

使用 EtherChannel 接口作为故障转移链路或状态链路时，必须在建立高可用性之前，确认具有相同 ID 和成员接口的同一 EtherChannel 在两台设备上都存在。如果 EtherChannel 不匹配，您需要先禁用 HA 并更正辅助设备的配置。要阻止无序数据包，仅使用 EtherChannel 中的一个接口。如果该接口发生故障，则会使用 EtherChannel 中的下一个接口。您不能在 EtherChannel 配置用作故障转移链路时对其进行修改。

连接故障转移和状态故障转移接口

您可以将任何未使用的数据物理接口用作故障转移链路和可选的专用状态链路。但是，您不能选择当前已配置名称或具有子接口的接口。故障转移和状态故障转移链路接口不会被配置为通常的网络接口。这些接口只是为了进行故障转移通信，不能用于直通流量或管理访问。

此配置在设备之间是同步的，因此您必须为链路的两端选择相同的端口号。例如，用于故障转移链路的两台设备都使用 GigabitEthernet1/3。

使用以下两种方法中的一种连接故障转移链路和专用状态链路（如已使用）：

- 使用不与任何其他设备处于相同网段（广播域或 VLAN）的交换机作为 Firewall Threat Defense 设备的故障转移接口。专用状态链路的要求与故障转移链路相同，只是必须与故障转移链路位于不同的网段上。

注释 使用交换机的优点是，如果设备的其中一个接口发生故障，可以轻松确定哪一个接口出现故障。如果使用直连电缆连接，那么当一个接口发生故障时，链路将在两个对等体上断开，这样将难以确定哪台设备出现故障。

- 使用以太网电缆直接连接设备，无需外部交换机。Firewall Threat Defense 在其铜缆以太网端口上支持自动 MDI/MDIX，因此您可以使用交叉电缆或直通电缆。如果使用的是直通电缆，接口会自动检测该电缆，并将其中一个发送/接收对交换为 MDIX。

使用长距离故障转移时，为实现最佳性能，状态链路的延迟应低于 10 毫秒且不超过 250 毫秒。如果延迟超过 10 毫秒，重新传输故障转移消息会导致一些性能降级。

避免中断故障转移和数据链路

我们建议，让故障转移链路和数据接口使用不同的路径，以便降低所有接口同时发生故障的可能性。如果故障转移链路发生故障，Firewall Threat Defense设备可使用数据接口来确定是否需要进行故障转移。随后，故障转移操作会被暂停，直到故障转移链路恢复正常。

请参阅以下连接情景，以设计具有弹性的故障转移网络。

情景 1 - 不推荐

如果单台交换机或一组交换机用于连接两台 Firewall Threat Defense设备之间的故障转移和数据接口，则交换机或交换机间链路发生故障时，两台 Firewall Threat Defense设备都将处于主用状态。因此，建议**不要**使用下图中显示的 2 种连接方法。

图 *1:* 使用单交换机连接 - 不推荐

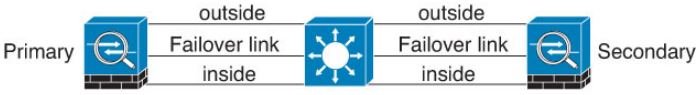
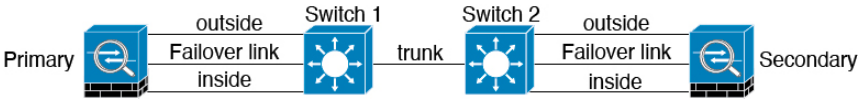


图 *2:* 使用双交换机连接 - 不推荐



情景 2 - 推荐

我们建议不要让故障转移链路和数据接口使用相同的交换机，而是应使用不同的交换机或使用直连电缆来连接故障转移链路，如下图所示。

图 *3:* 使用其他交换机连接

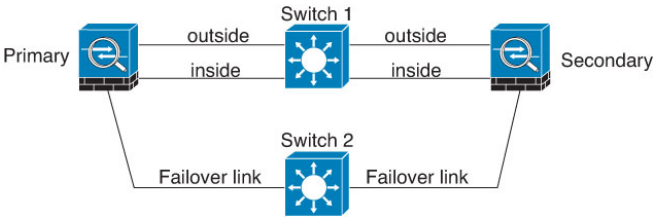
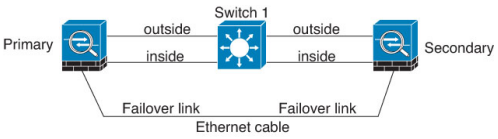


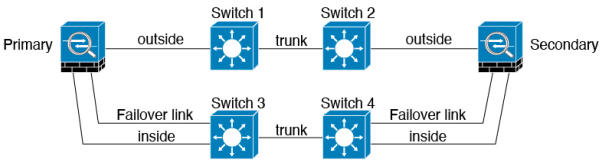
图 *4:* 通过电缆连接



情景 3 - 推荐

如果 Firewall Threat Defense数据接口连接到多台交换机，则故障转移链路可以连接到其中一台交换机，最好是处于网络的安全一侧（内部）的交换机，如下图所示。

图 *5:* 使用安全交换机连接



状态故障转移如何影响用户连接

主用设备与备用设备共享连接状态信息。这意味着，备用设备可以保持某些类型的连接，而不会影响用户。

但是，有一些类型的连接不支持状态故障转移。对于这些连接，如果发生故障转移，用户需要重新建立连接。通常，连接会根据连接中所用协议的行为自动进行。

以下主题介绍状态故障转移支持或不支持的功能。

支持的功能

支持的功能指高可用性功能中

- 能使状态信息在状态故障转移期间传递到备用 Firewall Threat Defense 设备
- 能维护连接状态及关键信息以确保流量无缝传输；以及
- 能确保故障转移期间最大限度减少中断。

状态信息类型

对于状态故障转移，这些状态信息将传至备用设备：

- NAT 转换表。
- TCP 和 UDP 连接和状态，包括 HTTP 连接状态。其他类型的 IP 协议和 ICMP 不会通过主用设备解析，因为它们是在新数据包到达时在新的主用设备上建立的。
- Snort 连接状态、检查结果和引脚信息，包括严格 TCP 实施。
- ARP 表
- 第 2 层网桥表（适用于桥接组）
- ISAKMP 和 IPsec SA 表
- GTP PDP 连接数据库
- SIP 信令会话和引脚。
- 静态和动态路由表 - 状态故障转移会参与动态路由协议（如 OSPF 和 EIGRP），因此通过主用设备上的动态路由协议获悉的路由，将会保留在备用设备的路由信息库 (RIB) 表中。发生故障转移事件时，数据包可以正常传输，并且只会对流量产生极小的影响，因为主用辅助设备一开始就具有镜像主设备的规则。进行故障转移后，新的主用设备上的重新融合计时器会立即启动。随后 RIB 表中的代编号将会增加。在重新融合期间，OSPF 和 EIGRP 路由将使用新的代编号进行更新。计时器到期后，过时的路由条目（由代编号确定）将从表中删除。于是 RIB 将包含新主用设备上的最新的路由协议转发信息。

注释 路由仅会因为主用设备上的链路打开或关闭事件而同步。如果备用设备上的链路打开或关闭，从主用设备发出的动态路由可能会丢失。这是预期的正常行为。

- DHCP 服务器 - 不会复制 DHCP 地址租用。但是，在接口上配置的 DHCP 服务器将发送 ping 命令，以确保在向 DHCP 客户端授予地址前不使用地址，使得服务不会受到影响。对于 DHCP 中继代理或 DDNS，状态信息不相关。
- 访问控制策略决策 - 在故障转移期间，会保留与流量匹配（包括 URL、URL 类别、地理位置等）、入侵检测、恶意软件和文件类型相关的决策。但是，对于在故障转移时评估的连接，有以下注意事项：
  - AVC - 系统会复制 App-ID 裁定，而不是检测状态。只要 App-ID 裁定是完整的，并且在发生故障转移之前完成同步，即可实现正确的同步。
  - 入侵检测状态 - 进行故障转移时，一旦出现拾取中间流的情况，新检测既已完成，但旧状态会丢失。
  - 文件恶意软件阻止 - 文件处置必须在故障转移之前变为可用。
  - 文件类型检测和阻止 - 文件类型必须在故障转移之前加以识别。如果在原始主用设备识别文件时发生故障转移，则文件类型不同步。即使文件策略阻止该文件类型，新的主用设备也会下载该文件。
- 来自身份策略的被动用户身份决策，并非通过主动身份验证和通过强制网络门户收集的决策。
- 安全智能决策。
- RA VPN - 故障转移后，远程访问 VPN 终端用户不必对 VPN 会话重新进行身份验证，也不必重新连接。但是，在VPN连接上运行的应用，在故障转移过程中可能会丢失数据包，并且无法从数据包丢失中恢复。
- 在所有连接中，只有已建立的连接会在备用设备上复制。

不支持的功能

不支持的功能指无法满足以下条件的设备功能

- 不会在状态故障转移中同步至备用 Firewall Threat Defense 设备
- 在故障转移事件期间不维护状态信息，以及
- 可能需要在故障转移发生后重新建立。

状态信息限制

对于状态故障转移，以下状态信息不会传送至备用 Firewall Threat Defense：

- 非 GREv0 和 IPv4-in-IP 明文隧道中的会话。不会复制隧道内部的会话，并且新的主动节点不能重复使用现有检测判定来匹配正确的策略规则。
- 已解密的 TLS/SSL 连接 - 解密状态不同步，如果主用设备发生故障，则系统会重置已解密的连接。需要与新的主用设备建立新连接。未解密的连接（也就是匹配TLS/SSL“不解密”规则操作的连接）不受影响，并且可以正确复制。
- 组播路由。

备用设备上允许的配置更改和操作

当设备在高可用性模式下运行时，仅需要对主用设备进行配置更改。部署配置时，新的更改也会传输到备用设备。

但某些属性是备用设备所特有的。您可以在备用设备上更改以下属性：

- 管理 IP 地址和网关。
- 自定义的登录页面。
- 用于 防火墙设备管理器 及设备 CLI 的本地管理用户账号及其密码。所有本地用户必须分别在两台设备上更改各自的密码。若在主用设备上创建了本地管理用户，必须在备用设备上同样创建，因为用户账号不会同步。

此外，您还可以在备用设备上执行以下操作。

- 高可用性操作（例如暂停、恢复、重置和中断HA）以及在主用设备和备用设备之间进行模式切换。
- 每个设备的控制面板和事件数据是唯一的，并且是不同步的。这包括事件查看器中的自定义视图。
- 每个设备的审核日志信息是唯一的。
- 智能许可注册。前提是，您必须启用或禁用主用设备上的可选许可证，并且该操作是与备用设备同步的，用于请求或释放相应的许可证。
- 备份，但不进行恢复。要恢复备份，您必须中断设备上的HA。如果备份包括HA配置，设备将重新加入高可用性组。
- 软件升级安装。
- 生成故障排除日志。
- 手动更新地理位置或安全智能数据库。这些数据库在设备之间不同步。如果您创建更新计划，设备可以独立地保持一致。
- 您可以从 **监控 (Monitoring)** > **会话 (Monitoring)** 页面查看活动 防火墙设备管理器 用户会话，并删除会话。

高可用性的系统要求

以下主题介绍整合高可用性配置中的两台设备之前必须满足的要求。

高可用性的硬件要求

要将高可用性配置中的两台设备链接在一起，必须满足以下硬件要求。

- 设备的硬件型号必须完全相同。

对于 Firepower 9300，高可用性仅在同种类型模块之间受支持；但是两个机箱可以包含混合模块。例如，各机箱均具有 SM-36 和 SM-44。可以在 SM-36 模块之间和 SM-44 模块之间创建高可用性对。

- 设备接口的数量和类型必须相同。

  对于 Firepower 4100/9300 机箱，在启用 HA 之前，所有接口必须在 FXOS 中进行完全相同的预配置。如果在启用 HA 后更改接口，请在备用设备上的 FXOS 中更改接口，然后在主用设备上进行相同更改。

- 设备安装的模块必须相同。例如，如果具有可选的网络接口模块，则必须在另一台设备中安装相同的模块。

- 不支持 Firepower 9300 的机箱内高可用性。不能在位于同一个机箱中的独立逻辑设备之间配置 HA。

高可用性的软件要求

要将两台设备链接到高可用性配置，必须满足以下软件要求。

- 设备必须运行完全相同的软件版本，也即，主要版本号（第一个）、次要版本号（第二个）以及维护版本号（第三个）都必须相同。您可以在 防火墙设备管理器 的 **设备 (Devices)** 页面，或者可以在 CLI 中使用 **show version** 命令找到版本。允许连接具有不同版本的设备，但配置不会导入备用设备且故障转移无法使用，直到您将设备升级到同一软件版本。

- 两台设备必须在本地管理器模式下运行，也即，使用 防火墙设备管理器配置设备。如果您可以在两个系统上登录防火墙设备管理器 ，则表示这两台设备是本地管理器模式。您还可以在 CLI 中使用 **show managers** 命令进行验证。

- 必须在每台设备中完成初始设置向导。

- 每台设备都必须有自己的管理 IP 地址。管理接口的配置在两台设备之间未同步。

- 设备必须具有相同的 NTP 配置。

- 不能配置任何接口使用 DHCP 获取地址。也就是说，所有接口都必须有静态 IP 地址。

- 对于云服务，两台设备必须在同一区域注册，或者两台设备都不能注册。您不能采用混合云服务注册。

- 在配置高可用性之前，必须先部署任何待处理更改。

高可用性的许可证要求

在配置高可用性之前，设备必须处于相同的状态：两台设备均注册基础版许可证，或均处于评估模式。如果设备已注册，可以将其注册到不同的思科智能软件管理器账户，但这些账户的出口控制功能设置的状态必须相同，要么都启用这类设置，要么都禁用。但是，如果您已在设备上启用不同的可选许可证，上述设置便不再重要。如果注册两台设备，则必须为它们选择相同的思科云服务区域。

如果设备已注册，它们必须使用相同的模式，即“智能许可证”或“永久许可证预留”(PLR)。

在运行过程中，高可用性对中的设备必须具有相同的许可证。在部署过程中，主用设备进行的任何许可证更改都会在备用设备上重复进行。

高可用性配置需要两种智能许可证权利；对中的每个设备各一个。您必须确保您的账户中有足够的许可证，可应用到每个设备。如果没有足够的许可证，可能会出现一台设备合规，另一台设备不合规的情况。

例如，如果主用设备具有 基础版 许可证和 IPS ，而备用设备只有 基础版 许可证，备用设备将与思科智能软件管理器通信，以从您的帐户获取可用 IPS 。如果您的智能许可证账户没有足够的已购授权，您的账户将不合规（且备用设备也将不合规，即使主用设备合规），直到您购买正确数量的许可证。

注意：

- 如果将用户注册到存在不同出口控制功能设置的账户，或者尝试创建一个 HA 对，注册其中的一台设备，而将另外一台设备设置为评估模式，则 HA 加入可能会失败。
- 对于出口控制功能，如果您使用不一致的设置配置 IPSec 加密密钥，当您激活 HA 后，两个设备都将变为主用状态。这会影响受支持网段上的路由，且您必须手动断开辅助设备上的 HA 才能消除影响。
- 请勿在创建 HA 组的过程中更改许可。在高可用性加入时，两个设备必须具有相同的配置，否则您将看到以下错误：“FDM validation failure - Cloud Service registration status mismatch between Primary and Secondary Node.”（FDM 验证失败 - 主节点和辅助节点之间的云服务注册状态不匹配）。有关详细信息，请查看 app-sync-history CLI。”

高可用性准则

型号支持

- Firepower 9300 - 可以在 Firepower 9300上配置 HA。但是，不能在位于同一个 Firepower 9300 机箱中的独立逻辑设备之间配置 HA。
- Firepower 1010 和安全防火墙 1210/1220：
  - 使用高可用性时，不应使用交换机端口功能。由于交换机端口在硬件中运行，因此它们会继续在主用和备用设备上传递流量。高可用性旨在防止流量通过备用设备，但此功能不延伸至交换机端口。在正常高可用性网络设置中，两台设备上的活动交换机端口将导致网络环路。建议将外部交换机用于任何交换功能。请注意，VLAN 接口可通过故障转移监控，而交换机端口无法通过故障转移监控。理论上，您可以将单个交换机端口置于 VLAN 上并成功使用高可用性，但更简单的设置是使用物理防火墙接口。
  - 仅可使用防火墙接口作为故障转移链路。
  - 当机箱处于高可用性对时，备用设备的“活动”LED 呈琥珀色光。
- （Firepower 1000 系列）- 在 HA 中部署配置了数百个接口的设备， 会导致故障转移时间（秒）延迟增加。

- Firewall Threat Defense Virtual — 对于 Microsoft Azure 云或 Amazon Web Services (AWS) 云，Firewall Threat Defense Virtual 不支持 HA 配置。

其他准则

- 169.254.0.0/16 和 fd00:0:0:*::/64 是内部使用的子网，不能用于故障转移或状态链路。
- 当您在主用设备上运行部署作业时，主用设备的配置会同步到备用设备。但是，在您部署更改之前，某些更改不会显示在待处理更改中，即使它们还未同步到备用设备上。如果您更改以下任一一项，所做的更改将会被隐藏，且您必须运行部署作业才能使它们配置在备用设备上。如果您需要立即应用更改，您将需要进行一些其他更改，这些更改会显示在待处理更改中。隐藏的更改包括对以下项目的编辑：规则计划、空间数据库、安全智能或 VDB 更新；备份计划；NTP； 管理连接的 HTTP 代理；许可证授权；云服务选项；URL 过滤选项。
- 您应在主设备和辅助设备上执行备份。要恢复备份，您必须首先中断高可用性。不要在两台设备上恢复相同备份，因为这两台设备都会变成活动状态。相反，您要在想要首先恢复活动状态的设备上恢复备份，然后在另一台设备上恢复等效备份。
- 适用于各种身份源的**测试**按钮仅在主用设备上可用。如果您需要测试备用设备的身份源连接，必须先切换模式，使备用对等体变成主用对等体。
- 创建或中断高可用性配置会在部署配置更改后重新启动两台设备上的 Snort 检测过程。这可能会导致直通流量中断，直到进程完全重新启动。
- 最初配置高可用性时，如果辅助设备上的安全智能和地理位置数据库的版本与主设备上的版本不同，请在辅助设备上安排作业来更新数据库。下一次部署时，从主用设备运行这些作业。即使高可用性加入失败，这些作业仍将保留，并将在下一次部署时执行。
- 当主用设备故障转移到备用设备时，所连接的运行生成树协议 (STP) 的交换机端口在感知到拓扑变化时，会进入阻塞状态 30 秒至 50 秒。当端口处于阻塞状态时，为避免流量丢失，您可以根据交换机启用 STP PortFast 功能：

  interface *interface_id* **spanning-tree portfast**

  此解决方法适用于连接到路由模式和桥接组接口的交换机。链路打开时，PortFast 功能会立即使端口转换到 STP 转发模式。该端口仍会参与 STP。因此，如果端口是环路的一部分，则端口最终会转换为 STP 阻塞模式。
- 发生故障转移事件时，在连接到高可用性对的交换机上配置端口安全性，可能会导致通信问题。一个安全端口上配置或获悉的安全 MAC 地址移至另一安全端口，交换机端口安全功能标记违规时，会发生此问题。
- 对于主用/备用高可用性和 VPN IPSec 隧道，无法使用 SNMP 通过 VPN 隧道监控主用设备和备用设备。备用设备没有有效的 VPN 隧道，将丢弃发往网络管理系统 (NMS) 的流量。您可以改为使用具有加密功能的 SNMPv3，因此不需要 IPsec 隧道。
- 用于高可用性故障转移和有状态故障转移链路的接口无需启用。接口状态应显示链路正常，但接口本身可能显示为已禁用。此外，接口信息不会使用高可用性配置中定义的 IP 地址进行更新。

配置高可用性

借助高可用性设置，即使设备发生故障，也可确保网络连接。设置主用/备用高可用性时，两台设备将链接到一起。如果主用设备发生故障，备用设备会接管相应的角色，因此用户几乎察觉不到连接问题。

以下过程介绍设置主用/备用高可用性 (HA) 对的　端到端流程。

过程

步骤 1 准备两台用于高可用性的设备，第 13 页。

步骤 2 配置高可用性的主设备，第 15 页。

步骤 3 配置高可用性的辅助设备，第 17 页。

步骤 4 配置故障转移运行状况监控条件，第 18 页。

条件包括对等体监控和接口监控。虽然所有故障转移条件都有默认设置，您至少应检查这些设置，验证是否适用于您的网络。

- 配置对等体运行状况监控故障转移条件，第 19 页。
- 配置接口运行状况监控故障转移条件，第 20 页。

  有关接口测试的信息，请参阅系统如何测试接口运行状况，第 21 页。

步骤 5 （推荐的可选项目。）配置备用 IP 地址和 MAC 地址，第 22 页。

步骤 6 （可选。）验证高可用性配置，第 23 页。

准备两台用于高可用性的设备

要成功配置高可用性，您需要正确做好多项准备。

过程

步骤 1 确保设备满足高可用性的硬件要求，第 9 页中列出的要求。

步骤 2 确定使用一个故障转移链路，还是使用单独的故障转移和状态故障转移链路，并确定您将使用的端口。

必须在每台设备上为每个链路使用相同的端口号。例如，在两台设备上均对故障转移链路使用 GigabitEthernet 1/3。确定您要使用哪些端口，避免将其意外用于其他用途。有关详细信息，请参阅故障转移和状态故障转移链路，第 3 页。

步骤 3 安装设备，将其连接到网络，并在每个设备上完成初始设置向导。

a) 查看避免中断故障转移和数据链路，第 5 页中的建议网络设计。
b) 必须至少连接外部接口，如连接接口中所述。

您还可以连接其他接口，但是必须确保在每个设备上使用相同的端口连接到指定子网。由于设备将共享相同的配置，必须将它们以并行方式连接到网络中。

注释
安装向导不允许更改管理和内部接口上的 IP 地址。因此，如果您将主要设备上的这些接口连接到网络，不要同时连接辅助设备上的同类接口，否则 IP 地址会发生冲突。您可以直接将工作站连接到其中一个接口并通过 DHCP 获取地址，以便您可以连接到 防火墙设备管理器 并配置设备。

c) 在每台设备上完成初始设置向导。确保指定外部接口的静态 IP 地址。此外，配置相同的 NTP 服务器。有关详细信息，请参阅使用设置向导完成初始配置。

为设备选择相同的许可和 Cisco Success Network 选项。例如，为每个设备选择评估模式或注册设备。

d) 在辅助设备上，依次选择**设备** > **系统设置** > **管理接口**并配置唯一的 IP 地址，更改网关（如有必要），并更改或禁用 DHCP 服务器设置，以满足您的需求。
e) 在辅助设备上，依次选择**设备** > **接口**并编辑内部接口。删除或更改 IP 地址。此外，删除为接口定义的 DHCP 服务器，因为不能在同一网络上有两个 DHCP 服务器。
f) 在辅助设备上部署配置。
g) 根据您的网络拓扑要求，登录到主设备，更改管理地址、网关与 DHCP 服务器设置以及内部接口 IP 地址与 DHCP 服务器设置。如果您进行任何更改，请部署配置。
h) 如果您未连接内部接口或管理接口（如果您使用单独的管理网络），现在可以将其连接到交换机。

步骤 4 验证设备是否具有完全相同的软件版本，也即，主要版本号（第一个）、次要版本号（第二个）以及维护版本号（第三个）都必须相同。您可以在设备页面 防火墙设备管理器 中，或者可以在 CLI 中使用 **show version** 命令找到版本。

如果设备未运行相同的软件版本，从 Cisco.com 获取首选的软件版本并将其安装在每台设备上。有关详细信息，请参阅升级 Firewall Threat Defense。

步骤 5 连接和配置故障转移和状态故障转移链路。

a) 按照您的首选网络设计（从避免中断故障转移和数据链路，第 5 页选择），酌情将每台设备的故障转移接口连接到交换机或直接互连。
b) 如果使用单独的状态链路，也请相应地连接每台设备的状态故障转移接口。
c) 依次登录到每台设备，然后转至**设备** > **接口**。编辑每个接口，并验证没有配置接口名称或 IP 地址。

如果为接口配置了名称，您可能需要从安全区中删除这些接口和其他配置，然后才能删除名称。如果删除名称失败，检查错误消息以确定需要进行哪些其他更改。

步骤 6 在主设备上，连接剩余的数据接口并配置设备。

a) 选择**设备** > **接口**，编辑用于直通流量的每个接口和配置主要静态 IP 地址。

b) 将接口添加到安全区，并配置处理已连接网络上的流量所需的基本策略。有关示例配置，请参阅最佳实践： Firewall Threat Defense的使用案例中列出的主题。

c) 部署配置。

步骤 7 验证您是否达到高可用性的软件要求，第 10 页中所述的所有要求。

步骤 8 确认您有一致的许可（注册或评估模式）。有关详细信息，请参阅高可用性的许可证要求，第 10 页。

步骤 9 在辅助设备上，将其余数据接口连接到主要设备上对等接口连接的网络。不要配置接口。

步骤 10 在每个设备上，依次选择**设备** > **系统设置** > **云服务**并确认设置相同。

现在您即可在主设备上配置高可用性。

配置高可用性的主设备

要设置主用/备用高可用性对，必须先配置主设备。主设备是您打算在正常情况下应该处于主用模式的设备。辅助设备保持备用模式，直到主设备不可用。

选择您要当做主设备的设备，然后在该设备上登录 防火墙设备管理器 并按照此程序操作。

注释 创建高可用性对后，必须拆分对，才能够按照此过程中的说明编辑配置。

开始之前

确保您为故障转移和状态故障转移链路配置的接口尚未命名。如果当前接口已命名，您必须从使用这些接口的任何策略（包括安全区对象）中将其删除，然后编辑接口以删除名称。接口还必须处于路由模式，而不是被动模式。这些接口必须专用于高可用性配置：不能将其用于任何其他用途。

如果存在任何待处理的更改，必须先部署这些更改，然后才能配置高可用性。

过程

步骤 1 点击**设备**。

步骤 2 在设备摘要的右侧，点击**高可用性**组旁边的**配置**。

如果您在设备上第一次配置高可用性，该组将如下所示。

步骤 3 在“高可用性”(High Availability) 页面上，点击**主设备 (Primary Device)** 框。

如果已配置辅助设备，并已将配置复制到剪贴板，您可以点击**从剪贴板粘贴**按钮并粘贴配置。这将使用适当的值更新字段，稍后，您可以验证这些值。

步骤 4 配置**故障转移链路**属性。

故障转移对中的两台设备会不断地通过故障转移链路进行通信，以确定每台设备的运行状态和同步配置更改。有关详细信息，请参阅故障转移链路，第 4 页。

- **物理接口** - 选择连接到辅助设备用作故障转移链路的接口。此接口必须是未命名的接口。

  使用 EtherChannel 接口作为故障转移链路或状态链路时，必须在建立高可用性之前，确认具有相同 ID 和成员接口的同一 EtherChannel 在两台设备上都存在。如果 EtherChannel 不匹配，您需要先禁用 HA 并更正辅助设备的配置。要阻止无序数据包，仅使用 EtherChannel 中的一个接口。如果该接口发生故障，则会使用 EtherChannel 中的下一个接口。您不能在 EtherChannel 配置用作故障转移链路时对其进行修改。

- **类型** - 选择是否对接口使用 IPv4 或 IPv6 地址。只能配置一种类型的地址。

- **主 IP** - 为此设备上的接口输入 IP 地址。例如：192.168.10.1。对于 IPv6 地址，您必须采用标准表示法添加前缀长度，例如 2001:a0a:b00::a0a:b70/64。

- **辅助 IP** - 输入应在链路的另一端为辅助设备上的接口配置的 IP 地址。地址必须与主地址位于同一子网，且必须与主地址不同。例如，192.168.10.2 或 2001:a0a:b00::a0a:b71/64。

- **子网掩码**（仅限 Ipv4） - 输入主/辅助 IP 地址的子网掩码。

步骤 5 配置状态故障转移链路属性。

系统使用状态链路将连接状态信息传送到备用设备。此信息可在发生故障转移时帮助备用设备保留现有连接。您可以使用同一链路作为故障转移链路，也可以配置一个单独的链路。

- **使用相同的接口作为故障转移链路** - 如果您想对故障转移和状态故障转移通信使用单一链路，请选择此选项。如果选择此选项，请继续执行下一步。

- **物理接口** - 如果您想要使用单独的状态故障转移链路，请选择连接到辅助设备的接口，以用作状态故障转移链路。此接口必须是未命名的接口。然后，配置以下属性：

  - **类型** - 选择是否对接口使用 IPv4 或 IPv6 地址。只能配置一种类型的地址。

  - **主 IP** - 为此设备上的接口输入 IP 地址。地址必须与用于故障转移链路的地址位于不同子网。例如：192.168.11.1。对于 IPv6 地址，您必须采用标准表示法添加前缀长度，例如 2001:a0a:b00:a::a0a:b70/64。

  - **辅助 IP** - 输入应在链路的另一端为辅助设备上的接口配置的 IP 地址。地址必须与主地址位于同一子网，且必须与主地址不同。例如，192.168.11.2 或 2001:a0a:b00:a::a0a:b71/64。

  - **子网掩码**（仅限 Ipv4） - 输入主/辅助 IP 地址的子网掩码。

步骤 6 （可选。）如果您希望对设备对中两台设备之间的通信加密，请输入 **IPsec 加密密钥**字符串。

必须在辅助节点上配置完全相同的密钥，因此请记下您输入的字符串。

如果您不输入密钥，故障转移和状态故障转移链路上的所有通信都是纯文本。如果您未在接口之间使用直连电缆连接，可能会引发安全问题。

注释

如果您在评估模式下配置 HA 故障转移加密，系统将使用 DES 进行加密。如果随后您使用出口合规账户注册设备，则设备将在重新启动后使用 AES。因此，如果系统出于任何原因重新启动，包括安装升级后，对等体将无法通信，两台设备将变为主用设备。建议您在注册设备之前不要配置加密。如果您在评估模式下进行此配置，建议您在注册设备之前删除加密。

步骤 7 点击**激活高可用性**。

系统立即将配置部署到设备。不需要启动部署作业。如果您没有看到指出配置已保存和部署正在进行的消息，请滚动至页面顶部，查看错误消息。

配置也会被复制到剪贴板。您可以使用 copy 命令快速配置辅助设备。为提高安全性，加密密钥不包含在剪贴板复制内容中。

配置完成后，您会收到介绍后续操作的消息。阅读信息后，点击**明白**。

此时，您应转至“高可用性”页面，且设备状态应为“协商”(Negotiating)。此状态应在配置对等体之前切换为“主用”，且对等体应显示为“故障”，直至开始配置此设备。

现在，您可以配置辅助设备。请参阅配置高可用性的辅助设备，第 17 页。

注释
所选的接口不直接配置。但是，如果您在 CLI 中输入 **show interface**，您将看到接口正在使用指定的 IP 地址。如果您配置了单独的状态链路，接口被命名为“failover-link”和“stateful-failover-link”。

配置高可用性的辅助设备

为主用/备用高可用性配置主设备后，必须再配置辅助设备。在此设备上登录 防火墙设备管理器 并按照此过程操作。

注释 如果您尚未执行此操作，请将高可用性配置从主设备复制到剪贴板。使用复制/粘贴配置辅助设备比手动输入数据更容易。

过程

步骤 1 点击**设备**。

步骤 2 在设备摘要的右侧，点击**高可用性**组旁边的**配置**。

如果您在设备上第一次配置高可用性，该组将如下所示。

步骤 3 在“高可用性”页面上，点击**辅助设备 (Secondary Device)** 框。

步骤 4 执行以下操作之一：

- **简单方法** - 点击**从剪贴板粘贴**按钮，粘贴配置并点击**确定**。这将使用适当的值更新字段，稍后，您可以验证这些值。
- **手动方法** - 直接配置故障转移和状态故障转移链路。在辅助设备上输入与主设备完全相同的设置。

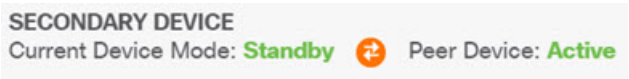
步骤 5 如果在主设备上配置了 **IPSec 加密密钥**，请在辅助设备上输入完全相同的密钥。

步骤 6 点击**激活高可用性**。

系统立即将配置部署到设备。不需要启动部署作业。如果您没有看到指出配置已保存和部署正在进行的消息，请滚动至页面顶部，查看错误消息。

配置完成后，您将收到说明已配置高可用性的消息。点击**明白**关闭该消息。

此时，您应转至“高可用性”(High Availability) 页面，且设备状态应指明此设备为辅助设备。如果与主设备连接成功，设备将与主设备同步，且最终模式应为备用、对等体应为主用模式。



注释
所选的接口不直接配置。但是，如果您在 CLI 中输入 **show interface**，您将看到接口正在使用指定的 IP 地址。如果您配置了单独的状态链路，接口被命名为“failover-link”和“stateful-failover-link”。

配置故障转移运行状况监控条件

采用高可用性配置的设备会监控自身的整体运行状况和接口运行状况。

故障转移条件定义运行状况监控度量，以此确定对等体是否发生故障。如果主用对等体违反了故障转移条件，会触发故障转移，切换到备用设备。如果备用对等体违反了故障转移条件，它将被标记为故障，且无法进行故障转移。

您可以仅在主用设备上配置故障转移条件。

下表列出了故障转移触发事件及关联的故障检测时间。

表 *2:* 基于故障转移条件的故障转移时间

故障触发事件	最小	默认	最大
主用设备断电或停止正常工作。	800 毫秒	15 秒	45 秒

故障触发事件	最小	默认	最大
主用设备接口物理链路关闭。	500 毫秒	5 秒	15 秒
主用设备接口正常运行，但是连接问题引发了接口测试。	5 秒	25 秒	75 秒

以下主题介绍如何自定义故障转移运行状况监控条件以及系统如何测试接口。

配置对等体运行状况监控故障转移条件

高可用性配置中的每个对等体均通过使用 hello 消息监控故障转移链路判断另一个对等体的运行状况。当设备在故障转移链路上没有收到三条连续的hello消息时，设备会在每个数据接口（包括故障转移链路）上发送 LANTEST 消息，以验证对等体是否响应。设备采取的操作取决于另一台设备的响应。

- 如果设备在故障转移链路上收到响应，则不会进行故障转移。
- 如果设备在故障转移链路上未收到响应，但在数据接口上收到响应，设备不会进行故障转移。故障转移链路会标记为发生故障。您应尽快恢复故障转移链路，因为当故障转移切换发生故障时，设备无法故障转移到备用设备。
- 如果设备未在任何接口上收到响应，则备用设备会切换至主用模式，并将另一台设备分类为故障设备。

您可以配置 hello 消息的轮询和保持时间。

过程

步骤 1 在主用设备上，点击**设备**。

步骤 2 点击设备摘要右侧的**高可用性**链接。

故障转移条件将在“高可用性”(High Availability) 页面的右侧列中列出。

步骤 3 定义**对等体时间配置**。

这些设置决定主用设备可以在多短的时间内故障转移至备用设备。设置的轮询时间越快，设备便可越快检测到故障并触发故障转移。但是，当网络临时堵塞时，更快的检测会导致不必要的切换。默认设置适用于大多数情况。

如果设备在一个轮询周期内未收到故障转移接口上的hello数据包，则会通过其余接口进行其他的测试。如果在保持时间内，仍未收到来自对等体设备的响应，该设备会被视为发生故障，如果故障设备为主用设备，则备用设备会进行接管，成为主用设备。

- **轮询时间** - hello 消息之间的等待时间。输入 1-15 秒或 200 到 999 毫秒。默认值为 1 秒。

- **保持时间** - 设备必须在故障转移链路上收到 hello 消息的时间，超出此时间仍未收到，则宣布对等体发生故障。保持时间必须至少是轮询时间的 3 倍。输入 1 到 45 秒或 800 到 999 毫秒。默认值为 15 秒。

步骤 4 点击**保存**。

配置接口运行状况监控故障转移条件

您可以监控最多 211 个接口，具体取决于您的设备型号。您应监控重要的接口。例如，确保重要网络之间吞吐量的接口。仅当您为其配置备用 IP 地址且接口应始终开启时，才监控接口。

当设备在 2 个轮询期内，未在受监控的接口上收到 hello 消息时，将运行接口测试。如果对于某个接口，所有接口测试均失败，但在另一设备上的此接口继续成功传送流量，则此接口会被视为发生故障。如果达到故障接口的阈值，则会进行故障转移。如果另一设备的接口在所有网络测试中也全部失败，则这两个接口会进入“Unknown”状态，并且不会计入故障转移限制。

如果接口收到任何流量，则该接口会再次变为正常工作状态。如果不再满足接口故障阈值，发生故障的设备将恢复为备用模式。

您可以使用 **show monitor-interface** 命令，从 CLI 或 CLI 控制台监控接口 HA 状态。有关详细信息，请参阅监控高可用性监控接口的状态，第 35 页。

注释 接口关闭时，为了进行故障转移，该接口仍被视为是设备问题。如果设备检测到接口已关闭，将立即发生故障转移（如果您保留 1 个接口的默认阈值），而不等待接口保持时间。仅当设备将接口状态视为正常时，接口保持时间才有用，尽管设备并不从对等体接收 hello 数据包。

开始之前

默认情况下，所有已命名的物理接口均进行高可用性监控。因此，您应禁止监控不重要的物理接口。对于子接口或网桥组，您必须手动启用监控。

要完全禁用接口监控并防止因接口故障导致的故障转移，只需确保未对接口启用高可用性监控。

过程

步骤 1 在主用设备上，点击**设备**。

步骤 2 点击设备摘要右侧的**高可用性**链接。

故障转移条件将在“高可用性”(High Availability) 页面的右侧列中列出。

步骤 3 定义**接口故障阈值**。

如果故障接口的数量达到阈值，设备会将自身标记为发生故障。如果设备是主用设备，它会故障转移到备用设备。如果设备是备用设备，通过将自身标记为发生故障，主用设备会将此设备视为不可用于故障转移。

设置此条件时，请考虑您要监控多少个接口。例如，如果您仅在 2 个接口上启用监控，则永远不会达到10个接口的阈值。编辑接口属性时，通过选择**高级选项**选项卡上的**启用高可用性监控**选项，配置接口监控。

默认情况下，如果其中一个监控接口发生故障，设备会将自身标记为故障。

您可以通过选择以下**故障转移条件**选项之一设置接口故障阈值：

- **超出故障接口数**-输入接口的原始值。默认值为1。最大值实际上取决于设备型号，可能不尽相同，但您不能输入超过 211 个。使用此条件时，如果输入的数字超过设备支持的数量，将出现部署错误。请尝试较小的数字或改为使用百分比。
- **超出故障接口的百分比** - 输入 1 到 100 之间的数字。例如，如果您输入 50%，且您正在监控 10 个接口，那么如果 5 个接口发生故障，设备会将自身标记为故障。

步骤 4 定义**接口时间配置**。

这些设置决定了主用设备能够以多快的速度确定接口是否发生故障。设置的轮询时间越快，设备便可越快检测到接口故障。但是，更快的检测速度可能也会导致繁忙的接口在实际状况良好时被标记为故障，从而造成不必要的频繁故障转移。默认设置适用于大多数情况。

如果接口链路关闭，则不会执行接口测试，如果发生故障的接口数达到或超出配置的接口故障转移阈值，备用设备可能仅在一个接口轮询周期内就会变为主用状态。

- **轮询时间** - 在数据接口上发出 hello 数据包的频率。输入 1-15 秒或 500 到 999 毫秒。默认值为 5 秒。
- **保持时间** - 保持时间确定，从一个 hello 数据包丢失到接口被标记为发生故障的时长。输入 5 - 75 秒。输入的保持时间不得短于设备轮询时间的 5 倍。

步骤 5 点击**保存**。

步骤 6 对您想要监控的每个接口启用高可用性监控。

a) 选择**设备** > **接口**。

如果接口被监控，高可用性列的监视器将指示“已启用”。

b) 对要更改监控状态的接口，点击编辑图标 ( )。

您无法编辑故障转移或状态故障转移接口。接口监控不适用于这些接口。

c) 点击**高级选项**选项卡。

d) 根据需要，选中或取消选中**启用高可用性监控**复选框。

e) 点击**确定**。

步骤 7 （可选，但不推荐。）为监控的接口配置备用IP地址和MAC地址。请参阅配置备用IP地址和MAC地址，第 22 页。

系统如何测试接口运行状况

系统将持续测试监控的接口，确保高可用性正常。用于测试接口的地址取决于配置的地址类型：

- 如果接口上配置了 IPv4 和 IPv6 地址，设备会使用 IPv4 地址执行运行状况监控。
- 如果接口上仅配置了 IPv6 地址， 设备会使用 IPv6 邻居发现，而不是 ARP 来执行运行状况监控测试。对于广播 Ping 测试， 设备会使用所有的 IPv6 节点地址 (FE02::1)。

系统将在每台设备上执行以下测试：

1. 链路打开/关闭测试 - 一种接口状态测试。如果链路打开/关闭测试指示接口关闭，则视为设备测试失败。如果状态为打开，则设备执行网络活动测试。
2. 网络活动测试 - 接收的网络活动测试。此测试旨在使用 LANTEST 消息生成网络流量，以确定发生故障的设备（如有）。测试开始时，每台设备会清除其接口的收到的数据包计数。在测试期间（最多5秒），一旦设备收到数据包，则接口会被视为正常运行。如果一台设备收到流量，另一设备未收到，则未收到流量的设备会被视为已发生故障。如果两台设备均未收到流量，则设备开始进行 ARP 测试。
3. ARP 测试 - 读取设备 ARP 缓存，以获取 2 个最近获得的条目。设备会逐一向这些设备发送 ARP 请求，从而尝试激发网络流量。在每次请求之后，设备会对最多 5 秒内收到的所有流量进行计数。如果收到流量，接口会被视为正常工作。如果未收到任何流量，系统会将 ARP 请求发送到下一台设备。如果到达列表末尾，也没有设备收到流量，设备开始进行 ping 测试。
4. Broadcast Ping 测试 - 包括发出广播 ping 请求的 ping 测试。随后设备会对最多 5 秒内收到的所有数据包进行计数。如果在此时间间隔内的任意时刻收到任何数据包，接口会被认为正常工作，并且会停止测试。如果未收到任何流量，测试将通过 ARP 测试再次开始。

配置备用 IP 地址和 MAC 地址

当您配置接口时，可以在相同网络上指定一个主用 IP 地址和一个备用 IP 地址。虽然建议指定备用 IP 地址，但它并不是必需的。如果没有备用 IP 地址，则主用设备无法执行用于检查备用接口运行状态的网络测试；它只能跟踪链路状态。此外，您也无法出于管理目的，连接到该接口上的备用设备。

1. 当主设备进行故障切换时，辅助设备会使用主设备的 IP 地址和 MAC 地址，并开始传送流量。
2. 此时处于备用状态的设备会接管备用 IP 地址和 MAC 地址。

由于网络设备不会发现 MAC 与 IP 地址配对的变化，网络上的任意位置都不会发生 ARP 条目变化或超时。

如果辅助设备启动时未检测到主设备，辅助设备将成为主用设备，并使用其自己的 MAC 地址，因为它不知道主设备的 MAC 地址。不过，当主设备可用时，辅助（主用）设备会将 MAC 地址更改为主设备的 MAC 地址，这可能会导致网络流量中断。同样，如果您用新硬件替换主设备，将使用新 MAC 地址。

使用虚拟 MAC 地址可防范这种中断，因为对于启动时的辅助设备，主用 MAC 地址是已知的，并在采用新的主设备硬件时保持不变。您可以手动配置虚拟 MAC 地址。

如果您没有配置虚拟 MAC 地址，则可能需要清除连接的路由器上的 ARP 表，以便恢复流量。当 MAC 地址发生变化时，设备不会发送静态 NAT 地址的免费 ARP，因此连接的路由器不会知道这些地址的 MAC 地址发生变化。

过程

步骤 1 选择**设备** > **接口**。

您至少应为进行高可用性监控的接口配置备用 IP 和 MAC 地址。如果接口被监控，高可用性列的监视器将指示“已启用”。

步骤 2 对要配置备用地址的接口，点击编辑图标 ( )。

您无法编辑故障转移或状态故障转移接口。配置高可用性时，您可以为这些接口设置 IP 地址。

步骤 3 在 **IPv4 地址**和 **IPv6 地址**选项卡上配置备用 IP 地址。

此接口在备用设备上使用备用地址。如果未设置备用IP地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。为要使用的每个 IP 版本配置备用地址。

步骤 4 点击**高级选项**选项卡，配置 MAC 地址。

默认情况下，系统对接口使用预烧到网络接口卡(NIC)的MAC地址。因此，该接口上的所有子接口都使用相同的 MAC 地址，也因此您可能想要为每个子接口创建唯一地址。如果您配置高可用性，建议手动配置主用/备用 MAC 地址。定义 MAC 地址有助于在故障转移时保持网络中的一致性。

- **MAC 地址** - 采用 H.H.H 格式的介质访问控制地址，其中 H 是 16 位十六进制数字。例如，您可以将 MAC 地址 00-0C-F1-42-4C-DE 输入为 000C.F142.4CDE。MAC 地址不能设置组播位，即左起第二个十六进制数字不能是奇数。
- **备用 MAC 地址** - 用于高可用性。如果主用设备发生故障转移，备用设备变为主用设备，则新的主用设备开始使用主用 MAC 地址，以最大限度地减少网络中断，而原来的主用设备使用备用地址。

步骤 5 点击**确定**。

验证高可用性配置

完成高可用性配置后，验证设备的状态是否表明两台设备均运行正常并处于主用/备用模式。

您可以通过以下程序验证高可用性配置是否在工作。

过程

步骤 1 测试您的主用设备是否在使用诸如 FTP 之类的协议在不同接口上的主机之间发送文件，从而如预期传送流量。

至少应测试从一个工作站到连接到每个已配置的接口系统的连接。

步骤 2 可以通过执行以下任一操作，切换模式，使主用设备立即变成备用设备：

- 在 防火墙设备管理器上，从**设备** > **高可用性**页面的齿轮菜单上选择**切换模式**。
- 在主用设备的 CLI 中，输入 **no failover active**。

步骤 3 重复连接测试，以验证可以通过高可用性对中的另一台设备进行相同的连接。

如果测试不成功，请验证是否已将设备的接口与另一台设备上的对等接口连接到相同的网络上。

您可以从“高可用性”(High Availability) 页面查看 HA 状态。您还可以使用设备的 CLI 或 CLI 控制台，输入 **show failover** 命令检查故障转移状态。此外，使用 **show interface** 命令，验证任何失败的连接测试中所用接口的接口配置。

如果这些操作找不到问题的症结所在，您可以尝试其他操作。请参阅高可用性故障排除（故障转移），第 37 页。

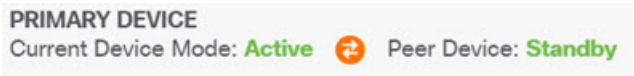
步骤 4 完成后，可以切换模式，使最初处于主用状态的设备恢复主用状态。

管理高可用性

您可以通过点击**设备**摘要页面上的**高可用性**链接，管理高可用性对。

“高可用性”页面包括以下内容：

- **角色和模式状态** - 左侧的状态区域显示设备是组中的主设备还是辅助设备。模式表示此设备处于主用模式还是备用模式，或者高可用性已被暂停还是设备正在等待加入对等体设备。它还显示对等体设备的状态，可以是主用、备用、暂停或失败状态。例如，当您登录主设备，并且该设备也是主用设备时，如果辅助设备正常并可在必要时用于故障转移，那么状态将如下所示。您可以点击对等体之间的图标获取设备之间的配置同步状态信息。

- **上次故障原因** - 如果高可用性 (HA) 配置由于某种原因（例如主用设备变得不可用并将故障转移到备用设备）而失败，则上次故障原因会显示在角色和模式状态的状态信息下方。此消息源自故障转移历史记录。
- **故障转移历史记录**链路 - 点击此链接可查看高可用性对中设备状态的详细历史记录。系统将打开 CLI 控制台并执行 **show failover history details** 命令。
- **部署历史记录**链接 - 点击此链接可转至审核日志，其中事件已过滤为仅显示部署作业。
- **齿轮按钮** - 点击此按钮可在设备上执行操作。

- **暂停高可用性/恢复高可用性** - 暂停高可用性会让设备停止作为高可用性对，但不删除高可用性配置。您可以随后在设备上恢复，也即重新启用高可用性。有关详细信息，请参阅暂停或恢复高可用性，第 25 页。
- **中断高可用性** - 中断高可用性将从两台设删除高可用性配置，并将它们恢复为独立设备。有关详细信息，请参阅中断高可用性，第 26 页。
- **切换模式** - 切换模式将强制主用设备变成备用设备，或备用设备变为主用设备，具体取决于您在哪台设备上执行操作。有关详细信息，请参阅切换主用和备用对等体（强制故障转移），第 27 页。

- **高可用性配置** - 此面板会显示故障转移对的配置。点击**复制到剪贴板**按钮将信息加载到剪贴板，从其中您可以将其粘贴到辅助设备的配置中。您可以也将其复制到另一个文件中做记录之用。此信息并不显示您是否已定义 IPsec 加密密钥。

注释 高可用性的接口配置不会反映在接口页面上（**设备**>**接口**）。您无法编辑高可用性配置中使用的接口。

- **故障转移条件** - 此面板包含在评估主用设备是否已出现故障、备用设备应变成主用设备时确定运行状况条件使用的设置。调整这些条件，以便您可以获得网络所需的故障转移性能。有关详细信息，请参阅配置故障转移运行状况监控条件，第 18 页。

以下主题介绍与高可用性配置相关的各种管理任务。

暂停或恢复高可用性

可以暂停高可用性对中的设备。此功能适用于以下情形：

- 两台设备都在主用 - 主用情况下，且修复故障切换链路上的通信不能更正问题。
- 希望对主用或备用设备进行故障排除，并且不希望设备在此期间发生故障转移。
- 您想要在备用设备上安装软件升级期间阻止故障转移。

暂停高可用性时，停止将设备对用作故障转移设备。当前主用设备保持活动状态，并处理所有用户连接。但是，不会再监控故障转移条件，并且系统永远不会故障转移到现在的伪备用设备。备用设备将保留其配置，但将保持非活动状态。

暂停 HA 和中断 HA 之间的主要区别是，在暂停的 HA 设备上将保留高可用性配置。如果中断 HA，则会清除配置。因此，您可以选择在暂停系统上恢复高可用性，这样可启用现有配置并再次将两台设备设置为故障转移对。

如果您从主用设备暂停高可用性，配置将在主用和备用设备上暂停。如果从备用设备暂停，配置仅在备用设备上暂停，但主用设备不会尝试故障转移至暂停的设备。

只能恢复处于暂停状态的设备。该设备将与对等设备协商主用/备用状态。

注释 如有必要，可以输入 **configure high-availability suspend** 命令从 CLI 暂停 HA。要恢复 HA，请输入 **configure high-availability resume**。

开始之前

如果您通过 防火墙设备管理器暂停高可用性，高可用性将一直暂停直至您进行恢复，即使您重新加载设备亦如此。但是，如果您通过 CLI 暂停，这样是一种临时状态，重新加载后，设备自动恢复高可用性配置，并与对等体协商主用/备用状态。

如果您在备用设备上暂停高可用性，请检查主用设备当前是否正在运行部署作业。如果在部署作业进行期间切换模式，部署作业将失败，配置更改也会丢失。

过程

步骤 1 点击**设备**。

步骤 2 点击设备摘要右侧的**高可用性**链接。

步骤 3 从齿轮图标 (⚙) 选择适当的命令。

- **暂停高可用性** - 系统会提示您确认操作。阅读消息，并点击**确定**。高可用性状态应显示设备处于暂停模式。
- **恢复高可用性** - 系统会提示您确认该操作。阅读消息，并点击**确定**。设备与对等体进行协商后，高可用性状态应恢复正常，或为主用或为备用状态。

中断高可用性

如果您不想让两台设备继续以高可用性对方式运行，可以中断高可用性配置。中断高可用性后，设备会变成独立设备。设备配置将发生如下变化：

- 主用设备保留中断高可用性之前的完整配置，删除高可用性配置。
- 备用设备删除所有接口配置以及高可用性配置。所有物理接口均被禁用，但不会禁用子接口。管理接口保持活动状态，因此您可以登录到设备并重新配置。

注释 或者，您可以使用 BreakHAStatus API 资源（来自 API Explorer），并使用 **interfaceOption** 属性指导系统使用备用 IP 地址重新配置备用设备的接口。如果希望获得这个结果，则必须使用 API； 防火墙设备管理器 始终禁用这些接口。请注意，系统会重新配置 IP 地址，但不会重新配置所有接口选项，因此流量的行为可能不符合预期，直到您在中断后部署更改为止。

中断实际上会如何影响设备取决于执行中断时每台设备的状态。

- 如果设备处于运行状况正常的主用/备用状态，从主用设备中断高可用性。这将从高可用性对的两台设备删除高可用性配置。如果您仅想在备用设备上中断高可用性，您必须登录该设备，先暂停高可用性，然后再中断高可用性。
- 如果备用设备处于暂停或故障状态，从主用设备中断高可用性将仅删除主用设备上的高可用性配置。必须登录备用设备，同时在该设备上中断高可用性。
- 如果对等体仍协商高可用性或同步其配置，无法中断高可用性。等待协商或同步完成或超时。如果您认为系统会停留在这种状态，您可以暂停高可用性，然后中断高可用性。

注释 使用 防火墙设备管理器时，不能使用 **configure high-availability disable** 命令从 CLI 中断 HA。

开始之前

要获得理想结果，请将设备置于正常的主用/备用状态，然后从主用设备执行此操作。

过程

步骤 1 点击**设备**。

步骤 2 点击设备摘要右侧的**高可用性**链接。

步骤 3 从齿轮图标 (⚙)，选择**中断高可用性**。

步骤 4 阅读确认消息，决定是否选择该选项以禁用接口，然后点击**确定**。

如果您从备用设备中断高可用性，必须选择该选项以禁用接口。

系统将立即在此设备和对等体设备上部署所做的更改（如果可能）。在每个设备上完成部署，并让每台设备都变成独立设备可能需要几分钟的时间。

切换主用和备用对等体（强制故障转移）

您可以对正常运行的高可用性对切换主用/备用模式，即一个对等体处于主用状态，另一个是备用状态。例如，如果您要安装软件升级，可以将主用设备切换为备用设备，以便升级不会影响用户流量。

您可以从主用或备用设备切换模式，但从另一台设备的角度来看，对等体设备必须正在运行。如果任何设备被暂停（必须先恢复高可用性）或发生故障，则无法切换模式。

注释 如有必要，可以从 CLI 在主用和备用模式之间切换。从备用设备，输入 **failover active** 命令。从主用设备，输入 **no failover active** 命令。

开始之前

在切换模式之前，验证主用设备没有在执行部署作业。等待部署完成后再切换模式。

如果主用设备包含待处理的未部署更改，请在切换模式之前部署这些更改。否则，如果您从新主用设备运行部署作业，这些更改会丢失。

过程

步骤 1 点击**设备**。

步骤 2 点击设备摘要右侧的**高可用性**链接。

步骤 3 从齿轮图标 (⚙) 中选择**切换模式**。

步骤 4 阅读确认消息，并点击**确定**。

系统将强制进行故障转移，以便主用设备成为备用设备，备用设备成为新的主用设备。

在故障转移后保留未部署的配置更改

对高可用性对中的设备进行配置更改时，需要在主用设备上编辑配置。然后部署更改，即可使用新配置同时更新主用和备用设备。主用设备是主设备还是辅助设备并不重要。

但是，未部署的更改不会在设备之间同步。任何未部署的更改仅在您做出这些更改的设备上可用。

因此，如果在有未部署更改的情况下进行故障转移，这些更改在新主用设备上不可用。但是，这些更改仍保留在现为备用状态的设备上。

要检索未部署的更改，您必须切换模式以强制进行故障转移，将另一台设备恢复为主用状态。当您登录到新主用设备时，未部署的更改可用，可以部署这些更改。使用**高可用性**设置齿轮菜单 (⚙) 中的**模式切换**命令。

记住以下几点：

- 如果从主用设备部署更改时备用设备上存在未部署的更改，备用设备上未部的署更改将被清除。这些更改无法检索。
- 当备用设备加入高可用性对时，备用设备上任何未部署的更改将被清除。每当设备加入或重新加入高可用性对时，都会同步配置。
- 如果包含未部署更改的设备发生灾难性的故障，并且您必须更换或重新映像该设备，未部署的更改会永久丢失。

在高可用性模式下更改许可证和注册

高可用性对中的设备必须具有相同的许可证和注册状态。要进行更改，请执行以下操作：

- 启用或禁用主用设备上的可选许可证。然后，部署配置，备用设备会请求（或释放）必要的许可证。启用许可证时，必须确保思科智能软件管理器账户具有足够的许可证，否则可能会造成一台设备合规，而另一台设备不合规。
- 单独注册或取消注册设备。两台设备必须均处于评估模式，或均已注册，才能正常使用。可以将设备注册到不同的思科智能软件管理器账户，但这些账户的出口控制功能设置的状态必须相同，要么都为启用，要么都为禁用。如果设备的注册状态不一致，将无法部署配置更改。

编辑 HA IPsec 加密密钥或 HA 配置

您可以通过登录到主用设备、进行更改并部署更改来更改任何故障转移条件。

但如果需要更改故障转移链路上使用的IPsec加密密钥，或更改故障转移链路或状态故障转移链路的接口或IP地址，则必须先中断HA配置。然后，可以使用新的加密密钥或故障转移/状态故障转移链路设置重新配置主设备和辅助设备。

将故障设备标记为运行状况正常

在常规运行状况监控过程中，高可用性配置中的设备可能会被标记为发生故障。如果设备运行状况正常，再次满足运行状况监控要求时，设备将恢复正常状态。如果您发现运行状况正常的设备频繁发生故障，您可能需要增加对等体超时，停止监控相对不重要的特定接口，或更改接口监控超时。

可以从CLI输入 **failover reset** 命令，强制将故障设备视为正常设备。我们建议您在主用设备上输入此命令，重置备用设备的状态。可以使用 **show failover** 或 **show failover state** 命令显示设备的故障转移状态。

将故障设备恢复到非故障状态不会自动将其设为主用设备。恢复后的设备仍处于备用状态，直到由于故障转移（强制或自然）变成主用设备。

重置设备状态不能解决导致设备被标记为故障设备的问题。如果您没有解决问题，或放宽监控超时，设备可能会被再次标记为故障设备。

升级 高可用性 Firewall Threat Defense

使用此程序可升级高可用性设备。逐一升级它们。要最大限度地减少中断，请始终升级备用设备。也就是说，升级当前的备用设备，切换角色，然后升级新的备用设备。如果您需要更新 FXOS，请在两个机箱上执行此操作，然后再在任一机箱上进行升级 Firewall Threat Defense。再次，始终升级备用设备。

⚠

注意 请勿在一台设备上进行或部署配置更改，而另一台设备正在升级或升级到混合版本对。即使系统显示为非活动，也不要在升级过程中手动重新启动或关闭；您可以将系统置于不可用状态并要求重新映像。您可以手动取消失败或正在进行的主要和维护升级，并重试失败的升级。如果问题持续存在，请联系 思科 TAC。

有关升级过程中可能遇到的这些问题和其他问题的详细信息，请参阅 高可用性 Threat Defense 升级故障排除，第 31 页。

开始之前

完成升级计划。确保部署中保持正常运行，并且能够成功通信。

注释 规划升级从阅读 Cisco Secure Firewall Threat Defense 版本说明 开始。然后，它将包括备份、获取升级包和执行相关升级（如 Firepower 4100/9300 的 FXOS）。它还包括必要的配置更改检查、 就绪性检查、磁盘空间检查，以及运行和计划任务的检查。有关详细信息，请参阅适用于您的版本的适用于 Firewall Device Manager 的 Cisco Secure Firewall Threat Defense 升级指南。

过程

步骤 1 登录备用设备。

步骤 2 选择**设备**，然后点击“更新”面板中的**查看配置** 。
“系统升级”(System Upgrade) 面板将显示当前运行的软件版本和您已上传的任何升级包。

步骤 3 上传升级包。

您只能上传一个软件包。如果上传新的软件包，它将替换旧的软件包。请确保您拥有适合您的目标版本和设备型号的软件包。点击**浏览 (Browse)** 或**替换文件 (Replace File)** 以开始上传。

上传完成后，系统将显示确认对话框。在点击**确定**之前，可以选择**立即运行升级**以选择回滚选项并立即升级。如果您现在升级，请务必完成尽可能多的升级前核对表（请参阅下一步）。

步骤 4 执行最终的升级前检查，包括就绪性检查。

重新查看预升级核对表。确保您已完成所有相关任务，尤其是最终检查。 如果不手动运行就绪性检查，它将在您启动升级时运行。如果就绪检查失败，则会取消升级。有关详细信息，请参阅运行Firewall Threat Defense的升级就绪性检查。

步骤 5 点击 **立即升级** 以开始安装过程。

a) 选择回滚选项。

您可以**升级失败时，系统将自动取消升级并回滚至上一版本**。启用此选项后，设备会在主要或维护升级失败时自动返回到升级前的状态。如果您希望能够手动取消或重试失败的升级，请禁用此选项。

b) 点击**继续**升级并重新启动设备。

您将自动注销并转到状态页面，您可以在其中监控升级，直到设备重新启动。该页面包含用于取消正在进行中的安装的选项。如果禁用了自动回滚并且升级失败，则可以手动取消或重试升级。

升级时会丢弃流量。 仅对于 ISA 3000，如果您为电源故障配置了硬件旁路，则在升级期间流量会被丢弃，但在设备完成其升级后重新启动时会通过而不进行检查。

步骤 6 尽可能重新登录并验证升级是否成功。

“设备摘要”(Device Summary) 页面显示当前运行的软件版本和高可用性状态。在验证成功且恢复高可用性之前，请勿继续操作。如果成功升级后高可用性仍处于暂停状态，请参阅 高可用性 Threat Defense 升级故障排除 ，第 31 页。

步骤 7 升级辅助设备。

a) 切换角色，使此设备处于活动状态：选择**设备** > **高可用性**，然后从齿轮菜单 (⚙) 中选择 **切换模式** 。等待设备的状态更改为活动，并确认流量正常流动。注销。

b) 升级：重复上述步骤，登录新的备用设备，上传软件包，升级设备，监控进度并验证是否成功。

步骤 8 检查设备角色。

如果您有特定设备的首选角色，请立即进行更改。

步骤 9 登录到主用设备。

步骤 10 完成升级后的任务。

a) 更新系统数据库。如果没有为入侵规则、VDB 和 GeoDB 配置自动更新，请立即进行更新。

b) 完成发行说明中所述的其他任何升级后配置更改。

c) 部署。

高可用性 Threat Defense 升级故障排除

一般升级故障排除

当您升级任何设备时，无论是独立设备还是高可用性对，都可能发生这些问题。

升级包错误。

要查找升级包正确的型号，请在 思科支持和下载站点上选择或搜索您的型号，然后浏览至相应版本的软件下载页面。列出了可用的升级包以及安装包、修补程序和其他适用的下载。升级包文件名反映平台、软件包类型（升级、补丁、修补程序）、软件版本和内部版本。

从 6.2.1 及更高版本进行升级包经过签名，并在 .sh.REL.tar 中终止。如果要从旧版本升级，请下载以 .sh 结尾的软件包。思科支持和下载站点 表示适用于您的版本的正确软件包。请勿解压已签名的升级包。请勿通过邮件来重命名升级包或传送它们。

升级期间根本无法访问设备。

设备在升级期间或在升级失败时停止传输流量。升级之前，请确保来自您所在位置的流量不必遍历设备本身即可访问设备的管理界面。

设备在升级期间显示为非活动状态或无响应。

您可以手动取消正在进行的主要和维护升级；请参阅 取消中 或重试中 Firewall Threat Defense 升级。如果设备无响应，或者如果您无法取消升级，请联系思科 TAC。

⚠

注意 即使系统显示为非活动状态，也不要在升级过程中手动重新启动或关闭。您可以将系统置于不可用状态并要求重新映像。

升级成功，但系统未按预期运行。

首先，确保缓存的信息得到刷新。不要简单地刷新浏览器窗口以重新登录。相反，请从URL中删除任何“额外”路径并重新连接到主页；例如，http://threat-defense.example.com/。

如果问题仍然存在并需要返回到较早的主要或维护版本，则可以恢复；请参阅 恢复中 Firewall Threat Defense。如果无法恢复，则必须重新映像。

升级失败。

启动主要或维护升级时，请使用 **升级失败自动取消...**（自动取消）选项，用于选择升级失败时的操作，如下所示：

- 自动取消已启用（默认）：如果升级失败，则升级会取消，并且设备会自动恢复到升级前的状态。请更正所有问题，然后重试。
- 自动取消已禁用：如果升级失败，设备将保持原样。请更正问题并立即重试，或手动取消升级并稍后重试。

有关详细信息，请参阅取消中 或重试中 Firewall Threat Defense 升级。如果无法重试或取消，或者问题持续存在，请联系思科 TAC。

高可用性升级故障排除

这些问题特定于高可用性升级。

如果未部署未提交的更改，则不会开始升级。

如果您收到一条错误消息，指出即使没有更改，也必须部署所有未提交的更改，请登录主用设备（请记住，您应该升级备用设备），创建一些细微更改，然后部署。然后，撤消更改，重新部署，并在备用设备上再次尝试升级。

如果这不起作用，并且设备根据建议运行不同的软件版本，请切换角色以使备用设备处于主用状态，然后暂停高可用性。从主用/暂停设备执行部署，恢复高可用性，然后切换角色，将主用设备再次切换为备用设备。这样，升级应该就会起作用。

从主用设备部署在备用升级期间失败，或导致应用同步错误。

如果在升级备用设备时从主用设备进行部署，可能会发生这种情况，但不支持这种情况。尽管出现错误，但仍继续进行升级。升级两台设备后，进行任何必要的配置更改并从主用设备进行部署。错误应该可以解决。

为避免这些问题，当一台设备正在升级或升级到混合版本对时，请勿在另一台设备上进行或部署配置更改。

升级期间所做的配置更改已丢失。

如果您绝对必须对混合版本对进行更改并部署，则必须对两台设备进行更改，否则在升级级别较低的主用设备后这些更改将会丢失。

升级后暂停高可用性。

升级后重新启动后，系统会暂时暂停高可用性，同时系统会执行一些最终自动化任务，例如更新库和重新启动 Snort。如果您在升级后不久登录 CLI，则很可能会注意到这一点。如果在升级完全完成且 防火墙设备管理器 可用后，高可用性无法自行恢复，请手动执行此操作：

1. 登录主用设备和备用设备，然后检查任务列表。等待所有任务在两台设备上完成运行。如果过早恢复高可用性，将来可能会出现故障转移导致中断的问题。
2. 选择 **设备** > **高可用性**，然后从齿轮菜单 (⚙) 选择 **恢复 HA** 。

混合版本对不会发生故障转移。

虽然高可用性的优势在于您可以在不中断流量或检查的情况下升级部署，但在整个升级过程中会禁用故障转移。也就是说，当一台设备处于离线状态时，不仅必须禁用故障转移（因为没有可故障转移的目标，您实际上已经进行了故障转移），而且还禁用了混合版本对的故障转移。升级期间是唯一（暂时）允许混合版本对的时间。在维护窗口期间安排升级，如果出现问题，升级的影响最小，并确保您有足够的时间在该窗口升级两台设备。

仅在一台设备上升级失败，或一台设备已恢复。该对现在运行的是混合版本。

一般操作不支持混合版本对。升级版本较低的设备或恢复较高版本的设备。对于修补程序，由于不支持恢复，如果您无法成功升级版本较低的设备，则必须中断高可用性，重新映像一个或两个设备，然后重新建立高可用性。

更换高可用性对中的设备

如有必要，您可以更换高可用性组中的一个设备，而不中断网络流量。

过程

步骤 1 如果要更换的设备能够正常使用，请确保故障转移至对等体设备，然后从该设备 CLI 使用 **shutdown** 命令正常关闭设备。如果设备不能使用，确认对等体在主用模式下运行。

如果具有管理员权限，还可以通过 防火墙设备管理器 CLI 控制台输入 **shutdown** 命令。

步骤 2 从网络中删除设备。

步骤 3 安装替换设备并重新连接接口。

步骤 4 在替换设备上完成设备安装向导。

步骤 5 在对等体设备上，转到“高可用性”(High Availability) 页面，并将配置复制到剪贴板。请注意，设备是主设备还是辅助设备。

如果有任何待处理更改，请现在部署这些更改并等待部署完成后再继续。

步骤 6 在替换设备上，点击**高可用性 (High Availability)** 中的**配置 (Configure)**，然后选择与对等体相反的设备类型。也即，如果对等体为主设备，选择**辅助**，如果对等体为辅助设备，选择**主**。

步骤 7 从对等体粘贴高可用性配置，然后输入 IPsec 密钥（如果您在使用）。点击**激活高可用性 (Activate HA)**。

部署完成后，设备将与对等体通信并加入高可用性组。系统随即导入主用对等体的配置，且根据您的选择替换设备可以在组中充当主要或辅助设备。您现在可以验证高可用性运行是否正常，而且如果需要，可切换模式使新设备变成主用设备。

监控高可用性

以下主题介绍如何监控高可用性。

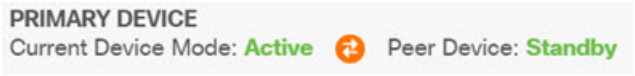
请注意，事件查看器和控制面板仅显示与您所登录设备相关的数据。它们不会显示两台设备的合并信息。

监控常规故障转移状态和历史记录

您可以使用以下方法监控常规高可用性状态和历史记录：

- 在“设备摘要”上（点击**设备**），高可用性组会显示设备状态。

- 在“高可用性”页面上（依次点击**设备** > **高可用性**），您可以看到两台设备的状态。如果发生任何故障，则会显示上次故障原因（来自故障转移历史记录）。点击两台设备之间的同步图标了解更多状态。



- 从“高可用性”(High Availability) 页面，点击状态旁边的**故障转移历史记录 (Failover History)** 链接。系统将打开 CLI 控制台并执行 **show failover history details** 命令。您还可以直接在 CLI 或 CLI 控制台中输入此命令。

CLI 命令

从 CLI 或 CLI 控制台中，您可以使用以下命令：

- **show failover**

  显示有关设备的故障转移状态的信息。

- **show failover history** ［**details**］

  显示过去的故障转移状态更改和状态变化的原因。添加 **details** 关键字可显示对等体的故障转移历史记录。此信息可帮助进行故障排除。

- **show failover state**

  显示两个设备的故障转移状态。信息包括设备的主要或辅助状态、设备的主用/备用状态以及最新报告的故障转移原因。

- **show failover statistics**

  显示故障转移接口传输和接收的数据包计数。例如，如果输出接口显示设备发送数据包，但未收到任何数据包，那么链路可能出现问题。这可能是电缆问题、对等体上配置的IP地址，或可能是设备将故障转移接口连接到不同的子网。

```
> show failover statistics
        tx:320875
        rx:0
```

- **show failover interface**

  显示故障转移和状态故障转移链路的配置。例如：

```
> show failover interface
        interface failover-link GigabitEthernet1/3
                System IP Address: 192.168.10.1 255.255.255.0
                My IP Address    : 192.168.10.1
                Other IP Address : 192.168.10.2
        interface stateful-failover-link GigabitEthernet1/4
                System IP Address: 192.168.11.1 255.255.255.0
                My IP Address    : 192.168.11.1
                Other IP Address : 192.168.11.2
```

- **show monitor-interface**

  显示为高可用性监控的接口的相关信息。有关详细信息，请参阅监控高可用性监控接口的状态，第 35 页。

- **show running-config failover**

  显示运行配置中的故障转移命令。这些是配置高可用性的命令。

监控高可用性监控接口的状态

如果对任何接口启用了高可用性监控，您可以使用 **show monitor-interface** 命令在 CLI 或 CLI 控制台中查看受监控接口的状态。

```
> show monitor-interface
 This host: Primary - Active
  Interface inside (192.168.1.13): Normal (Monitored)
  Interface outside (192.168.2.13): Normal (Monitored)
 Other host: Secondary - Standby Ready
  Interface inside (192.168.1.14): Normal (Monitored)
  Interface outside (192.168.2.14): Normal (Monitored)
```

受监控接口可以具有以下状态：

- (Waiting) 加上任何其他状态，例如 Unknown (Waiting) - 接口尚未从对等体设备上的相应接口收到 hello 数据包。
- Unknown - 初始状态。此状态也可能意味着状态无法确定。
- Normal - 接口正在接收流量。
- Testing - 接口上有 5 个轮询时间未收听到 Hello 消息。
- Link Down - 接口或 VLAN 通过管理方式关闭。
- No Link - 接口的物理链路关闭。
- Failed - 在接口上没有收到流量，但在对等体接口上收听到流量。

监控与高可用性相关的系统日志消息

系统在优先级别 2 发出大量与故障转移有关的系统日志消息，级别 2 表示一种关键情况。与故障转移关联的消息 ID 的范围是：101xxx、102xxx、103xxx、104xxx、105xxx、210xxx、311xxx、709xxx 和 727xxx。例如，105032 和 105043 表示故障转移链路存在问题。有关系统日志消息的说明，请参阅 https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html中的 *Cisco Threat Defense* 系统日志消息 指南。

注释 故障转移期间，系统按照逻辑先关闭接口，再启动接口，从而生成日志消息 411001 和 411002。这是正常活动。

必须先在**设备** > **日志记录设置**上配置诊断日志记录，才能查看系统日志消息。设置外部系统日志服务器，以便您可以稳定持续地监控消息。

在对等体设备上远程执行 CLI 命令

在 CLI 中，您可以使用 failover exec 命令在对等体上输入 show 命令，无需登录到对等体。

failover exec {**active** | **standby** | **mate**} 命令

必须指明哪一台设备应执行命令，主用设备还是备用设备，或输入**mate**，如果您想要另一台设备而非您登录的设备响应。

例如，如果您想要查看对等体的接口配置和统计信息，可以输入：

```
> failover exec mate show interface
```

您不能输入 **configure** 命令。此功能与 **show** 命令搭配使用。

注释 如果您登录到主用设备，可以使用 **failover reload-standby** 命令重新加载备用设备。

不能通过 防火墙设备管理器 CLI 控制台输入这些命令。

高可用性故障排除（故障转移）

如果高可用性组中设备的表现未能达到预期，请考虑以下步骤排除配置故障。

如果主用设备显示对等体设备出现故障，请参阅设备故障状态故障排除，第 39 页。

过程

步骤 1 从每个设备（主要和辅助设备）：

- 对故障转移链路的另一设备的 IP 地址执行 ping 操作。
- 如果您使用单独的链接，对状态故障转移链路的另一设备的 IP 地址执行 ping 操作。

如果 ping 操作失败，请确保每个设备上的接口都连接到同一网段。如果您使用直连电缆连接，请检查电缆。

步骤 2 进行以下一般检查：

- 检查主要和辅助设备上是否存在重复的管理 IP 地址。
- 检查两台设备上是否存在重复的故障转移和状态故障切 IP 地址。
- 检查每台设备上的等效接口端口是否连接到同一网段。

步骤 3 检查备用设备上的任务列表或审核日志。主用设备上每次部署成功后，您都应该看到“从活动节点导入配置”任务。如果任务失败，请检查故障转移链路，并再次尝试部署。

注释
如果任务列表指示存在失败的部署任务，则可能是在部署作业期间发生了故障转移。如果启动部署任务时备用设备是主用设备，但在任务期间发生了故障转移，则部署将失效。要解决此问题，请切换模式，使备用设备再次成为主用设备，然后重新部署配置更改。

步骤 4 使用 **show failover history** 命令获取有关设备上状态更改的详细信息。

查找以下情况：

- 应用同步失败：

```
12:41:24 UTC Dec 6 2017

App Sync     Disabled     HA state progression failed due to APP SYNC timeout
```

在应用同步阶段，将配置从主用设备传输到备用设备。应用同步失败会导致设备被禁用，使设备无法再被设置为主用设备。

如果设备因应用同步问题被禁用，您可能需要对故障转移和状态故障转移链路的端点使用设备上的其他接口。必须对链路的两端使用相同的端口号。

如果 show failover 命令显示辅助设备处于伪备用状态，这可能意味着您在辅助设备上为故障转移链路配置的 IP 地址与您在主设备上配置的地址不同。确保在两台设备为故障转移链路使用相同的主要/辅助 IP 地址。

伪备用状态也可能表示您在主设备和辅助设备上配置的 IPsec 密钥不同。

有关其他应用同步问题，请参阅高可用性应用同步失败故障排除，第 39 页。

- 异常频繁的故障转移（从主用转到备用，然后再切换）可能意味着故障转移链路出现问题。最坏的情况是，两台设备可能都变为主用状态，导致流经的流量中断。对链路的两端执行 ping 操作以验证连接性。您还可以使用 **show arp** 检查故障转移 IP 地址和 ARP 映射是否正确。

  如果故障转移链路正常，并配置正确，请考虑增加对等体轮询和保持时间、接口轮询和保持时间，减少高可用性监控的接口数量，或增加接口阈值。

- 接口检查导致的故障。接口检查原因包括被视为故障的接口列表。检查这些接口，以确保它们配置正确，并且不存在硬件问题。验证链路另一端的交换机配置没有问题。如果没有任何问题，请考虑在这些接口上禁用高可用性监控，或者增加接口故障阈值或时间。

```
06:17:51 UTC Jan 15 2017

Active     Failed     Interface check

                         This Host:3

                            admin: inside

                            ctx-1: ctx1-1

                            ctx-2: ctx2-1

                         Other Host:0
```

步骤 5 如果无法检测到备用设备，而且您找不到具体原因（例如，故障转移链路上的LAN错误或电缆连接出错等），请尝试以下步骤。

a) 在备用设备上登录 CLI 并输入 **failover reset** 命令。此命令应将设备从故障状态更改为无故障状态。现在，检查主用设备上的高可用性状态。如果现在可检测到备用对等体，则问题解决。

b) 在主用设备上登录CLI并输入**failover reset**命令。这会重置主用和备用设备上的高可用性状态。理想情况下，它将重新建立设备之间的链路。检查高可用性状态。如果状态仍然不正确，请继续。

c) 在主用设备的 CLI 或从 防火墙设备管理器首先暂停高可用性，然后恢复高可用性。CLI 命令是 **configure high-availability suspend** 和 **configure high-availability resume**。

d) 如果这些操作失败，请对备用设备执行 **reboot** 命令。

设备故障状态故障排除

如果一台设备在对等体设备的高可用性状态中被标记为故障设备（在**设备**或**设备** > **高可用性**页），可能有如下原因，假设设备 A 是主用设备，设备 B 是出现故障的对等体。

- 如果设备 B 尚未配置高可用性（仍然是单机模式），设备 A 显示设备 B 为故障设备。
- 如果在设备 B 上暂停高可用性，设备 A 将显示设备 B 为故障设备。
- 如果重新启动设备 B，设备 A 将显示设备 B 为故障设备，直至 B 完成重新启动并通过故障转移链路恢复通信。
- 如果应用同步 (App Sync) 在设备 B 上失败，设备 A 将显示设备 B 为故障设备。请参阅高可用性应用同步失败故障排除，第 39 页。
- 如果设备 B 在设备或接口运行状况监控中表现不合格，设备 A 将其标记为故障设备。检查设备 B 是否出现系统性问题。请尝试重启设备。如果设备大体运行状况正常，请考虑放宽设备或接口运行状况监控设置。**show failover history** 输出应提供有关接口运行状况检查失败的信息，
- 如果两台设备都变为主用状态，那么每台设备都会将对等体显示为故障设备。这通常表示故障转移链路出现问题。

  还可以指出与许可相关的问题。设备必须有一致的许可，要么均处于评估模式，要么都已注册。如果已注册，使用的智能许可证账户可以不同，但两个账户的出口控制功能设置必须相同，均为启用或禁用。对于出口控制功能，如果您使用不一致的设置配置 IPSec 加密密钥，当您激活 HA 后，两个设备都将变为主用状态。这会影响受支持网段上的路由，且您必须手动断开辅助设备上的 HA 才能消除影响。

高可用性应用同步失败故障排除

如果对等体无法加入高可用性组，或在您从主用设备部署更改时发生故障，请登录发生故障的设备，转至**高可用性 (High Availability)** 页面，然后点击**故障转移历史记录 (Failover History)** 链接。如果 **show failover history** 输出指出应用同步失败，即表示在 HA 验证阶段（在此过程中，系统检查设备是否可以作为高可用性组正常运行）出现问题。

这种故障可能会如下所示：

```
==========================================================================
From State                To State                  Reason
==========================================================================
16:19:34 UTC May 9 2018
Not Detected              Disabled                  No Error

17:08:25 UTC May 9 2018
Disabled                  Negotiation               Set by the config command

17:09:10 UTC May 9 2018
Negotiation               Cold Standby              Detected an Active mate

17:09:11 UTC May 9 2018
Cold Standby              App Sync                  Detected an Active mate

17:13:07 UTC May 9 2018
```

```
App Sync                    Disabled                    CD App Sync error is
High Availability State Link Interface Mismatch between Primary and Secondary Node
```

理想情况下，当 From State 为 App Sync 时，您希望收到的消息是“All validation passed”，并且节点的状态变为 Standby Ready。任何验证失败都会将对等体的状态转换成 Disabled (Failed)。您必须解决这些问题，使对等体能够再次用作高可用性组。请注意，如果通过对主用设备进行更改来修复应用同步错误，则必须先对其进行部署，然后再恢复高可用性以使对等节点加入。

以下消息表示发生了故障，并介绍如何解决问题。这些错误可能发生在节点加入和每次后续部署时。节点加入期间，系统会对主用设备上的最新部署配置执行检查。

- 主要和辅助节点之间的许可证注册模式不匹配。

  许可证错误指出，一个对等体已注册，而另一个对等体处于评估模式。对等体必须同时为注册状态或同处于评估模式，才能加入高可用性组。由于无法将注册设备恢复为评估模式，必须从**设备** > **智能许可证**页面注册另一台对等体。

  如果您注册的设备为主用设备，请在注册设备后执行部署。部署将强制设备刷新并同步配置，从而允许辅助设备正确加入高可用性组。

- 主要和辅助节点之间的许可证导出合规性不匹配。

  许可证合规性错误表示，设备注册到不同的思科智能软件管理器账户，并且其中一个账户启用了出口控制功能，而另一个账户没有启用。必须使用具有相同出口控制功能设置（启用或禁用）的账户注册设备。在**设备** > **智能许可证**页面上更改设备注册。

- 主要和辅助节点之间的软件版本不匹配。

  软件不匹配错误表示，对等体运行不同版本的 Firewall Threat Defense 软件。一次在一台设备上安装软件升级时，系统仅临时允许不匹配。但是，您无法在升级对等体的过程中部署配置更改。要解决此问题，请升级对等体，然后重新部署。

- 主要和辅助节点之间的物理接口不匹配。

  HA 组中的备用设备必须具有主用设备上存在的所有物理接口，且这些接口必须具有相同的硬件名称和类型（例如 GigabitEthernet1/1）。此错误表示备用设备缺少主用设备上存在的某些接口。允许在备用设备上拥有比主用设备更多的接口，因此请切换哪台设备为主用设备或选择另一个对等体设备。但是，不匹配的接口应该是临时状态，例如，如果正在替换一台设备上的接口模块，且需要在短时间内不使用该模块进行运行。对于正常操作，两台设备应具有相同数量和类型的接口。

- 主要和辅助节点之间的故障转移链路接口不匹配。

  将每台设备的故障转移物理接口连接到网络时，必须选择相同的物理接口。例如，每台设备上的 GigabitEthernet1/8 接口。此错误表示您使用不同的接口。要解决错误，请更正对等体设备上的电缆。

- 主要和辅助节点之间的状态故障转移链路接口不匹配。

  如果您使用单独的状态故障转移链路，将每台设备的状态故障转移物理接口连接到网络时，必须选择相同的物理接口。例如，每台设备上的 GigabitEthernet1/7 接口。此错误表示您使用不同的接口。要解决错误，请更正对等体设备上的电缆。

- 主要和辅助节点之间的故障转移/状态故障转移链路 EtherChannel 成员接口不匹配。

  如果选择故障转移或状态故障转移接口的 EtherChannel 接口，则 Etherchannel 必须在每台设备上具有相同的 ID 和成员接口。此错误消息指示是故障转移还是具有不匹配的状态故障转移链路。要解决此错误，请更正 EtherChannel 接口的配置，使其使用相同的 ID，并在每台设备上包含相同的接口。

- 主要和辅助节点之间的设备型号不匹配。

  加入高可用性组的对等体必须是型号完全相同的设备。此错误消息表示，对等体的设备型号不相同。必须选择不同的对等体来配置高可用性。

- 主用和备用节点不能位于同一机箱上。

  无法使用在同一硬件机箱上托管的设备配置高可用性。在同一机箱上支持多个设备的型号上配置高可用性时，必须选择驻留在单独硬件上的设备。

- 发生未知错误，请重试。

  应用同步期间出现问题，但系统无法识别该问题。再次尝试部署配置。

- 规则数据包损坏。请更新规则数据包，并重试。

  入侵规则数据库出现问题。在发生故障的对等体上，请转至**设备** > **更新**，然后点击**规则**组中的**立即更新**。等待更新完成，然后部署更改。然后，您可以从主用设备重试部署。

- 主节点和辅助节点之间的云服务注册状态不匹配。

  其中一个节点注册到了思科云，但另一个节点未注册。两个节点必须都注册，或者两个节点都没有注册，才能形成高可用性组。转到每台设备上的**设备** > **系统设置** > **服务**，并确保两台设备注册在同一云服务区域中。

- 主用和备用节点无法具有不同的云区域。

  设备在不同的思科云服务区域中注册。确定正确的区域，从智能许可取消注册另一台设备，并在重新注册期间选择正确的区域。如果两台设备均有错误的区域，请取消注册这两台设备，然后在正确的区域重新注册。

- 部署数据包损坏。请重试。

  这是一个系统错误。再次尝试部署，应该能解决此问题。

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。

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。