ASA/PIX：在透明模式配置主/备故障切换

目录

简介

故障切换配置要求两个相同的安全设备通过专用的故障切换链路（还可选择通过有状态故障切换链路）相互连接。系统会监视活动接口和单元的运行状况，以确定是否符合特定故障切换条件。如果符合这些条件，则发生故障切换。

安全设备支持两种故障切换配置：

- 活动/活动故障切换
- 活动/备用故障切换

每种故障切换配置都有自身的确定和执行故障切换的方法。使用活动/活动故障切换时，两个单元都能传递网络流量。因而您能够在网络上配置负载均衡。活动/活动故障切换仅适用于在多上下文模式下运行的单元。使用活动/备用故障切换时，只有一个单元传递流量，而另一个单元处于备用等待状态。活动/备用故障切换适用于在单上下文模式或多上下文模式下运行的单元。这两种故障切换配置都支持有状态或无状态（常规）的故障切换。

透明防火墙是第2层防火墙，其作用*类似于电*线中的*突起*，或者是隐*形防火墙*，不被视为连接设备的路由器跳。安全设备的内部端口和外部端口连接相同的网络。由于防火墙不是路由跃点，因此，可以很容易地将透明防火墙引入到现有网络，而无需重新分配 IP 地址。您可以设置自适应安全设备，使其在默认的路由防火墙模式或透明防火墙模式下运行。更改模式时，自适应安全设备会清除配置，因为许多命令在这两种模式中不受支持。如果您已拥有填充配置，则在更改模式之前务必备份此配置；创建新配置时，可以使用此备份配置作为参考。有关在透明模式下配置防火墙设备的详细信息，请参阅透明防火墙配置示例。

本文档重点介绍如何在ASA安全设备的透明模式下配置主用/备用故障切换。

注意：在多情景模式下运行的设备不支持VPN故障切换。VPN故障切换仅适用于主**用/备用故障切**换配置。

Cisco 建议您不要使用管理接口来进行故障切换，对于不断从一个安全设备向另一个安全设备发送连接信息的有状态故障切换，尤其如此。用于执行故障切换的接口至少必须与传递常规流量的接口具有相同的容量，当 ASA 5540 上的接口是千兆位时，管理接口只能使用 FastEthernet。管理接口仅用于管理流量，并指定为management0/0。但是，您可以使用**management-only**命令将任何接口配置为仅管理接口。对于 Management0/0，您也可以禁用“仅管理”模式，这样，管理接口就可以和其他任何接口一样传递流量。有关management-only命令的详细信息，请参阅思科安**全设备命**令参考。

此配置指南提供了一个示例配置，简要介绍 PIX/ASA 7.x 活动/备用技术。有关此项技术的理论基础的更多详细信息，请参阅 ASA/PIX 命令参考指南。

先决条件

要求

硬件要求

故障切换配置中的两个单元必须具有相同的硬件配置。它们的型号、接口的数量和类型，以及 RAM 量都必须相同。

注意：这两个单元不需要具有相同大小的闪存。如果故障切换配置使用闪存大小不同的单元，请确保闪存较小的单元有足够空间容纳软件映像文件和配置文件。否则，从闪存较大的单元向闪存较小的单元进行配置同步就会失败。

软件要求

故障切换配置中的两个单元必须处于操作模式（路由或透明，单上下文或多上下文）。 它们必须具有相同的主软件版本（第一个数字）和次软件版本（第二个数字），不过，在升级过程中，可以使用不同的软件版本；例如，可以将一个单元从版本 7.0(1) 升级为版本 7.0(2) 并使故障切换保持为活动状态。Cisco 建议您将两个单元都升级为同一版本以确保长期兼容。

有关如何在故障切换对上升级软件的详细信息，*请参阅Cisco安全设备命令行配置指南8.0版*的“为故障切换对执行零停机时间升级”部分。

许可证要求

在ASA安全设备平台上，至少一个设备必须具有不受限**制(UR)许可证**。

注意：可能需要升级故障切换对上的许可证，以获得其他功能和优势。有关详细信息，请参阅故障切换对上的许可证密钥升级。

注意：参与故障切换的两个安全设备上的许可功能（如SSL VPN对等体或安全情景）必须相同。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 7.x及更高版本的ASA安全设备

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

相关产品

此配置也可用于以下硬件和软件版本：

- 7.x 版及更高版本的 PIX 安全设备

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

活动/备用故障切换

本部分介绍活动/备用故障切换，其中包括以下主题：

活动/备用故障切换概述

通过活动/备用故障切换，可以使用备用安全设备代为提供故障单元的功能。活动单元发生故障时，将变为备用状态，同时备用单元变为活动状态。变为活动状态的设备将采用IP地址，或者，对于透明防火墙，采用故障设备的管理IP地址和MAC地址，并开始传输流量。现在处于备用状态的单元采用备用 IP 地址和 MAC 地址。因为网络设备检测不到 MAC 和 IP 地址配对的变化，所以网络上的任何位置都不会出现 ARP 条目变化或超时。

注意：对于多情景模式，安全设备可以故障转移整个设备（包括所有情景），但不能单独故障转移单个情景。

主要/辅助状态和活动/备用状态

故障切换对中两个单元之间的主要区别在于：哪个单元处于活动状态，哪个单元处于备用状态，也就是说，要使用哪些 IP 地址以及哪个单元是主要单元并有效传递流量。

根据配置中指定的主设备和辅助设备，设备之间存在一些差异：

- 如果两个单元同时启动（并且运行状况相同），则主要单元始终会成为活动单元。
- 主要单元的 MAC 地址始终会与活动 IP 地址配对。如果辅助单元处于活动状态，但无法通过故障切换链路获得主要 MAC 地址，则不适用此规则。在这种情况下，将使用辅助 MAC 地址。

设备初始化和配置同步

引导故障切换对中的一个或两个设备时，将进行配置同步。配置始终是从活动单元到备用单元进行同步的。当备用设备完成其初始启动时，它会清除其运行配置，但与主用设备通信所需的failover命令除外，并且主用设备会将其整个配置发送到备用设备。

活动单元的确定依据如下：

- 如果某个单元引导并检测到以活动状态运行的对等体，则会成为备用单元。
- 如果某个单元引导并且未检测到对等体，则会成为活动单元。
- 如果两个单元同时引导，则主要单元成为活动单元，辅助单元成为备用单元。

注：如果辅助设备启动且未检测到主设备，则它会成为主用设备。它使用自身的 MAC 地址作为活动 IP 地址。主要单元变为可用时，辅助单元会将 MAC 地址更改为主要单元的 MAC 地址，这会导致网络流量中断。若要避免这种情况，请用虚拟 MAC 地址配置故障切换对。有关详细信息，请参阅本文档的配置活动/备用故障切换部分。

当复制启动时，主用设备上的安全设备控制台将显示消息“Beginning configuration replication:(开始配)”，当完成时，安全设备显示消息“要匹配的”在复制期间，在活动单元上输入的命令无法正确复制到备用单元，在备用单元上输入的命令可由从活动单元复制而来的配置覆盖。在复制配置的过程

中，请勿在故障切换对中的任何单元上输入命令。根据配置的大小，复制过程所需时间从几秒到几分钟不等。

在辅助设备上，当复制消息与主设备同步时，您可以观察该复制消息：

```
ASA> .

        Detected an Active mate
Beginning configuration replication from mate.
End configuration replication from mate.

ASA>
```

在备用单元上，配置仅存在于运行内存中。若要在同步后将配置保存到闪存，请输入以下命令：

- 对于单上下文模式，在活动单元上输入 **copy running-config startup-config 命令。**该命令将被复制到备用单元，该单元继而将其配置写入闪存。
- 对于多上下文模式，从系统执行空间和磁盘上的每个上下文，对活动单元输入 **copy running-config startup-config 命令。**该命令将被复制到备用单元，该单元继而将其配置写入闪存。从任一单元都可通过网络访问外部服务器上的启动配置上下文，不需要针对每个单元单独保存。或者，也可将上下文从活动单元磁盘复制到外部服务器，然后复制到备用单元磁盘，在重新加载备用单元时，即可使用这些上下文。

命令复制

命令复制的方向始终是从活动单元到备用单元。在活动单元上输入命令时，这些命令通过故障切换链路发送到备用单元。不必为复制这些命令而将活动配置保存到闪存。

注意：在备用设备上所做的更改不会复制到主用设备。如果在备用单元上输入命令，安全设备将显示以下消息：`**** WARNING **** Configuration Replication is NOT performed from Standby unit to Active unit.`配置不会再同步。即使输入不影响配置的命令，也会显示此消息。

如果在主用设备上输入**write standby**命令，则备用设备会清除其运行配置，但用于与主用设备通信的failover命令除外，主用设备会将其整个配置发送到备用设备。

对于多上下文模式，在系统执行空间中输入 **write standby 命令时，将复制所有上下文。**如果在某个上下文中输入 write standby 命令，该命令只会复制该上下文的配置。

复制的命令存储在运行配置中。若要将复制的命令保存到备用单元上的闪存，请输入以下命令：

- 对于单上下文模式，在活动单元上输入 **copy running-config startup-config 命令。**该命令将被复制到备用单元，该单元继而将其配置写入闪存。
- 对于多上下文模式，从系统执行空间和磁盘上的每个上下文内，对活动单元输入 **copy running-config startup-config 命令。**该命令将被复制到备用单元，该单元继而将其配置写入闪存。从任一单元都可通过网络访问外部服务器上的启动配置上下文，不需要针对每个单元单独保存。或者，您也可从活动单元上的磁盘将上下文复制到外部服务器，然后复制到备用单元上的磁盘。

故障切换触发器

如果发生以下事件之一，则单元可能发生故障：

- 单元存在硬件故障或电源故障。
- 单元存在软件故障。
- 太多受监视的接口发生故障。
- 在活动单元上输入了 **no failover active 命令，或在备用单元上输入了 failover active 命令。**

故障切换操作

在活动/备用故障切换中，故障切换是对一个单元进行的。即使是在多上下文模式下运行的系统上，也不能对各上下文或一组上下文进行故障切换。

下表列出了每个故障事件所对应的故障切换操作。对于每个故障事件，下表都列出了相应的故障切换策略（执行故障切换或不执行故障切换）、活动单元执行的操作、备用单元执行的操作以及关于故障切换条件和操作的所有特殊说明。下表列出了故障切换行为。

故障事件	策略	活动单元操作	备用单元操作	备注
活动单元发生故障（电源或硬件）	故障转移	不适用	变为活动状态；将活动单元标记为发生故障	在任何受监视接口或故障切换链路上都未接收到 hello 消息。
以前的活动单元恢复	不执行故障切换	变为备用单元	无操作	无
备用单元发生故障（电源或硬件）	不执行故障切换	将备用单元标记为发生故障	不适用	当备用单元标记为发生故障时，活动单元不会尝试执行故障切换，即使超过接口故障阈值也是如此。
在执行操作期间故障切换链路发生故障	不执行故障切换	将故障切换接口标记为发生故障	将故障切换接口标记为发生故障	必须尽快恢复故障切换链路，因为故障切换链路发生故障时，活动单元无法故障切换到备用单元。
故障切换链路在启动时发生故障	不执行故障切换	将故障切换接口标记为发生故障	变为活动单元	如果故障切换链路在启动时发生故障，则两个单元都变为活动单元。

有状态故障切换链路发生故障	不执行故障切换	无操作	无操作	如果发生故障切换，则状态信息将过时且会话将终止。
活动单元上的接口故障超出阈值	故障转移	将活动单元标记为发生故障	变为活动单元	无
备用单元上的接口故障超出阈值	不执行故障切换	无操作	将备用单元标记为发生故障	当备用单元标记为发生故障时，活动单元不会尝试执行故障切换，即使超过接口故障阈值也是如此。

常规和有状态故障切换

安全设备支持两种类型的故障切换：常规和有状态。本部分包括以下主题：

- 常规故障切换
- 有状态故障切换

常规故障切换

发生故障切换时，所有活动的连接都将中断。客户端需要在新的活动单元接管时重建连接。

有状态故障切换

启用有状态故障切换时，活动单元会向备用单元持续传递每个连接的状态信息。在发生故障切换之后，新的活动单元具有相同的连接信息。受支持的最终用户应用程序可继续进行原来的通信会话，而无需重新连接。

向备用单元传递的状态信息包括：

- NAT 转换表
- TCP 连接状态
- UDP 连接状态
- ARP 表
- 第2层网桥表(仅当防火墙在透明防火墙模式**下运行**时)
- HTTP 连接状态（如果启用了 HTTP 复制）
- ISAKMP 和 IPSec SA 表
- GTP PDP 连接数据库

启用有状态故障切换时不会传递给备用单元的信息包括：

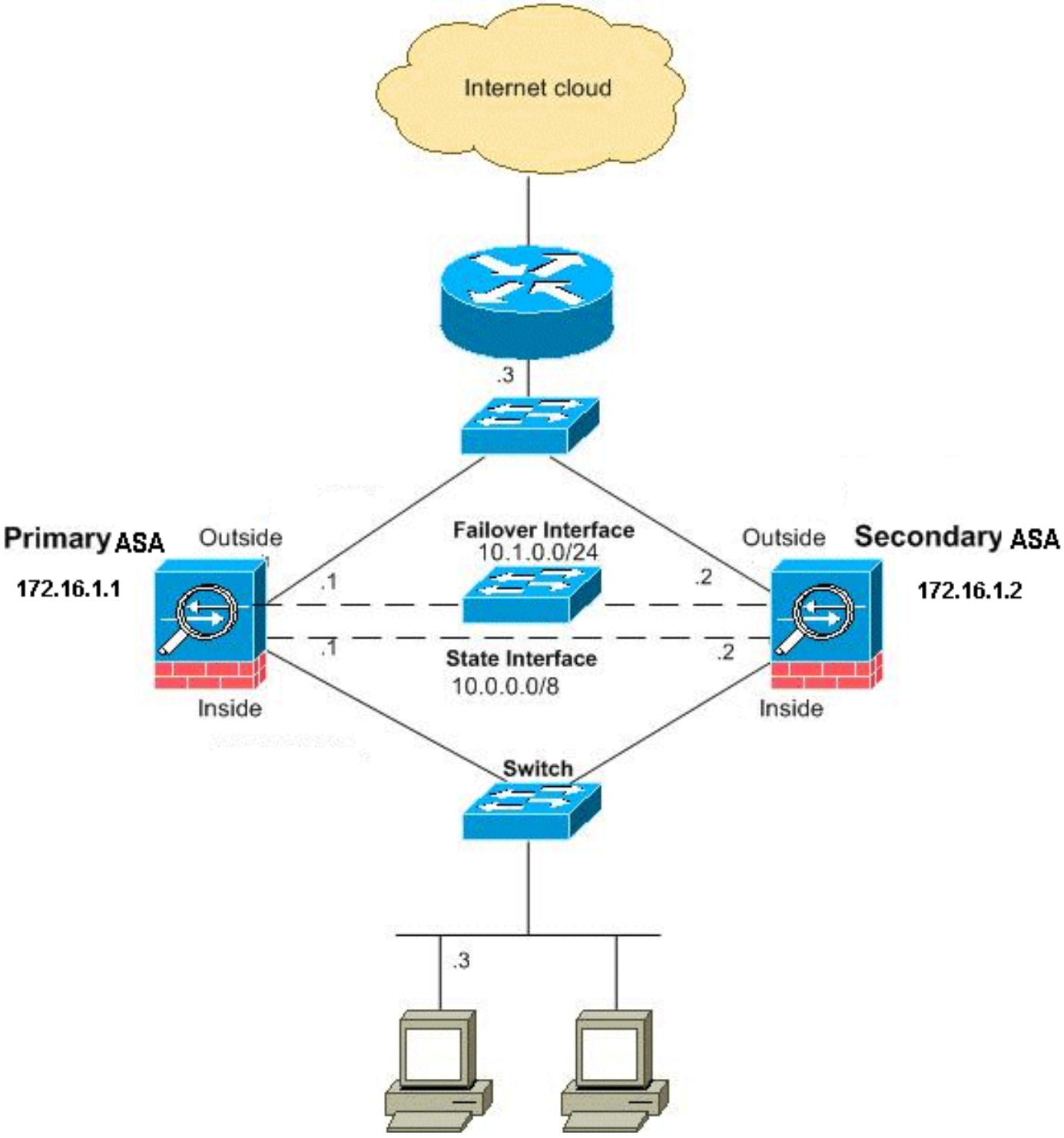
- HTTP 连接表（除非启用了 HTTP 复制）
- 用户身份验证 (uauth) 表
- 路由表
- 安全服务模块的状态信息

注意： 如果在活动 Cisco IP SoftPhone 会话中发生故障切换，则呼叫保持为活动状态，因为呼叫会话状态信息会复制到备用单元。当呼叫终止时，IP SoftPhone客户端将失去与Cisco CallManager的连接。发生这种情况的原因是备用单元上没有 CTIQBE 挂起消息的会话信息。当IP SoftPhone客户端在某段时间内未收到Cisco CallManager的回复时，它会认为Cisco CallManager不可达并注销自己。

基于 LAN 的活动/备用故障切换配置

网络图

本文档使用以下网络设置：



本节介绍如何使用以太网故障切换链路在透明模式下配置主用/备用故障切换。配置基于 LAN 的故障切换时，必须引导辅助设备以识别故障切换链路，然后辅助设备才能从主要设备获得运行配置。

注意：如果从基于电缆的故障切换更改为基于LAN的故障切换，则可以跳过为基于电缆的故障切换配置完成的许多步骤，例如为每个接口分配活动和备用IP地址。

主要单元配置

要在基于LAN的主用/备用故障转移配置中配置主设备，请完成以下步骤。这些步骤提供在主要单元上启用故障切换所需要的最低配置。除非另有说明，否则，对于多上下文模式，所有步骤都在系统执行空间中执行。

要配置主用/备用故障转移对中的主设备，请完成以下步骤：

1. 如果尚未配置，请为管理接口（透明模式）配置主用和备用IP地址。 备用 IP 地址用在当前作为备用单元的安全设备上。它必须与活动 IP 地址处于同一子网中。**注意：**如果使用专用的有状态故障切换接口，请勿为有状态故障切换链路配置IP地址。在后面的步骤中，请使用 **failover interface ip 命令配置专用的有状态故障切换接口。**

   ```
   hostname(config-if)#ip address active_addr netmask
                           standby standby_addr
   ```

   路由模式的每个接口都需要一个 IP 地址，而与路由模式不同的是，透明防火墙为整个设备分配一个 IP 地址。安全设备将此 IP 地址用作安全设备上始发的数据包（例如系统消息或 AAA 通信）的源地址。在示例中，主ASA的IP地址配置如下所示：

   ```
   hostname(config)#ip address 172.16.1.1 255.255.0.0 standby 172.16.1.2
   ```

   此处，主设备使用172.16.1.1，而辅助（备用）设备使用172.16.1.2。**注意：在**多情景模式下，必须从每个情景中配置接口地址。使用**changeto context**命令可在情景之间切换。命令提示符将变为 `hostname/context(config-if)#`，其中 context 是当前上下文的名称。
2. （仅限 PIX 安全设备平台）启用基于 LAN 的故障切换。

   ```
   hostname(config)#failover lan enable
   ```

3. 将该单元指定为主要单元。

   ```
   hostname(config)#failover lan unit primary
   ```

4. 定义故障切换接口。指定要用作故障切换接口的接口。

   ```
   hostname(config)#failover lan interface if_name phy_if
   ```

   在本文档中，“failover”（以太网接口0的接口名称）用于故障切换接口。

   ```
   hostname(config)#failover lan interface failover Ethernet3
   ```

   *if_name 参数对 phy_if 参数指定的接口分配名称。phy_if 参数可以是物理端口名（如 Ethernet1），也可以是以前创建的子接口（如 Ethernet0/2.3）。*对故障切换链路分配活动和备用 IP 地址

   ```
   hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr
   ```

   在本文档中，要配置故障切换链路，10.1.0.1用于主用设备，10.1.0.2用于备用设备，而“failover”是以太网接口0的接口名称。

   ```
   hostname(config)#failover interface ip failover 10.1.0.1
                           255.255.255.0 standby 10.1.0.2
   ```

   备用 IP 地址必须与活动 IP 地址处于同一子网中。您不需要识别备用地址子网掩码。在发生故障切换时，故障切换链路 IP 地址和 MAC 地址不会更改。故障切换链路的活动 IP 地址始终用于主要单元，而备用 IP 地址始终用于辅助单元。启用接口

   ```
   hostname(config)#interface phy_if

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

   在本示例中，Ethernet3 用于故障切换：

   ```
   hostname(config)#interface ethernet3

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

5. （可选）若要启用有状态故障切换，请配置有状态故障切换链路。指定要用作有状态故障切换链路的接口。

   ```
   hostname(config)#failover link if_name phy_if
   ```

本示例使用“state”作为 Ethernet2 的接口名称，用于交换故障切换链路状态信息：

```
hostname(config)#failover link state Ethernet2
```

注：如果有状态故障切换链路使用故障切换链路或数据接口，则只需提供*if_name*参数。**if_name 参数对 phy_if 参数指定的接口分配逻辑名称。***phy_if参数*可以是物理端口名称（如 Ethernet1）或先前创建的子接口（如Ethernet0/2.3）。此接口不得用于任何其他用途，但作为故障切换链路除外。对有状态故障切换链路分配活动和备用 IP 地址。**注意：如**果有状态故障切换链路使用故障切换链路或数据接口，请跳过此步骤。您已经为接口定义了活动和备用 IP 地址。

```
hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr
```

在本示例中，10.0.0.1 用作有状态故障切换链路的活动 IP 地址，10.0.0.2 用作该链路的备用 IP 地址。

```
hostname(config)#failover interface ip state 10.0.0.1 255.0.0.0
                      standby 10.0.0.2
```

备用 IP 地址必须与活动 IP 地址处于同一子网中。您不需要识别备用地址子网掩码。除非有状态故障切换链路 IP 地址和 MAC 地址使用数据接口，否则它们在发生故障切换时不会更改。活动 IP 地址始终用于主要单元，而备用 IP 地址始终用于辅助单元。启用该接口。**注意：如**果有状态故障切换链路使用故障切换链路或数据接口，请跳过此步骤。您已经启用了该接口。

```
hostname(config)#interface phy_if

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

注意：例如，在此场景中，Ethernet2用于有状态故障切换链路：

```
hostname(config)#interface ethernet2

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

6. 启用故障切换。

```
hostname(config)#failover
```

注意：首先在主**设**备上发出failover命令，然后在辅助设备上发出该命令。在辅助设备上发出 **failover 命令之后，辅助设备将立即从主要设备获取配置，并将自己设置为***备用*。主要 ASA 会始终运行，正常传递流量，并将自己标记为*活动设备*。从这时起，只要活动设备发生故障，备用设备就会成为活动设备。

7. 将系统配置保存到闪存。

```
hostname(config)#copy running-config startup-config
```

辅助单元配置

在辅助单元上，只需要配置故障切换接口。辅助单元需要这些命令才能开始与主要单元进行通信。在主要单元将其配置发送到辅助单元之后，这两种配置之间的唯一永久性区别就是 **failover lan unit 命令，该命令用于识别每个单元是主要单元还是辅助单元。**

对于多情景模式，除非另有说明，否则所有步骤都在系统执行空间中执行。

要配置辅助设备，请完成以下步骤：

1. （仅限 PIX 安全设备平台）启用基于 LAN 的故障切换。
   ```
   hostname(config)#failover lan enable
   ```

2. 定义故障切换接口。请使用与主要单元相同的设置。指定要用作故障切换接口的接口。
   ```
   hostname(config)#failover lan interface if_name phy_if
   ```

   在本文档中，以太网接口0用于LAN故障切换接口。
   ```
   hostname(config)#failover lan interface failover Ethernet3
   ```

   *if_name 参数对 phy_if 参数指定的接口分配名称。*对故障切换链路分配活动和备用 IP 地址。
   ```
   hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr
   ```

   在本文档中，要配置故障切换链路，10.1.0.1用于主用设备，10.1.0.2用于备用设备，而“failover”是以太网接口0的接口名称。
   ```
   hostname(config)#failover interface ip failover 10.1.0.1
                        255.255.255.0 standby 10.1.0.2
   ```

   注意：在主设备上配置故障切换接口时，请完全按照在主设备上输入的命令输入此命令。启用该接口。
   ```
   hostname(config)#interface phy_if

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

   例如，在此场景中，以太网接口0用于故障切换。
   ```
   hostname(config)#interface ethernet3

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

3. （可选）将此单元指定为辅助单元。
   ```
   hostname(config)#failover lan unit secondary
   ```

   注：此步骤是可选的，因为默认情况下，除非先前配置，否则设备会指定为辅助设备。
4. 启用故障切换。
   ```
   hostname(config)#failover
   ```

   注意：启用故障切换后，主用设备将运行内存中的配置发送到备用设备。进行配置同步时，活动单元控制台将显示消息 *Beginning configuration replication:Sending to mate and End Configuration Replication to mate。*
5. 在完成运行配置的复制之后，将配置保存到闪存。
   ```
   hostname(config)#copy running-config startup-config
   ```

配置

本文档使用以下配置：

主ASA

```
ASA#show running-config
 ASA Version 7.2(3)
!
```

```
!--- To set the firewall mode to transparent mode, !---
use the firewall transparent command !--- in global
configuration mode.

firewall transparent
hostname ASA
domain-name default.domain.invalid
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0
 nameif failover

  description LAN Failover Interface
!
interface Ethernet1
 nameif inside
 security-level 100
!
interface Ethernet2
 nameif outside
 security-level 0

!--- Configure no shutdown in the stateful failover
interface !--- of both Primary and secondary ASA.

interface Ethernet3
 nameif state
 description STATE Failover Interface
!
interface Ethernet4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet5
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain.invalid
access-list 100 extended permit ip any any
pager lines 24
mtu outside 1500
mtu inside 1500

!--- Assign the IP address to the Primary and !---
Seconday ASA Security Appliance. ip address 172.16.1.1
255.255.255.0 standby 172.16.1.2

failover
failover lan unit primary
failover lan interface failover Ethernet0
failover lan enable
failover key ******
failover link state Ethernet3
failover interface ip failover 10.1.0.1 255.255.255.0
standby 10.1.0.2
failover interface ip state 10.0.0.1 255.0.0.0 standby
```

```
10.0.0.2

asdm image flash:/asdm-522.bin
no asdm history enable
arp timeout 14400
access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.3 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

辅助ASA

```
ASA#show running-config
ASA Version 7.2(3)
!
hostname ASA
domain-name default.domain.invalid
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
failover
```

```
failover lan unit secondary
failover lan interface failover Ethernet0
failover lan enable
failover key ******
failover interface ip failover 10.1.0.1 255.255.255.0
standby 10.1.0.2
```

验证

使用 show failover 命令

本部分介绍 **show failover 命令输出。**在每个单元上，都可使用 **show failover 命令验证故障切换状态。**

主ASA

```
ASA#show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: failover Ethernet0 (up)
Unit Poll frequency 200 milliseconds, holdtime 800 milliseconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 7.2(3), Mate 7.2(3)
Last Failover at: 00:08:03 UTC Jan 1 1993
        This host: Primary - Active
                Active time: 1820 (sec)
                  Interface inside (172.16.1.1): Normal
                  Interface outside (172.16.1.1): Normal
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                  Interface inside (172.16.1.2): Normal
                  Interface outside (172.16.1.2): Normal

Stateful Failover Logical Update Statistics
        Link : state Ethernet3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         185        0          183        0
        sys cmd         183        0          183        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        L2BRIDGE Tbl    2          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       7012
        Xmit Q:         0       1       185
```

辅助ASA

```
ASA(config)#show failover
Failover On
```

```
Cable status: N/A - LAN-based failover enabled
Failover unit Secondary
Failover LAN Interface: failover Ethernet0 (up)
Unit Poll frequency 200 milliseconds, holdtime 800 milliseconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 7.2(3), Mate 7.2(3)
Last Failover at: 16:39:12 UTC Aug 9 2009
        This host: Secondary - Standby Ready
                Active time: 0 (sec)
                  Interface inside (172.16.1.2): Normal
                  Interface outside (172.16.1.2): Normal
        Other host: Primary - Active
                Active time: 1871 (sec)
                  Interface inside (172.16.1.1): Normal
                  Interface outside (172.16.1.1): Normal

Stateful Failover Logical Update Statistics
        Link : state Ethernet3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         183        0          183        0
        sys cmd         183        0          183        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        L2BRIDGE Tbl    0          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       7043
        Xmit Q:         0       1       183
```

使用 **show failover state** 命令可验证状态。

主ASA

```
ASA#show failover state
               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  Comm Failure             00:02:36 UTC Jan 1 1993

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

辅助单元

```
ASA#show failover state
               State          Last Failure Reason      Date/Time
This host  -   Secondary
               Standby Ready  None
Other host -   Primary
               Active         None

====Configuration State===
```

```
        Sync Done - STANDBY
====Communication State===
        Mac set
```

要验证故障切换设备的IP地址，请使用**show failover interface**命令。

主要单元

```
ASA#show failover interface
        interface failover Ethernet0
                System IP Address: 10.1.0.1 255.255.255.0
                My IP Address    : 10.1.0.1
                Other IP Address : 10.1.0.2
        interface state Ethernet3
                System IP Address: 10.0.0.1 255.255.255.0
                My IP Address    : 10.0.0.1
                Other IP Address : 10.0.0.2
```

辅助单元

```
ASA#show failover interface
        interface failover Ethernet0
                System IP Address: 10.1.0.1 255.255.255.0
                My IP Address    : 10.1.0.2
                Other IP Address : 10.1.0.1
        interface state Ethernet3
                System IP Address: 10.0.0.1 255.255.255.0
                My IP Address    : 10.0.0.2
                Other IP Address : 10.0.0.1
```

查看受监视的接口

若要查看受监视的接口的状态：在单上下文模式下，请在全局配置模式下输入 **show monitor-interface 命令。**在多上下文模式下，请在上下文内输入 **show monitor-interface。**

主ASA

```
ASA(config)#show monitor-interface
        This host: Primary - Active
                Interface inside (172.16.1.1): Normal
                Interface outside (172.16.1.1): Normal
        Other host: Secondary - Standby Ready
                Interface inside (172.16.1.2): Normal
                Interface outside (172.16.1.2): Normal
```

辅助ASA

```
ASA(config)#show monitor-interface
        This host: Secondary - Standby Ready
                Interface inside (172.16.1.2): Normal
                Interface outside (172.16.1.2): Normal
        Other host: Primary - Active
                Interface inside (172.16.1.1): Normal
                Interface outside (172.16.1.1): Normal
```

注意：如果未输入故障切换IP地址，则**show failover** 命令会显示0.0.0.0，以便IP地址，并且接口监控仍处于等*待状*态。有关不同故障切换状态的详细信息，请参阅 *Cisco 安全设备命令参考 7.2 版 的* show failover 部分。

显示运行配置中的故障切换命令

若要查看运行配置中的故障切换命令，请输入以下命令：

```
hostname(config)#show running-config failover
```

将显示所有的故障切换命令。在多上下文模式下运行的单元上，请在系统执行空间中输入 **show running-config failover 命令。**输入**show running-config all failover**命令以显示运行配置中的failover命令，并包括您未更改其默认值的命令。

故障切换功能测试

要测试故障切换功能，请完成以下步骤：

1. 测试活动单元或故障切换组是否如预期那样，经由 FTP（举例来说）传递流量，从而基于不同接口在主机之间发送文件。
2. 使用以下命令强制向备用单元执行故障切换：对于活动/备用故障切换，请在活动单元上输入以下命令：
   ```
   hostname(config)#no failover active
   ```
3. 使用 FTP 在上述两台主机之间发送其他文件。
4. 如果测试未成功，请输入**show failover**命令以检查故障切换状态。
5. 完成后，可以使用以下命令将该单元或故障切换组恢复到活动状态：对于活动/备用故障切换，请在活动单元上输入以下命令：
   ```
   hostname(config)#failover active
   ```

强制故障切换

若要强制将备用单元变为活动单元，请输入以下命令之一：

在备用单元上输入以下命令：

```
hostname#failover active
```

在活动单元上输入以下命令：

```
hostname#no failover active
```

禁用故障切换

若要禁用故障切换，请输入以下命令：

```
hostname(config)#no failover
```

如果在活动/备用对上禁用故障切换，则每个单元的活动和备用状态将保持不变，直到重新启动为止

。例如，备用单元保持为备用模式，这样，两个单元都不会开始传递流量。若要使备用单元变为活动状态（甚至在禁用故障切换的情况下），请参阅强制故障切换部分。

如果在活动/活动对上禁用故障切换，则无论哪个单元配置为首选，故障切换组当前在哪个单元上为活动状态，它们就将一直处于活动状态。**no failover 命令可在系统执行空间中输入。**

恢复故障单元

若要将故障单元恢复为无故障状态，请输入以下命令：

```
hostname(config)#failover reset
```

如果将故障单元恢复为无故障状态，它并不会自动变为活动单元；恢复后的单元或组将保持为备用状态，直到故障切换将其变为活动状态（通过强制或自然方式）为止。 但使用 preempt 命令配置的故障切换组例外。如果使用 preempt 命令配置的故障切换组以前为活动状态，并且故障单元是其首选单元，则该故障切换组将变为活动状态。

故障排除

发生故障切换时，两个安全设备都将发出系统消息。本节包括以下主题

- 故障切换监视
- 单元故障
- %ASA-3-210005：LU 分配连接失败
- 故障切换系统消息
- 调试消息
- SNMP
- 已知问题

故障切换监视

本示例演示故障切换尚未开始监视网络接口时的情况。在从该接口上的另一台设备收到第二个hello数据包之前，故障切换不会开始监控网络接口。这需要大约 30 秒时间。如果设备连接到运行生成树协议(STP)的网络交换机，则这需要两倍于交换机中配置的转发延迟时间（通常配置为15秒），外加30秒的延迟。这是因为在ASA启动时和故障切换事件发生后，网络交换机会立即检测到临时网桥环路。检测到此环路后，它会停止在这些接口上转发数据包以延迟。然后，它进入侦听模，等待额外的时间，在此时间内，交换机会侦听网桥环路，但不转发流量或转发故障切换hello据包。在两倍转发延迟时间（30 秒）之后，继续传送数据。每个ASA都保持在模式，直到它从另一台设备听到30秒hello数据包。在ASA传递流量的时间内，它不会因未听到hello数据包而使另一设备败。所有其他故障切换监控仍然发生，即电源、链路接口丢失和故障切换电缆hello。

对于故障切换，思科强烈建议客户在连接到ASA接口的所有交换机端口上启用portfast。另外，必须在这些端口上禁止开辟信道和建立中继。如果ASA的接口在故障切换期间关闭，则交换机无需等待30秒，同时端口从侦听状态转换到学习状态转换到转发状态。

```
Failover On
Cable status: Normal
Reconnect timeout 0:00:00
```

```
This host: Primary - Active
Active time: 6930 (sec)
Interface inside (172.16.1.1): Normal (Waiting)
Interface outside (172.16.1.1): Normal (Waiting)
Other host: Secondary - Standby
Active time: 15 (sec)
Interface inside (172.16.1.2): Normal (Waiting)
Interface outside (172.16.1.2): Normal (Waiting)
```

总之，请检查以下步骤以缩小故障切换问题：

- 检查与处于等待/故障状态的接口相连的网络电缆，如有必要，更换这些电缆。
- 如果两个单元之间连接了交换机，请验证与处于等待/故障状态的接口相连的网络是否正常运行。
- 检查与处于等待/故障状态的接口相连的交换机端口，如有必要，使用交换机上的其他 FE 端口。
- 检查是否在接口所连接的交换机端口上启用了 Portfast 并禁止建立中继和开辟信道。

单元故障

在本示例中，故障切换检测到一个故障。请注意，主要单元上的 Interface 1 是故障的来源。由于故障，设备恢复等待模式。故障设备已从网络中自行删除（接口关闭），不再在网络上hello数据包。主用设备保持在等态，直到更换故障设备并重新启动故障切换通信。

```
Failover On
Cable status: Normal
Reconnect timeout 0:00:00
This host: Primary - Standby (Failed)
Active time: 7140 (sec)
Interface inside (172.16.1.2): Normal (Waiting)
Interface outside (172.16.1.2): Failed (Waiting)
Other host: Secondary - Active
Active time: 30 (sec)
Interface inside (172.16.1.1): Normal (Waiting)
Interface outside (172.16.1.1): Normal (Waiting)
```

LU 分配连接失败

如果收到以下错误消息，说明可能有内存问题：

```
LU
```

此问题记录在Cisco Bug ID CSCte80027(仅限注册客户)中(仅限注册客户)。 要解决此问题，请将防火墙升级到修复此漏洞的软件版本。修复此Bug的一些ASA软件版本是8.2(4)、8.3(2)、8.4(2)。

故障切换系统消息

安全设备发出优先级为 2 的与故障切换有关的大量系统消息，说明存在严重的问题。若要查看这些消息，请参阅 Cisco 安全设备日志记录配置和系统日志消息，以启用日志记录和查看有关系统消息的说明。

注意：在切换中，故障切换逻辑关闭，然后打开接口，生成系统日志**411001**和**411002**消息。这是正常的活动。

调试消息

若要查看调试消息，请输入 **debug fover 命令。**有关详细信息，请参阅 Cisco 安全设备命令参考。

注意：由于调试输出在CPU进程中被分配了高优先级，因此它会严重影响系统性能。因此，只有在针对特定问题排除故障或在与 Cisco 技术支持人员进行故障排除会话期间，才应使用 **debug fover 命令。**

SNMP

若要接收故障切换的 SNMP 系统日志陷阱，请配置 SNMP 代理以将 SNMP 陷阱发送到 SNMP 管理站，定义系统日志主机，并将 Cisco 系统日志 MIB 编译到 SNMP 管理站中。有关详细信息，请参阅 Cisco 安全设备命令参考中的 **snmp-server 和日志记录命令。**

故障切换轮询时间

若要指定故障切换单元轮询和保持时间，请在全局配置模式下使用 **failover polltime 命令。**

故[]轮询hello消息以表示时间间隔，以检查备用单元是否存在。

同样，`failover holdtime unit msec [time]  hello`

若要在活动/备用故障切换配置中指定数据接口轮询和保持时间，请在全局配置模式下使用 **failover polltime interface 命令。**若要恢复默认轮询和保持时间，请使用此命令的 **no 形式。**

failover polltime interface [msec] *time* **[holdtime** *time***]**

若要更改 hello 数据包在数据接口上的发送频率，请使用 **failover polltime interface 命令。**此命令只适用于活动/备用故障切换。对于活动/活动故障切换，请在故障切换组配置模式下使用 **polltime interface 命令，而不是 failover polltime interface 命令。**

对于 **holdtime value，输入的时间不能少于接口轮询时间的 5 倍。**轮询时间越快，安全设备检测故障和触发故障切换的速度就越快。但是，如果网络只是临时拥塞，更快地检测到故障可能导致不必要的切换。如果在接口上经过一半保持时间仍未听到 hello 数据包，则会开始接口测试。

在配置中可以同时包括 failover polltime unit 和 failover polltime interface 命令。

本示例将接口轮询时间频率设置为 500 毫秒，将保持时间设置为 5 秒：

```
hostname(config)#failover polltime interface msec 500 holdtime 5
```

有关详细信息，请参阅 *Cisco 安全设备命令参考 7.2 版 的* failover polltime 部分。

导出故障切换配置中的证书/专用密钥

主要设备自动将专用密钥/证书复制到辅助单元。在主用设备中发出**write memory**命令，以便将配置（包括证书/私钥）复制到备用设备。活动单元配置会清除并重新填充备用单元上的所有密钥/证书。

注意：您不能手动从活动设备导入证书、密钥和信任点，然后导出到备用设备。

警告：故障切换消息解密失败。

错误消息：

```
Failover message decryption failure. Please make sure both units have the
same failover shared key and crypto license or system is not out of memory
```

此问题是因故障切换密钥配置造成的。若要解决此问题，请移除故障切换密钥，并配置新的共享密钥。

问题：配置透明主用/备用多模式故障切换后，故障切换始终抖动

当两个ASA的内部接口直接连接，并且两个ASA的外部接口直接连接时，故障切换是稳定的。但是，当交换机在两者之间使用时，故障切换会抖动。

解决方案：在ASA接口上禁用BPDU以解决此问题。

ASA 模块故障切换

如果活动和备用单元中使用了高级检查和防御安全服务模块 (AIP-SSM) 或内容安全和控制安全服务模块 (CSC-SSM)，则这些模块在故障切换时将独立于 ASA 运行。**必须在主用和备用设备中手动配置模块，故障切换不会复制模块配置。**

对于故障切换，具有 AIP-SSM 或 CSC-SSM 模块的两个 ASA 单元必须属于同一硬件类型。例如，如果主要单元具有 ASA-SSM-10 模块，则辅助单元也必须具有 ASA-SSM-10 模块。

故障切换消息块分配失败

错误消息 `%PIX|ASA-3-105010:(Primary) Failover message block alloc failed`

说明：块内存已耗尽。这是一个暂时性的消息，安全设备应会恢复。*主要 单元也能列为辅助单元的备件。*

建议操作：若要监视当前块内存，请使用 **show blocks 命令。**

AIP 模块故障切换问题

如果在一个故障切换配置中有两个 ASA，且每个 ASA 都有一个 AIP-SSM，则必须手动复制 AIP-SSM 的配置。故障切换机制只复制 ASA 的配置。故障切换不包括 AIP-SSM。

首先，AIP-SSM 在故障切换时独立于 ASA 运行。进行故障切换时，ASA 只要求 AIP 模块为同一硬件类型。此外，与故障切换的其他所有部分一样，活动和备用单元之间的 ASA 配置必须同步。

至于 AIP 的设置，它们实际上是独立的传感器。如果两者之间没有故障切换，它们就不会相互感知。它们能运行不同版本的代码。也就是说，它们不必相互匹配，进行故障切换时，ASA 不关心 AIP 上的代码版本。

ASDM 通过在 AIP 上配置的管理接口 IP 发起与 AIP 的连接。换句话说，它通常通过HTTPS连接到传感器，这取决于您如何设置传感器。

可独立于 IPS (AIP) 模块对 ASA 执行故障切换。您仍然连接到同一个，因为您连接到其管理IP。若

要连接到其他 AIP，必须重新连接其管理 IP 才能对其进行配置和访问。

请参阅 ASA：将网络流量从ASA发送到AIP SSM配置示例，了解有关如何将通过Cisco ASA 5500系列自适应安全设备(ASA)的网络流量发送到高级检测和防御安全服务模块(AIP-SSM)(IPS)的详细信息和配置示例)

已知问题

当您尝试访问辅助ASA上的ASDM（使用8.x软件版本和ASDM 6.x版本进行故障切换配置）时，会收到以下错误：

```
Error:The name on the security certificate is invalid or does not match the name of the site
```

在证书中，颁发者和使用者名称是主用设备的IP地址，*而*不是备用设备的IP*地*址。

在 ASA 8.x 版中，内部 (ASDM) 证书从活动单元复制到备用单元，导致该错误消息出现。但是，如果同一防火墙在版本7.x代码上运行，并且您尝试访问ASDM，则会收到以下常规安全警告：

```
The security certificate has a valid name matching the name of the page you are trying to view
```

如果检查该证书，则会发现 Issuer 和 Subject Name 是备用单元的 IP 地址。

相关信息

- Cisco ASA 5500 系列自适应安全设备
- Cisco PIX 防火墙软件
- 防火墙服务模块 (FWSM) 故障切换配置
- FWSM 故障切换故障排除
- Cisco Secure PIX 防火墙故障切换的工作原理
- 技术支持和文档 - Cisco Systems