ASA/PIX:在透明模式下配置主用/主用故障切換

目錄

警告：故障轉移消息解密失敗。
相關資訊

簡介

故障切換配置需要兩個完全相同的安全裝置，它們通過專用故障切換鏈路和狀態故障切換鏈路相互連線。活動介面和裝置的運行狀況受到監控，以確定是否滿足特定的故障切換條件。如果滿足這些條件，則進行故障切換。

安全裝置支援兩種故障切換配置：

- 主用/主用故障轉移
- 主用/備用故障轉移

每個故障切換配置都有自己的方法來確定和執行故障切換。通過主用/主用故障轉移，兩台裝置都可以傳遞網路流量。這樣，您便可以在網路上配置負載均衡。「主用/主用故障轉移」僅適用於在多情景模式下運行的裝置。使用主用/備用故障切換時，只有一個單元會傳遞流量，而另一個單元在備用狀態下等待。在單情景或多情景模式下運行的裝置上提供主用/備用故障轉移。兩種故障切換配置都支援有狀態或無狀態（常規）故障切換。

透明防火牆是第2層防火牆，其作用類似於線路中的*bump*或*stealth firewall*，不會被視為連線到裝置的路由器躍點。安全裝置在其內部和外部埠上連線同一網路。由於防火牆不是路由躍點，因此您可以輕鬆地在現有網路中引入透明防火牆；無需重新定址IP。您可以將自適應安全裝置設定為在預設路由防火牆模式或透明防火牆模式下運行。更改模式時，自適應安全裝置會清除配置，因為兩種模式均不支援許多命令。如果您已填入組態，請在變更模式之前務必備份此組態；您可以使用此備份配置作為建立新配置的參考。有關透明模式下防火牆裝置配置的詳細資訊，請參閱透明防火牆配置示例。

本文檔重點介紹如何在ASA安全裝置上以透明模式配置主用/主用故障切換。

注意：在多情景模式下運行的裝置上不支援VPN**故障**轉移。VPN故障切換僅適用於主**用/備用故**障切換配置。

思科建議您不要將管理介面用於故障切換，尤其是對於安全裝置不斷將連線資訊從一個安全裝置傳送到另一個安全裝置的狀態故障切換。故障轉移的介面必須至少與傳遞常規流量的介面具有相同容量，而且，雖然ASA 5540上的介面是千兆位介面，但管理介面僅是FastEthernet。管理介面設計為僅用於管理流量，並指定為management0/0。但是，您可以使用**management-only**命令將任何介面配置為僅管理介面。此外，對於管理0/0，您可以禁用僅管理模式，以便介面可以像任何其它介面一樣通過流量。有關**management-only**命令的詳細資訊，請參閱思科安全裝置命令參考8.0版。

本配置指南提供示例配置，其中包含ASA/PIX 7.x主用/備用技術的簡要介紹。請參閱ASA/PIX命令參考指南以瞭解基於此技術的理論的更深層含義。

必要條件

需求

硬體要求

故障切換配置中的兩個裝置必須具有相同的硬體配置。它們必須是相同的型號，具有相同的介面數量和型別以及相同的RAM大小。

注意：這兩個單元不需要具有相同大小的快閃記憶體。如果在故障切換配置中使用快閃記憶體大小不同的裝置，請確保快閃記憶體較小的裝置有足夠的空間容納軟體映像檔案和配置檔案。如果沒有，則從快閃記憶體較大的裝置到快閃記憶體較小的裝置的配置同步失敗。

軟體需求

故障切換配置中的兩個裝置必須處於操作模式（路由或透明、單情景或多情景）。 它們必須具有相同的主要（第一個數字）和次要（第二個數字）軟體版本，但是您可以在升級過程中使用不同版本的軟體；例如，您可以將一個裝置從7.0(1)版升級到7.0(2)版，並使故障切換保持活動狀態。思科建議將兩台裝置升級到相同版本以確保長期相容性。

有關如何升級故障轉移對上的軟體的詳細資訊，請參閱*思科安全裝置命令列配置指南8.0版*中的對故障轉移對執行零停機升級部分。

許可證要求

在ASA安全裝置平台上，至少一個裝置必須具有不受限**制(UR)許可證**。

注意：可能需要升級故障轉移對上的許可證，以獲得其他功能和優勢。有關詳細資訊，請參閱故障轉移對上的許可證金鑰升級。

注意：**參**與故障切換的兩個安全裝置上的許可功能（例如SSL VPN對等裝置或安全情景）必須相同。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 7.x及更高版本的ASA安全裝置

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

相關產品

此配置還可以用於以下硬體和軟體版本：

- 7.x及更高版本的PIX安全裝置

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

主用/主用故障轉移

本節介紹主用/備用故障切換，包括以下主題：

- 主用/主用故障切換概述
- 主要/輔助狀態和活動/備用狀態
- 裝置初始化和組態同步
- 命令複製

- 故障轉移觸發器
- 故障切換操作

主用/主用故障切換概述

主用/主用故障切換僅適用於多情景模式下的安全裝置。在主用/主用故障切換配置中，兩個安全裝置都可以傳遞網路流量。

在主用/主用故障切換中，將安全裝置上的安全情景分為故障切換組。故障切換組只是一個或多個安全情景的邏輯組。在安全裝置上最多可以建立兩個故障轉移組。管理上下文始終是故障轉移組1的成員。預設情況下，任何未分配的安全上下文也是故障轉移組1的成員。

故障切換組構成主用/主用故障切換中故障切換的基本單元。介面故障監控、故障切換和主用/備用狀態是故障切換組而不是裝置的所有屬性。當活動故障切換組發生故障時，當備用故障切換組變為活動狀態時，該故障切換組將變為備用狀態。故障轉移組中變為活動狀態的介面假定發生故障的故障轉移組中的介面的MAC和IP地址。故障切換組中目前處於備用狀態的介面將接管備用MAC和IP地址。

注意：裝置上的故障切換組發生故障並不表示裝置發生故障。裝置仍然可以有另一個故障轉移組來傳遞流量。

主要/輔助狀態和活動/備用狀態

與主用/備用故障切換一樣，主用/主用故障切換對中的一個裝置被指定為主裝置，另一個裝置被指定為輔助裝置。與主用/備用故障切換不同，此標識不指示當兩個裝置同時啟動時哪個裝置變為主用裝置。相反，主/輔指定具有兩個作用：

- 確定當裝置對同時啟動時，哪個裝置為其提供運行配置。
- 確定當裝置同時啟動時，每個故障切換組出現在哪個裝置上。配置中的每個故障轉移組都配置了主裝置或輔助裝置首選項。可以將兩個故障切換組配置為對中單個裝置上的主用狀態，而將包含故障切換組的另一裝置配置為備用狀態。但是，更典型的配置是為每個故障切換組分配不同的角色首選項，以使每個故障切換組在不同的裝置上都處於活動狀態，並在裝置之間分配流量。**注意**：安全裝置**不提供**負載均衡服務。負載均衡必須由將流量傳送到安全裝置的路由器來處理。

確定每個故障切換組在哪個裝置上變為活動狀態，如下所示

- 當裝置啟動而對等裝置不可用時，兩個故障切換組都會在該裝置上變為活動狀態。
- 當裝置在對等裝置處於主用狀態（兩個故障切換組均處於主用狀態）時啟動時，無論故障切換組的主首選項或輔助首選項如何，故障切換組都會保持主用裝置上的主用狀態，直到發生以下情況之一：發生故障轉移。您可以使用**no failover active**命令手動將故障切換組強制切換到其他裝置您使用**preempt**命令配置故障切換組，這會使故障切換組在首選裝置可用時自動成為主用裝置。
- 當兩個裝置同時啟動時，配置同步後，每個故障切換組在其首選裝置上變為活動狀態。

裝置初始化和組態同步

當故障轉移對中的一個或兩個裝置啟動時，會發生配置同步。配置已同步，如下所示：

- 當裝置在對等裝置處於主用狀態（兩個故障切換組都處於主用狀態）時啟動時，引導裝置會與

主用裝置聯絡以獲取運行配置，而不管引導裝置的主要或次要指定是什麼。
- 當兩個裝置同時啟動時，輔助裝置從主裝置獲取運行配置。

複製啟動時，傳送配置的裝置上的安全裝置控制檯會顯示消息Sending to mate完成後，安全裝置顯示消息「End Configuration Replication to mate 在複製期間，在傳送配置的裝置上輸入的命令不能正確複製到對等裝置，在接收配置的裝置上輸入的命令可能被收到的配置覆蓋。在配置複製過程中，請勿在故障切換對中的任一裝置上執行命令。複製過程取決於配置的大小，可能需要幾秒鐘到幾分鐘。

在接收配置的裝置上，配置僅存在於運行記憶體中。要在同步後將配置儲存到快閃記憶體，請在故障切換組1處於活動狀態的裝置上的系統執行空間中輸入**write memory all**命令。該命令被複製到對等單元，該對等單元繼續將其配置寫入快閃記憶體。在此命令中使用**all**關鍵字將導致儲存系統和所有上下文配置。

注意：儲存在外部伺服器上的啟動配置可以通過網路從任一裝置訪問，無需為每個裝置單獨儲存。或者，您可以將情景配置檔案從主裝置上的磁碟複製到外部伺服器，然後將它們複製到輔助裝置上的磁碟上，在輔助裝置重新載入時這些配置檔案可用。

命令複製

兩台裝置運行後，命令從一台裝置複製到另一台，如下所示：

- 在安全上下文內輸入的命令從安全上下文顯示為活動狀態的單元複製到對等單元。**附註：** 如果裝置所屬故障轉移組在該裝置上處於活動狀態，則該裝置上的情景被視為處於活動狀態。
- 在系統執行空間中輸入的命令從故障切換組1處於活動狀態的裝置複製到故障切換組1處於備用狀態的裝置。
- 在管理上下文中輸入的命令將從故障切換組1處於活動狀態的裝置複製到故障切換組1處於備用狀態的裝置。

所有配置和檔案命令(**copy、rename、delete、mkdir、rmdir**等)都會被複製，但以下情況除外。**show、debug、mode、firewall**和**failover lan unit**命令不會複製。

未能在適當的裝置上輸入命令以進行命令複製會導致配置不同步。下次進行初始配置同步時，這些更改可能會丟失。

您可以使用**write standby**命令重新同步已不同步的配置。對於主用/**write standby**主用故障切換，**write standby**命令的行為如下所示：

- 如果在系統執行空間中輸入**write standby**命令，則安全裝置上所有安全上下文的系統配置和配置都將寫入對等裝置。其中包括處於備用狀態的安全上下文的配置資訊。必須在故障切換組1處於活動狀態的裝置上的系統執行空間中輸入命令。**注意：如**果對等裝置上存在處於活動狀態的安全情景，則**write standby命令會導致通過這些情景的活動連線終止。**在提供配置的裝置上使用**failover active**命令，確保在輸入**write standby**命令之前該裝置上所有情景都處於活**動狀**態。
- 如果在安全上下文中輸入**write standby**命令，則只有安全上下文的配置才會寫入對等裝置。必須在安全上下文出現在活動狀態的裝置上的安全上下文中輸入該命令。

複製到對等裝置時，複製的命令不會儲存到快閃記憶體。它們被新增到運行配置中。要將複製命令儲存到兩台裝置上的快閃記憶體中，請在進行更改的裝置上使用**write memory**或**copy running-config startup-config**命令。該命令會複製到對等單元，並使配置儲存到對等單元上的快閃記憶體中。

故障轉移觸發器

在主用/主用故障切換中，如果發生以下事件之一，可以在裝置級別觸發故障切換：

- 裝置出現硬體故障。
- 裝置出現電源故障。
- 裝置出現軟體故障。
- 在系統執行空間中輸入**no failover active**或**failover active**命令。

當發生以下事件之一時，將在故障切換組級別觸發故障切換：

- 組中太多受監控的介面出現故障。
- 輸入了**no failover active group group_id**或**failover active group group_id**命令。

故障切換操作

在主用/主用故障切換配置中，故障切換以故障切換組為基礎，而不是以系統為基礎。例如，如果將兩個故障切換組指定為主裝置上的主用故障切換組，並且故障切換組1發生故障，則故障切換組2在主裝置上保持主用狀態，而故障切換組1在輔助裝置上變為主用狀態。

注意：配置主用/主用故障切換時，請確保兩台裝置的合併流量都在每台裝置的容量內。

此表顯示了每個故障事件的故障切換操作。對於每個故障事件，都會給出策略、是否發生故障轉移、活動故障切換組的操作以及備用故障切換組的操作。

故障事件	政策	活動組操作	備用組操作	備註
裝置出現電源或軟體故障	容錯移轉	變為備用標籤as failed	待命。將活動標籤為失敗	當故障轉移對中的某個裝置發生故障時，該裝置上的任何活動故障轉移組都會標籤為發生故障，並在對等裝置上變為活動狀態。
活動故障轉移組上的介面故障超過閾值	容錯移轉	將活動組標籤為失敗	啟用	無
備用故障轉移組上的介面故障超過閾值	無故障切換	無操作	將備用組標籤為失敗	當備用故障轉移組標籤為發生故障時，主用故障轉移組不會嘗試進行故障轉移，即使超過介面故障閾值也是如此。

以前的活動故障切換組恢復	無故障切換	無操作	無操作	除非使用**preempt**命令進行配置，否則故障切換組在其當前裝置上保持活動狀態。
故障轉移鏈路在啟動時失敗	無故障切換	啟用	啟用	如果故障切換鏈路在啟動時關閉，兩台裝置上的兩個故障切換組都將變為活動狀態。
狀態故障切換鏈路失敗	無故障切換	無操作	無操作	狀態資訊已過期，如果發生故障轉移，會話將被終止。
故障切換鏈路在操作期間失敗	無故障切換	不適用	不適用	每台裝置將故障切換介面標籤為發生故障。您應儘快恢復故障切換鏈路，因為當故障切換鏈路關閉時，裝置無法故障切換到備用裝置。

常規和狀態故障切換

安全裝置支援兩種型別的故障轉移：常規故障轉移(Regular)和有狀態故障轉移(Stateful)。本節包括以下主題：

常規故障轉移

發生故障切換時，所有活動連線都將被丟棄。當新的活動單元接管時，客戶端需要重新建立連線。

狀態容錯移轉

啟用狀態故障切換後，主用裝置會不斷將每個連線的狀態資訊傳遞給備用裝置。發生故障切換後，新的主用裝置會提供相同的連線資訊。無需支援的終端使用者應用程式重新連線即可保持相同的通訊會話。

傳遞給備用單元的狀態資訊包括：

- NAT轉換表
- TCP連線狀態
- UDP連線狀態
- ARP表
- 第2層橋接表（當其在透明防火牆模式下運行時）
- HTTP連線狀態（如果已啟用HTTP複製）
- ISAKMP和IPSec SA表
- GTP PDP連線資料庫

啟用有狀態故障切換時，未傳遞給備用單元的資訊包括：

- HTTP連線表（除非已啟用HTTP複製）
- 使用者驗證(uauth)表
- 路由表
- 安全服務模組的狀態資訊

附註： 如果在活動Cisco IP SoftPhone會話中發生故障切換，呼叫將保持活動狀態，因為呼叫會話狀態資訊會複製到備用裝置。當呼叫終止時，IP SoftPhone客戶端將失去與呼叫管理器的連線。之所以會出現這種情況，是因為備用裝置上沒有CTIQBE掛斷消息的會話資訊。當IP SoftPhone客戶端在某個時間段內未收到來自呼叫管理器的響應時，它將認為呼叫管理器不可達且會自行註銷。

故障切換配置限制

不能使用以下型別的IP地址配置故障切換：

- 通過DHCP獲取的IP地址
- 通過PPPoE獲取的IP地址
- IPv6地址

此外，以下限制適用：

- ASA 5505自適應安全裝置不支援狀態故障切換。
- ASA 5505自適應安全裝置不支援主用/主用故障切換。
- 在ASA 5505自適應安全裝置上啟用Easy VPN Remote時，無法配置故障轉移。
- 多情景模式不支援VPN故障切換。

不支援的功能

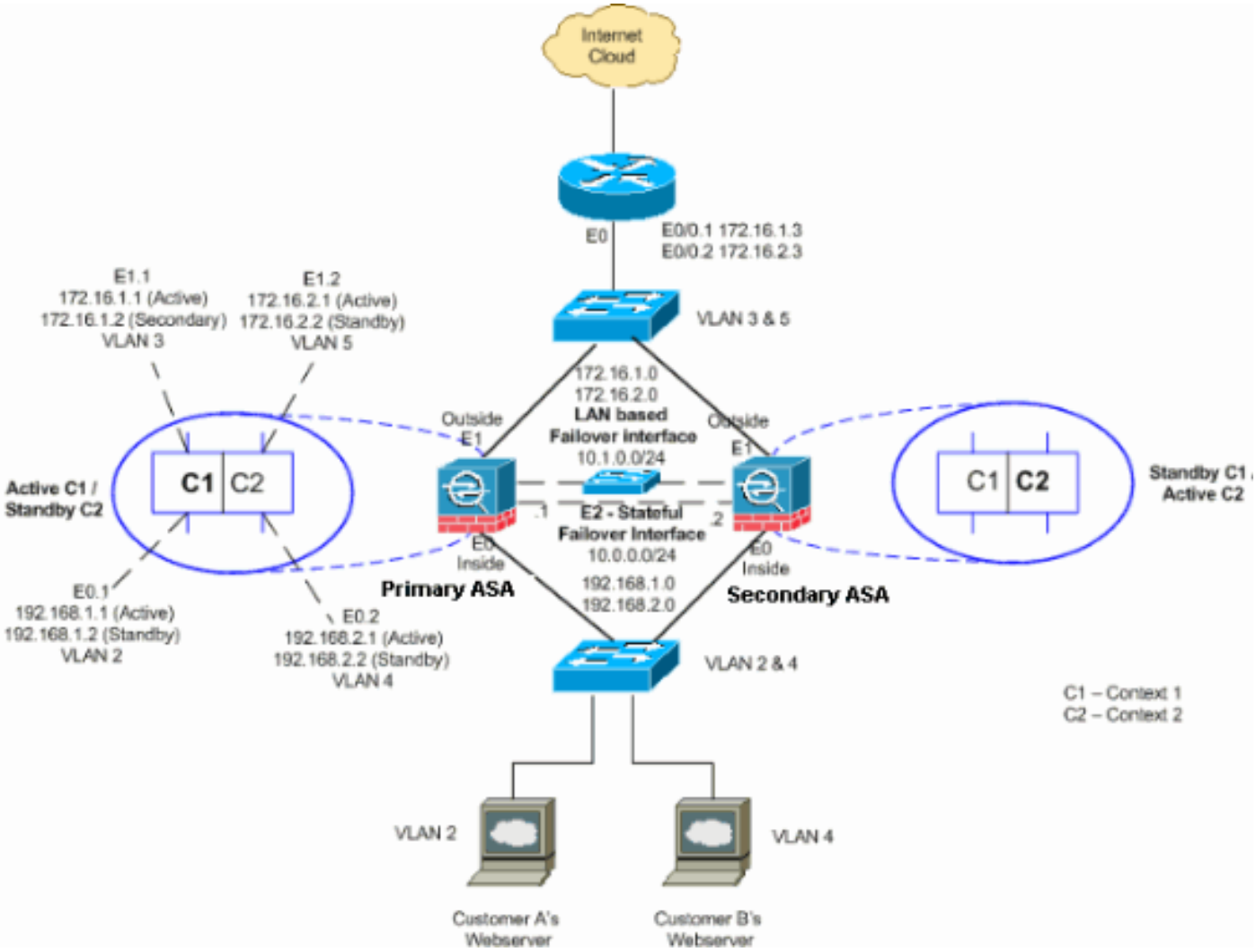
多情景模式不支援以下功能：

- 動態路由協定安全情景僅支援靜態路由。不能在多情景模式下啟用OSPF或RIP。
- VPN
- 多點傳播

基於LAN的主用/主用故障切換配置

網路圖表

本檔案會使用以下網路設定：



本節介紹如何使用乙太網故障切換鏈路配置主用/主用故障切換。配置基於LAN的故障切換時，必須先引導輔助裝置以識別故障切換鏈路，然後輔助裝置才能從主裝置獲取運行配置。

注意：思科建議您在主要裝置和輔助裝置之間使用專用交換機，而不是使用交叉乙太網電纜直接連線裝置。

本節包括以下主題：

- 主裝置配置
- 輔助裝置配置

主裝置配置

完成以下步驟，以在主用/主用故障切換配置中配置主裝置：

1. 如果尚未配置主用和備用IP地址，請為每個資料介面（路由模式）、管理IP地址（透明模式）或僅管理介面配置主用和備用IP地址。備用IP地址用於當前作為備用裝置的安全裝置。它必須與活動IP地址位於同一個子網中。您必須在每個情景中配置介面地址。使用**changeto context**命令在情景之間切換。命令提示符將更改為hostname/context(config-if)#，其中context是當前上下文的名稱。在透明防火牆模式下，必須為每個情景輸入管理IP地址。**注意：如**果您使用專用的狀態故障切換介面，則不要為狀態故障切換鏈路配置IP地址。您可以使用**failover interface ip**命令在後續步驟中配置專用有狀態故障切換介面。
   ```
   hostname/context(config-if)#ip address active_addr netmask standby standby_addr
   ```

在本示例中，主ASA的context1的外部介面配置如下：

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

對於Context2:

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

在路由防火牆模式和僅管理介面中，每個介面的介面配置模式下都會輸入此命令。在透明防火牆模式下，命令在全域性配置模式下輸入。

2. 在系統執行空間中配置基本故障切換引數。（僅限PIX安全裝置）啟用基於LAN的故障切換：

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

將該單位指定為主要單位：

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

指定故障切換鏈路：

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

在本例中，我們將介面ethernet 3用作基於LAN的故障切換介面。

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

if_name引數為phy_if引數指定的介面分配邏輯名稱。phy_if引數可以是物理埠名稱（例如Ethernet1）或先前建立的子介面（例如Ethernet0/2.3）。在ASA 5505自適應安全裝置上，phy_if指定VLAN。此介面不應用於任何其他目的（有狀態故障切換鏈路除外）。指定故障切換鏈路的主用和備用IP地址：

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

在本示例中，我們將10.1.0.1用作主用地址，將10.1.0.2用作故障切換介面的備用IP地址。

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

備用IP地址必須與活動IP地址位於同一子網中。您無需標識備用IP地址子網掩碼。故障切換時故障切換鏈路IP地址和MAC地址不會更改。活動IP地址始終位於主裝置上，而備用IP地址則位於輔助裝置上。

輔助裝置配置

配置基於LAN的主用/主用故障切換時，需要引導輔助裝置以識別故障切換鏈路。這樣，輔助裝置就可以與主裝置通訊並從主裝置接收運行配置。

完成以下步驟，以便在主用/主用故障切換配置中引導輔助裝置：

1. （僅限PIX安全裝置）啟用基於LAN的故障切換。

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

2. 定義故障切換介面。使用與主裝置相同的設定：指定要用作故障轉移介面的介面。

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

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

if_name引數為phy_if引數指定的介面分配邏輯名稱。phy_if引數可以是物理埠名稱（例如Ethernet1）或先前建立的子介面（例如Ethernet0/2.3）。在ASA 5505自適應安全裝置上，phy_if指定VLAN。將主用和備用IP地址分配給故障切換鏈路：

```
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：輸入此命令與配置故障切換介面時在主裝置上輸入的命令完全相同。備用IP地址必須與活動IP地址位於同一子網中。您無需標識備用地址子網掩碼。啟用介面。

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

3. 將此裝置指定為輔助裝置：

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

註：此步驟是可選的，因為預設情況下裝置被指定為輔助裝置，除非事先進行了其他配置。

4. 啟用故障轉移。

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

啟用故障切換後，主用裝置會將運行記憶體中的配置傳送到備用裝置。當配置同步時，會出現Beginning configuration replication:Sending to mate和End Configuration Replication to mate顯示在主用裝置控制檯上。**注意**：首先在主裝置上發出failover命令，然後在輔助裝置上發出該命令。在輔助裝置上發出failover命令後，輔助裝置會立即從主裝置拉出配置，並將自身設定為*備用*。主ASA保持正常運行並正常傳遞流量，並將自身標籤為*活動*裝置。從那時起，無論何時主用裝置發生故障，備用裝置都會變為主用裝置。

5. 運行配置完成複製後，輸入以下命令將配置儲存到快閃記憶體：

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

6. 如有必要，強制主裝置上處於活動狀態的所有故障轉移組進入輔助裝置上的活動狀態。要強制故障切換組在輔助裝置上變為活動狀態，請在主裝置上的系統執行空間中輸入以下命令：

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

group_id引數指定要在輔助裝置上處於活動狀態的組。

組態

本檔案會使用以下設定：

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
```

輔助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
```

驗證

使用show failover命令

本節介紹**show failover**命令輸出。在每個裝置上，可以使用**show failover**命令驗證故障切換狀態。

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
```

輔助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** 命令驗證狀態。

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
```

輔助裝置

```
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
```

要驗證故障切換單元的IP地址，請使用**show failover** 介面命令。

主裝置

```
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
```

輔助裝置

```
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
```

受監控介面的檢視

若要檢視受監控介面的狀態：在單情景模式下，在全域性配置模式下輸入`show monitor-interface`命令。在多情景模式下，在情景中輸入`show monitor-interface`。

注意：要在特定介面上啟用運行狀況監控，請在全域性配置模式下使用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
```

輔助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：如果不輸入故障切換IP地址，**show failover**命令將顯示該IP地址的0.0.0.0，並且介面的監控仍保持等待態。您必須設定故障切換IP地址才能使故障切換正常工作。有關故障切換的不同狀態的詳細資訊，請參閱show failover。

運行配置中故障切換命令的顯示

要檢視運行配置中的failover命令，請輸入以下命令：

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

將顯示所有**failover**命令。在多情景模式下運行的裝置上，在系統執行空間中輸入`show running-config failover`命令。輸入**show running-config all failover**命令以在運行配置中顯示故障切換命令，並包括尚未更改預設值的命令。

故障轉移功能測試

完成以下步驟以測試故障轉移功能：

1. 測試您的主用裝置或故障切換組是否按預期通過FTP傳輸流量，例如，在不同介面上的主機之間傳送檔案。
2. 使用以下命令強制故障切換至備用裝置：對於主用/主用故障切換，請在故障切換組（包含連線主機的介面）處於主用狀態的裝置上輸入以下命令：
   ```
   hostname(config)#no failover active group group_id
   ```
3. 使用FTP在同一兩台主機之間傳送另一個檔案。
4. 如果測試未成功，請輸入**show failover**命令以檢查故障切換狀態。
5. 完成後，您可以使用以下命令將裝置或故障切換組還原為活動狀態：對於主用/主用故障切換，請在故障切換組（包含連線主機的介面）處於主用狀態的裝置上輸入以下命令：
   ```
   hostname(config)#failover active group group_id
   ```

強制故障轉移

要強製備用裝置處於活動狀態，請輸入以下命令之一：

在故障切換組處於備用狀態的裝置的系統執行空間中輸入以下命令：

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

或者，在故障切換組處於活動狀態的裝置的系統執行空間中輸入以下命令：

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

在系統中輸入此命令時，執行空間會導致所有故障切換組變為活動狀態：

```
hostname#failover active
```

已禁用故障轉移

若要停用容錯移轉，請輸入以下命令：

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

如果在主用/備用對上禁用故障轉移，將導致每個裝置的主用和備用狀態保持到重新啟動為止。例如，備用裝置保持備用模式，這樣兩個裝置就不會開始傳遞流量。要使備用裝置處於活動狀態（即使禁用了故障轉移），請參見強制故障轉移部分。

如果在主用/主用對上禁用故障切換，將導致故障切換組在其當前處於主用狀態的任一裝置上保持主用狀態，無論它們配置為首選哪台裝置。可以在系統執行空間中輸入**no failover**命令。

恢復故障裝置

要將發生故障的主用/主用故障切換組恢復到未故障狀態，請輸入以下命令：

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

如果將故障裝置恢復為未故障狀態，它不會自動將其啟用；恢復的裝置或組將保持備用狀態，直到通過故障轉移（強制或自然）變為主用狀態。 例外是使用**preempt**命令配置的故障切換組。如果以前處於活動狀態，則如果使用**preempt**命令配置故障轉移組，且其發生故障的單元是其首選單元，則該故障轉移組將變為活動狀態。

疑難排解

發生故障切換時，兩個安全裝置都會傳送系統消息。本節包括以下主題：

1. 故障切換系統消息
2. 調試消息
3. SNMP

故障切換系統消息

安全裝置發出許多與優先順序級別2的故障切換相關的系統消息，指示出現嚴重狀況。要檢視這些消息，請參閱思科安全裝置日誌記錄配置和系統日誌消息以啟用日誌記錄並檢視系統消息的說明。

注意：在切換過程中，故障切換在邏輯上關閉，然後開啟介面，這樣會生成**系統日**志41001**和** 41002消息。這是正常活動。

主要丟失與介面interface_name上的mate的故障切換通訊

如果故障切換對中的一個裝置無法再與故障切換對中的另一個裝置通訊，則會顯示此故障切換消息。對於輔助裝置，主裝置也可以列為輔助裝置。

（主要）在介面interface_name上與mate丟失故障切換通訊

驗證連線到指定介面的網路是否工作正常。

調試消息

若要檢視偵錯訊息，請輸入**debug fover**指令。有關詳細資訊，請參閱思科安全裝置命令參考7.2版。

註：由於調試輸出在CPU進程中分配了高優先順序，因此可能會嚴重影響系統效能。因此，請使用**debug over**命令僅對特定問題進行故障排除，或在與思科技術支援人員進行的故障排除會話中進行。

SNMP

為了接收故障轉移的SNMP系統日誌陷阱，請配置SNMP代理以向SNMP管理站傳送SNMP陷阱，定

義系統日誌主機，並將Cisco syslog MIB編譯到SNMP管理站中。如需詳細資訊，請參閱思科安全裝置命令參考7.2版中的**snmp-server**和**logging**命令。

故障轉移輪詢時間

要指定故障切換裝置輪詢和保持時間，請在全域性配置模式下發出**failover polltime**命令。

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

同樣，`failover holdtime unit msec [time]`表示裝置必須在故障轉移鏈路上接收hello消息的時間段，在此時間段之後，對等裝置被宣告出現故障。

有關詳細資訊，請參閱failover polltime。

警告：故障轉移消息解密失敗。

錯誤消息：

```
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
```

發生此問題的原因是故障轉移金鑰配置。為了解決此問題，請刪除故障切換金鑰，然後配置新的共用金鑰。

相關資訊

- Cisco ASA 5500系列調適型安全裝置
- Cisco PIX防火牆軟體
- 防火牆服務模組(FWSM)故障轉移配置
- FWSM故障轉移故障排除
- 故障切換在Cisco Secure PIX防火牆上的工作方式
- 技術支援與文件 - Cisco Systems