ASA/PIX：在透明模式的配置活动/活动故障切换

目录

[警告：故障切换消息解密失败。](#)
[相关信息](#)

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/主用故障切换。

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。

本配置指南提供了配置示例，以包括ASA/PIX 7.x主用/备用技术的简要介绍。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/活动故障切换

本部分介绍活动/备用故障切换，其中包括以下主题：

- 活动/活动故障切换概述
- 主要/辅助状态和活动/备用状态
- 设备初始化和配置同步

- 命令复制
- 故障切换触发器
- 故障切换操作

活动/活动故障切换概述

活动/活动故障切换仅适用于多上下文模式下的安全设备。在活动/活动故障切换配置中，两个安全设备都可以传递网络流量。

在活动/活动故障切换中，可将安全设备上的安全上下文划分为多个故障切换组。故障切换组只是一个或多个安全上下文的逻辑组。您可以在安全设备上最多创建两个故障切换组。管理情景始终是故障转移组1的成员。默认情况下，任何未分配的安全情景也是故障转移组1的成员。

故障切换组构成了活动/活动故障切换中故障切换的基本单元。接口故障监视、故障切换和活动/备用状态全部都是故障切换组（而不是单元）的属性。当活动故障切换组出现故障时，它会变为备用状态，而备用故障切换组会变为活动状态。变为活动状态的故障切换组中的接口会采用出现故障的故障切换组中接口的 MAC 和 IP 地址。当前处于备用状态的故障切换组中的接口将接管备用 MAC 和 IP 地址。

注：设备上的故障切换组发生故障并不意味着设备发生故障。设备仍然可以有另一个故障切换组来传递流量。

主要/辅助状态和活动/备用状态

与活动/备用故障切换相同的是，活动/活动故障切换对中的一个单元指定为主要单元，而另一个单元指定为辅助单元。与活动/备用故障切换不同的是，此指定并不表明在两个单元同时启动时哪个单元变为活动状态。相反，主要/辅助指定有两个作用：

- 确定在两个单元同时引导时哪个单元向故障切换对提供运行配置。
- 确定在两个单元同时引导时每个故障切换组在哪个单元上显示为活动状态。配置中的每个故障切换组都配置了主要单元或辅助单元首选。可以将两个故障切换组配置为在对中的单个设备上处于活动状态，而将包含故障切换组的另一设备配置为备用状态。但是，更典型的配置是为每个故障切换组分配不同的角色首选项，以使每个故障切换组在不同的设备上处于活动状态，并在设备间分配流量。**注意：**安全设备**不提**供负载平衡服务。负载均衡必须由将流量传递到安全设备的路由器来处理。

每个故障切换组在哪个单元上变为活动状态按如下所述确定

- 当一个单元引导而对等单元不可用时，该单元上的两个故障切换组都会变为活动状态。
- 当设备在对等设备处于活动状态时启动时（两个故障切换组均处于主用状态），故障切换组在主用设备上保持主用状态，而与故障切换组的主要或辅助首选项无关，直到出现以下情况之一：发生故障切换。您使用 **no failover active 命令手动强制将故障切换组切换到另一个单元**您使用 **preempt 命令配置了故障切换组，这导致首选的单元可用时该单元上的故障切换组自动变为活动状态。**
- 当两个单元同时引导时，在同步配置之后，每个故障切换组都在其首选单元上变为活动状态。

设备初始化和配置同步

当故障切换对中的一个或两个单元引导时，会发生配置同步。配置按如下所述同步：

- 当一个单元引导而对等单元处于活动状态（其上的两个故障切换组都处于活动状态）时，引导单元会与活动单元联系以获取运行配置，而不管引导单元的主要指定或辅助指定是什么。
- 当两个单元同时引导时，辅助单元从主要单元获取运行配置。

当复制启动时，发送配置的设备上的安全设备控制台显示消息“Beginning configuration replication:Sending to mate”“End Configuration Replication to mate” 在复制期间，在发送配置的设备上输入的命令无法正确复制到对等设备，在接收配置的设备上输入的命令可能被收到的配置覆盖。在配置复制过程中，请勿在故障切换对中的任一设备上执行命令。复制取决于配置的大小，可能需要几秒钟到几分钟。

在接收配置的单元上，配置仅存在于运行内存中。要在同步后将配置保存到闪存，请在故障切换组1处于活动状态的设备上的系统执行空间中输入**write memory all**命令。该命令将被复制到对等单元，该单元继而将其配置写入闪存。将all关键字与此命令一起使**用会**保存系统和所有情景配置。

注意：外部服务器上保存的启动配置可从任何一台设备通过网络进行访问，无需为每台设备单独保存。或者，您可以将上下文配置文件从主要单元上的磁盘复制到外部服务器，然后再将它们复制到辅助单元上的磁盘，当重新加载辅助单元时，这些配置文件即会变为可用。

命令复制

在两个单元都运行之后，命令会从一个单元复制到另一个单元，如下所示：

- 对于在安全上下文之内输入的命令，命令将从安全上下文在其上处于活动状态的单元复制到对等单元。**注意：** 如果上下文所属的故障切换组在一个单元上处于活动状态，则上下文在该单元上会视为处于活动状态。
- 对于在系统执行空间中输入的命令，命令将从故障切换组 1 在其上处于活动状态的单元复制到故障切换组 1 在其上处于备用状态的单元。
- 对于在管理上下文中输入的命令，命令将从故障切换组 1 在其上处于活动状态的单元复制到故障切换组 1 在其上处于备用状态的单元。

所有配置和文件命令(**复制、重命名、删除、**mkdir、rmdir等)都会复制，但这些情况除外。不会复制**show、debug、mode、firewall 和 failover lan unit 命令。**

未在要进行命令复制的相应单元上输入命令会导致配置不同步。下次进行初始配置同步时，这些更改可能会丢失。

您可以使用 **write standby 命令，以重新同步尚未同步的配置。**对于主用/写**入备**用主用故障转移，**write standby命**令的行为如下所示：

- 如果在系统执行空间中输入 **write standby 命令，则安全设备上的系统配置和所有安全上下文的配置都会写入对等单元。**这包括处于备用状态的安全上下文的配置信息。您必须在故障切换组 1 处于活动状态的单元上的系统执行空间中输入命令。**注意：**如果对等设备上有处于活动状态的安全情景，则**write standby** 命令会终止通过这些情景的活动连接。在提供配置的设备**上使用 failover active**命令，以确保在输入write standby命令之前该设备上的所有情景都**处于活动状态**。
- 如果您在安全上下文中输入 **write standby 命令，则只有安全上下文的配置会写入对等单元。**您必须在单元上的安全上下文中输入命令，且该单元应处于活动状态。

当命令复制到对等单元时，复制的命令不会保存到闪存。这些命令会添加到运行中的配置。要在两个单元上将复制的命令保存到闪存，请在已进行更改的单元上使用 **write memory 或 copy running-config startup-config 命令。**命令将复制到对等单元，并使配置保存到对等单元上的闪存。

故障切换触发器

在主用/主用故障切换中，如果发生以下事件之一，可以在设备级别触发故障切换：

- 单元发生硬件故障。
- 单元发生电源故障。
- 单元存在软件故障。
- 在系统执行空间中输入 **no failover active 或 failover active 命令。**

当下列任一事件发生时，会在故障切换组级别上触发故障切换：

- 组中太多受监视的接口发生故障。
- 输入 **no failover active group group_id 或 failover active group group_id 命令。**

故障切换操作

在活动/活动故障切换配置中，故障切换会基于故障切换组发生，而不是基于系统。例如，如果您在主要单元上指定两个故障切换组都处于活动状态，而故障切换组 1 发生故障，则主要单元上的故障切换组 2 仍处于活动状态，而辅助单元上的故障切换组 1 会变为活动状态。

注意：配置主用/主用故障切换时，请确保两台设备的组合流量在每台设备的容量内。

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，策略（无论是否发生故障切换）、活动故障切换组的操作以及备用故障切换组的操作都会给出。

故障事件	**策略**	**活动组操作**	**备用组操作**	**备注**
单元发生电源或软件故障	故障转移	变为备用单元并标记为发生故障	变为备用单元。将活动单元标记为发生故障	当故障切换对中的一个单元发生故障时，该单元上的所有活动故障切换组都将标记为发生故障并在对等单元上变为活动状态。
活动故障切换组上的接口故障超过阈值	故障转移	将活动组标记为发生故障	变为活动单元	无
备用故障切换组上的接口故障超过阈值	不执行故障切换	无操作	将备用组标记为发生故障	当备用故障切换组标记为发生故障时，活动故障切换组不会尝试进行故障切换（即使超过接口故障阈值）。
先前的活动故障切换组恢复	不执行故障	无操作	无操作	除非使用 preempt **命令进行了配置，否则故障切换组会在其当前单元上保持活动状态。**

	切换			
故障切换链路在启动时发生故障	不执行故障切换	变为活动单元	变为活动单元	如果故障切换链路在启动时关闭，则两个单元上的故障切换组都会变为活动状态。
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。
故障切换链路在操作期间发生故障	不执行故障切换	不适用	不适用	每个单元都会将故障切换接口标记为发生故障。您应该尽快恢复故障切换链路，因为故障切换链路关闭时，活动单元无法故障切换到备用单元。

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。当新的活动单元接管时，客户端需要重新建立连接。

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（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。呼叫终止时，IP SoftPhone 客户端将丢失与 Call Manager 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。如果 IP SoftPhone 客户端在特定时间内未收到 Call Manager 的响应，则会认为无法访问 Call Manager 从而自行注销。

故障切换配置限制

您无法使用以下类型的 IP 地址配置故障切换：

- 通过 DHCP 获得的 IP 地址
- 通过 PPPoE 获得的 IP 地址
- IPv6 地址

此外，还适用以下限制：

- ASA 5505 自适应安全设备不支持有状态的故障切换。
- ASA 5505 自适应安全设备不支持活动/活动故障切换。
- 当在 ASA 5505 自适应安全设备上启用 Easy VPN Remote 时，您无法配置故障切换。
- 多上下文模式下不支持 VPN 故障切换。

不支持的功能

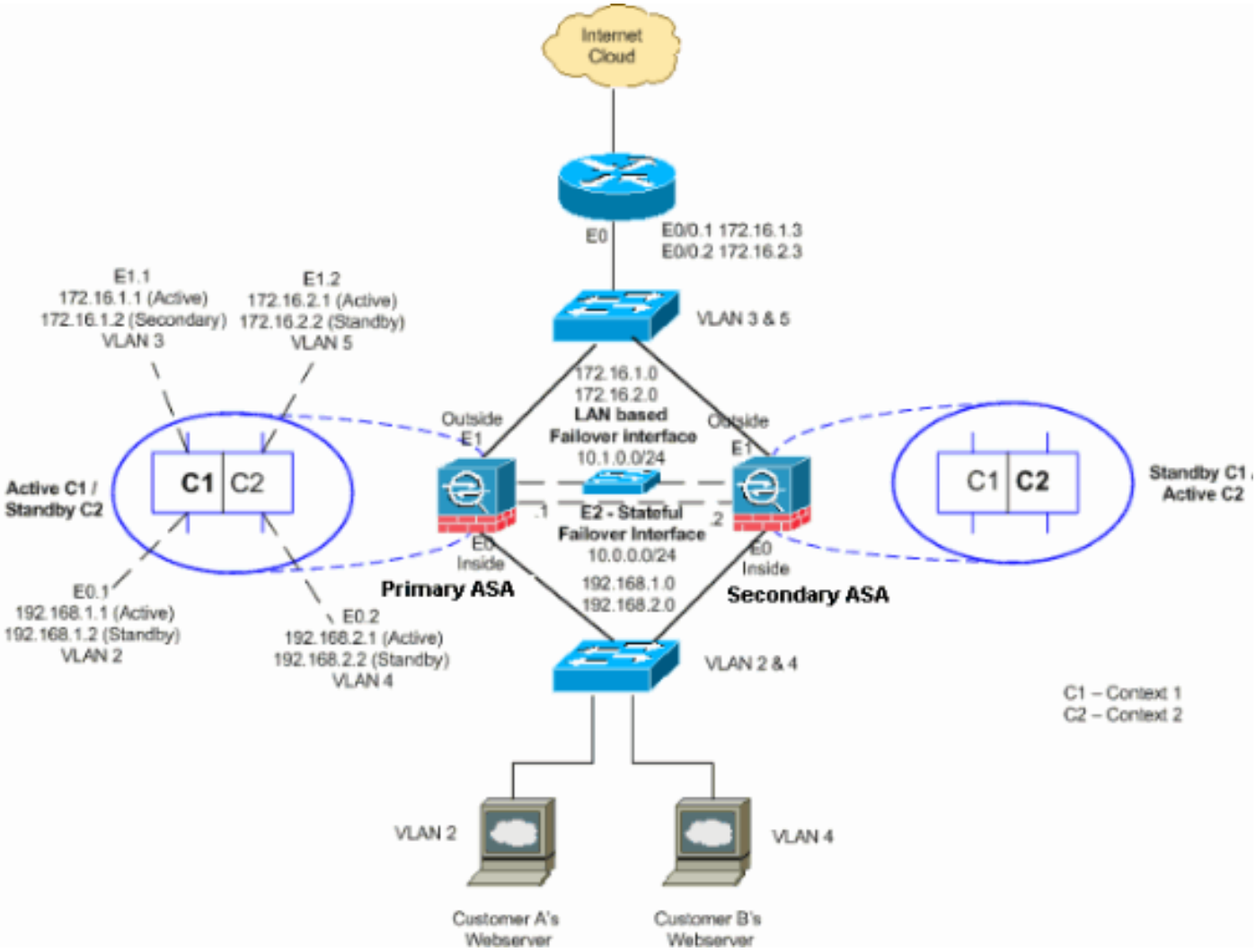
多上下文模式不支持以下功能：

- 动态路由协议安全上下文仅支持静态路由。不能在多上下文模式下启用 OSPF 或 RIP。
- VPN
- 组播

基于 LAN 的活动/活动故障切换配置

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配置主用/主用故障切换。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：思科建议您在主设备和辅助设备之间使用专用交换机，而不是使用交叉以太网电缆直接连接设备。

本部分包含如下主题：

- 主要单元配置
- 辅助单元配置

主要单元配置

完成以下步骤，以在活动/活动故障切换配置中配置主要单元：

1. 为每个数据接口（路由模式）、管理 IP 地址（透明模式）或仅管理接口配置活动和备用 IP 地址（如果尚未配置）。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。您必须从每个上下文的内部配置接口地址。使用 **changeto context 命令可在上下文之间进行切换。**命令提示符将变为 hostname/context(config-if)#，其中 context 是当前上下文的名称。在透明防火墙模式下，您必须输入每个上下文的管理 IP 地址。**注意：**如果使用专用的状态故障切换接口，请勿为状态故障切换链路配置IP地址。在后续步骤中，**使用 failover interface ip命令**配置专用的状态故障切换接口。

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

在示例中，主要ASA的context1的外部接口配置方式如下：

```
ASA/context1(config)#ip address 172.16.1.1 255.255.255.0
                                    standby 172.16.1.2
```

对于 Context2：

```
ASA/context2(config)#ip address 192.168.2.1 255.255.255.0
                                    standby 192.168.2.2
```

在路由防火墙模式下，对于仅管理接口，在接口配置模式下为每个接口输入此命令。在透明防火墙模式下，在全局配置模式下输入此命令。

2. 在系统执行空间中配置基本的故障切换参数。（仅限 PIX 安全设备）启用基于 LAN 的故障切换：

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

将该单元指定为主要单元：

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

指定故障切换链路：

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

在本示例中，我们使用接口以太网 3 作为基于 LAN 的故障切换接口。

```
ASA(config)#failover lan interface LANFailover ethernet3
```

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）。在ASA 5505自适应安全设备上，phy_if指定VLAN。此接口不可用于任何其他用途（但可以选择用作有状态的故障切换链路）。指定故障切换链路的活动和备用 IP 地址：

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

对于本示例，我们将 10.1.0.1 用作故障切换接口的活动 IP 地址，10.1.0.2 用作其备用 IP 地址。

```
ASA(config)#failover interface ip LANFailover
      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 IP 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。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。

辅助单元配置

配置基于LAN的主用/主用故障切换时，需要引导辅助设备以识别故障切换链路。这允许辅助单元与主要单元进行通信并从主要单元接收运行配置。

完成以下步骤，以在活动/活动故障切换配置中引导辅助单元：

1. （仅限 PIX 安全设备）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
```

```
ASA(config)#failover lan interface LANFailover ethernet3
```

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）。在ASA 5505自适应安全设备上，phy_if指定VLAN。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
```

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

注意：在配置故障切换接口时，输入此命令与在主设备上输入的命令完全相同。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。启用该接口。

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

3. 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，除非之前另有配置，否则单位会指定为辅助单元。

4. 启用故障切换。

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

在启用故障切换之后，活动单元将运行内存中的配置发送到备用单元。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。**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。

5. 在运行配置完成复制之后，请输入以下命令以将配置保存到闪存：

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

6. 如果需要，请强制将主要单元上处于活动状态的任何故障切换组在辅助单元上变为活动状态。要强制故障切换组在辅助单元上变为活动状态，请在主要单元上的系统执行空间中输入以下命令：

```
hostname#no failover active group group_id
```

group_id 参数指定要在辅助单元上变为活动状态的组。

配置

本文档使用以下配置：

主ASA - Context1配置

```
ASA/context1(config)#show running-config
: Saved
:
ASA Version 7.2(3)
```

```
!
hostname context1
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface inside_context1
 nameif inside
 security-level 100
!--- Configure the active and standby IP's for the
logical inside !--- interface of the context1. ip
address 192.168.1.1 255.255.255.0 standby 192.168.1.2
!
interface outside_context1
 nameif outside
 security-level 0
!--- Configure the active and standby IP's for the
logical outside !--- interface of the context1. ip
address 172.16.1.1 255.255.255.0 standby 172.16.1.2
!
passwd 2KFQnbNIdI.2KYOU encrypted
access-list 100 extended permit tcp any host 172.16.1.1
eq www
pager lines 24
mtu inside 1500
mtu outside 1500
monitor-interface inside
monitor-interface outside
icmp unreachable rate-limit 1 burst-size 1
asdm image flash:/asdm-522.bin
no asdm history enable
arp timeout 14400
static (inside,outside) 172.16.1.1 192.168.1.5 netmask
255.255.255.255
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
telnet timeout 5
ssh timeout 5
!
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
Cryptochecksum:00000000000000000000000000000000
: end
```

主ASA - Context2配置

```
ASA/context2(config)#show running-config
: Saved
:
ASA Version 7.2(3)




!
hostname context2
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface inside_context2
 nameif inside
 security-level 100
!--- Configure the active and standby IP's for the
logical inside !--- interface of the context2. ip
address 192.168.2.1 255.255.255.0 standby 192.168.2.2
!
interface outside_context2
 nameif outside
 security-level 0
!--- Configure the active and standby IP's for the
logical outside !--- interface of the context2. ip
address 172.16.2.1 255.255.255.0 standby 172.16.2.2
!
passwd 2KFQnbNIdI.2KYOU encrypted
access-list 100 extended permit tcp any host 172.16.2.1
eq www
pager lines 24
mtu inside 1500
mtu outside 1500
monitor-interface inside
monitor-interface outside
icmp unreachable rate-limit 1 burst-size 1
asdm image flash:/asdm-522.bin
no asdm history enable
arp timeout 14400
static (inside,outside) 172.16.2.1 192.168.2.5 netmask
255.255.255.255
access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.2.3 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
telnet timeout 5
ssh timeout 5
!
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
Cryptochecksum:00000000000000000000000000000000
: end
```

主ASA

```
ASA(config)#show running-config
: Saved
:
ASA Version 7.2(3) <system>
!
 !--- Use the firewall transparent command !--- in
global configuration mode in order to !--- set the
firewall mode to transparent mode.

firewall transparent
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
no mac-address auto
!
interface Ethernet0
!
interface Ethernet0.1
 vlan 2
!
interface Ethernet0.2
 vlan 4
```

```
!
interface Ethernet1
!
interface Ethernet1.1
 vlan 3
!
interface Ethernet1.2
 vlan 5
!
!--- Configure "no shutdown" in the stateful failover
interface as well as !--- LAN Failover interface of both
Primary and secondary ASA/PIX. interface Ethernet2
description STATE Failover Interface
!
interface Ethernet3
 description LAN Failover Interface
!
interface Ethernet4
 shutdown
!
interface Ethernet5
 shutdown
!
class default
  limit-resource All 0
  limit-resource ASDM 5
  limit-resource SSH 5
  limit-resource Telnet 5
!

ftp mode passive
pager lines 24
failover
failover lan unit primary
!--- Command to assign the interface for LAN based
failover failover lan interface LANFailover Ethernet3
!--- Configure the Authentication/Encryption key
failover key *****
failover link stateful Ethernet2
!--- Configure the active and standby IP's for the LAN
based failover failover interface ip LANFailover
10.1.0.1 255.255.255.0 standby 10.1.0.2
failover interface ip stateful 10.0.0.1 255.255.255.0
standby 10.0.0.2
failover group 1
failover group 2
  secondary
no asdm history enable
arp timeout 14400
console timeout 0

admin-context admin
context admin
  config-url flash:/admin.cfg
!

context context1
  allocate-interface Ethernet0.1 inside_context1
  allocate-interface Ethernet1.1 outside_context1
  config-url flash:/context1.cfg
  join-failover-group 1
!

context context2
```

```
  allocate-interface Ethernet0.2 inside_context2
  allocate-interface Ethernet1.2 outside_context2
  config-url flash:/context2.cfg
  join-failover-group 2
!

prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

辅助ASA

```
ASA#show running-config

failover
failover lan unit secondary
failover lan interface LANFailover Ethernet3
failover key *****
failover interface ip LANFailover 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(config-subif)#show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: LANFailover Ethernet3 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Version: Ours 7.2(3), Mate 7.2(3)
Group 1 last failover at: 06:12:45 UTC Jan 17 2009
Group 2 last failover at: 06:12:43 UTC Jan 17 2009

  This host:    Primary
  Group 1       State:          Active
                Active time:    359610 (sec)
  Group 2       State:          Standby Ready
                Active time:    3165 (sec)

                  context1 Interface inside (192.168.1.1): Normal
                  context1 Interface outside (172.16.1.1): Normal
                  context2 Interface inside (192.168.2.2): Normal
                  context2 Interface outside (172.16.2.2): Normal

  Other host:   Secondary
  Group 1       State:          Standby Ready
                Active time:    0 (sec)
  Group 2       State:          Active
                Active time:    3900 (sec)
```

```
                  context1 Interface inside (192.168.1.2): Normal
                  context1 Interface outside (172.16.1.2): Normal
                  context2 Interface inside (192.168.2.1): Normal
                  context2 Interface outside (172.16.2.1): Normal

Stateful Failover Logical Update Statistics
        Link : stateful Ethernet2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         48044      0          48040      1
        sys cmd         48042      0          48040      1
        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         2          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       72081
        Xmit Q:         0       1       48044
```

辅助ASA

```
ASA(config)#show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Secondary
Failover LAN Interface: LANFailover Ethernet3 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Version: Ours 7.2(3), Mate 7.2(3)
Group 1 last failover at: 06:12:46 UTC Jan 17 2009
Group 2 last failover at: 06:12:41 UTC Jan 17 2009

  This host:    Secondary
  Group 1       State:          Standby Ready
                Active time:    0 (sec)
  Group 2       State:          Active
                Active time:    3975 (sec)

                  context1 Interface inside (192.168.1.2): Normal
                  context1 Interface outside (172.16.1.2): Normal
                  context2 Interface inside (192.168.2.1): Normal
                  context2 Interface outside (172.16.2.1): Normal

  Other host:   Primary
  Group 1       State:          Active
                Active time:    359685 (sec)
  Group 2       State:          Standby Ready
                Active time:    3165 (sec)

                  context1 Interface inside (192.168.1.1): Normal
                  context1 Interface outside (172.16.1.1): Normal
                  context2 Interface inside (192.168.2.2): Normal
                  context2 Interface outside (172.16.2.2): Normal

Stateful Failover Logical Update Statistics
        Link : stateful Ethernet2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
```

```
        General         940        0          942        2
        sys cmd         940        0          940        2
        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          2          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       1419
        Xmit Q:         0       1       940
```

使用 **show failover state** 命令可验证状态。

主ASA

```
ASA(config)#show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
    Group 1    Active         None
    Group 2    Standby Ready  None
Other host -   Secondary
    Group 1    Standby Ready  None
    Group 2    Active         None

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

辅助单元

```
ASA(config)#show failover state

               State          Last Failure Reason      Date/Time
This host  -   Secondary
    Group 1    Standby Ready  None
    Group 2    Active         None
Other host -   Primary
    Group 1    Active         None
    Group 2    Standby Ready  None

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

若要验证故障切换单元的 IP 地址，请使用 **show failover interface** 命令。

主要单元

```
ASA(config)#show failover interface
        interface stateful Ethernet2
                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
        interface LANFailover Ethernet3
                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
```

辅助单元

```
ASA(config)#show failover interface
        interface LANFailover Ethernet3
                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 stateful Ethernet2
                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` 在多上下文模式下，请在上下文内输入 `show monitor-interface`

注意：要在特定接口上启用运行状况监控，请在全局配置模式下使用monitor-interface命令：

```
monitor-interface <if_name>
```

主ASA

```
ASA/context1(config)#show monitor-interface
        This host: Secondary - Active
                Interface inside (192.168.1.1): Normal
                Interface outside (172.16.1.1): Normal
        Other host: Secondary - Standby Ready
                Interface inside (192.168.1.2): Normal
                Interface outside (172.16.1.2): Normal
```

辅助ASA

```
ASA/context1(config)#show monitor-interface
        This host: Secondary - Standby Ready
                Interface inside (192.168.1.2): Normal
                Interface outside (172.16.1.2): Normal
        Other host: Secondary - Active
                Interface inside (192.168.1.1): 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作为IP地址，并且对接口的监控仍处于等待态。您必须为故障切换设置一个故障切换 IP 地址以便其正常工作。有关故障切换的不同状态的详细信息，请参阅show failover。

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` 输入 **show running-config all failover 命令以显示运行配置中的故障切换命令，包括未更改默认值的命令。**

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. 测试主用设备或故障切换组是否按照预期通过FTP传递流量，例如，在不同接口上的主机之间发送文件。
2. 使用以下命令强制向备用单元执行故障切换：对于主用/主用故障切换，请在故障切换组所在的设备上输入以下命令，该故障切换组包含连接主机的接口：
   `hostname(config)#no failover active group group_id`

3. 使用FTP在同一台主机之间发送另一个文件。
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：对于主用/主用故障切换，请在故障切换组所在的设备上输入以下命令，该故障切换组包含连接主机的接口：
   `hostname(config)#failover active group group_id`

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：

请在故障切换组在其中处于备用状态的单元的系统执行空间中输入以下命令：

```
hostname#failover active group group_id
```

或者，在故障切换组在其中处于活动状态的单元的系统执行空间中输入以下命令：

```
hostname#no failover active group group_id
```

在系统中输入此命令时，执行空间会导致所有故障切换组变为活动状态：

```
hostname#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。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

为了将出现故障的活动/活动故障切换组恢复到未出现故障的状态，请输入以下命令：

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

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。本部分包括以下主题：

1. 故障切换系统消息
2. 调试消息
3. SNMP

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。

主要单元在接口 interface_name 上丢失了与伙伴的故障切换通信

如果故障切换对的一个单元无法再与该对的另一个单元通信，则会显示以下故障切换消息。主要 单元也能列为辅助单元的备件。

（主要单元）在接口 interface_name 上丢失了与伙伴的故障切换通信

检验连接到指定接口的网络是否正常运行。

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 7.2 版。

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 7.2 版中的 **snmp-server 和日志记录命令。**

故障切换轮询时间

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发出 **failover polltime 命令。**

```
failover polltime unit msec [time]  hello
```

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

有关详细信息，请参阅故障切换轮询时间。

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。

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