ASA/PIX:在透明模式下配置主用/備用故障切換

目錄

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/備用故障切換。

注意：在多情景模式下運行的裝置上不支援VPN故障切換。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PIX/ASA 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/備用故障轉移

本節介紹主用/備用故障切換，包括以下主題：

主用/備用故障切換概述

主用/備用故障切換允許您使用備用安全裝置接管故障裝置的功能。當主用裝置發生故障時，它會變為備用狀態，而備用裝置變為主用狀態。變為活動狀態的裝置會假定IP地址，或者，對於透明防火牆，會假定為故障裝置的管理IP地址和MAC地址，並開始傳遞流量。現在處於備用狀態的裝置將接管備用IP地址和MAC地址。由於網路裝置在MAC地址與IP地址配對中沒有看到任何變化，因此ARP條目不會在網路中的任何位置發生變化或超時。

注意：對於多情景模式，安全裝置可以故障轉移整個裝置（包括所有情景），但不能單獨故障轉移單個情景。

主要/輔助狀態和活動/備用狀態

故障轉移對中的兩個裝置之間的主要差異與哪個裝置是主用裝置和哪個裝置是備用裝置有關，即使用哪個IP地址，哪個裝置是主用裝置並主動傳遞流量。

裝置之間存在一些差異，這些差異基於哪個裝置是主裝置（如配置中所指定）和哪個裝置是輔助裝置：

- 如果兩個裝置同時啟動（並且運行狀況相同），則主裝置始終成為主用裝置。
- 主裝置MAC地址始終與活動IP地址耦合。當輔助裝置處於活動狀態且無法通過故障轉移鏈路獲取主MAC地址時，此規則將發生異常。在這種情況下，使用輔助MAC地址。

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。配置始終從主用裝置同步到備用裝置。當備用裝置完成初始啟動時，它將清除其運行配置（與主用裝置通訊所需的故障切換命令除外），主用裝置將其整個配置傳送到備用裝置。

活動單元由以下內容確定：

- 如果裝置啟動並檢測到對等裝置已作為主用裝置運行，它將成為備用裝置。
- 如果裝置啟動但未檢測到對等裝置，則它成為活動裝置。
- 如果兩個裝置同時啟動，則主裝置成為主用裝置，輔助裝置成為備用裝置。

注意：如果輔助裝置啟動並且未檢測到主裝置，它將成為主裝置。它將自己的MAC地址用於活動IP地址。當主裝置可用時，輔助裝置會將MAC地址更改為主裝置的MAC地址，這可能導致網路流量中斷。為了避免這一點，請使用虛擬MAC地址配置故障轉移對。有關詳細資訊，請參閱本文檔的配置主用/備用故障切換部分。

複製啟動時，活動裝置上的安全裝置控制檯會顯示消息`Beginning configuration replication: mate`，並在完成時，安全裝置顯示消息`End Configuration Replication to mate`在複製過程中，在活動

裝置上輸入的命令不能正確複製到備用裝置，在備用裝置上輸入的命令可由從活動裝置上複製的配置覆蓋。在配置複製過程中，請勿在故障切換對中的任一裝置上輸入命令。根據配置的大小，複製可能需要幾秒到幾分鐘。

從輔助裝置中，可以在複製消息從主裝置同步時觀察它：

```
ASA> .

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

ASA>
```

在備用裝置上，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，請輸入以下命令：

- 對於單情景模式，在活動裝置上輸入**copy running-config startup-config**命令。該命令被複製到備用單元，備用單元繼續將其配置寫入快閃記憶體。
- 對於多情景模式，請從系統執行空間以及磁碟上每個情景中的活動裝置上輸入**copy running-config startup-config**命令。該命令被複製到備用單元，備用單元繼續將其配置寫入快閃記憶體。可通過網路從任一裝置訪問外部伺服器上具有啟動配置的情景，無需為每個裝置單獨儲存。或者，您可以將磁碟上的上下文從活動單元複製到外部伺服器，然後將它們複製到備用單元上的磁碟中，在備用單元重新載入時這些上下文可用。

命令複製

命令複製始終從主用裝置流向備用裝置。當在活動裝置上輸入命令時，這些命令將通過故障切換鏈路傳送到備用裝置。您不必將活動配置儲存到快閃記憶體以複製命令。

注意：對備用裝置所做的更改不會複製到主用裝置。如果在備用裝置上輸入命令，則安全裝置將顯示以下消息`**** WARNING **** Configuration Replication is NOT performed from Standby unit to Active unit`配置不再同步。即使輸入了不影響配置的命令，也會顯示此消息。

如果在主用裝置上輸入**write standby**命令，則備用裝置會清除其運行配置（用於與主用裝置通訊的故障切換命令除外），主用裝置會將其整個配置傳送到備用裝置。

對於多情景模式，當您在系統執行空間中輸入**write standby**命令時，所有情景都會被複製。如果在情景中輸入write standby命令，則該命令僅複製情景配置。

複製命令儲存在運行配置中。若要將複製命令儲存到備用裝置上的快閃記憶體中，請輸入以下命令：

- 對於單情景模式，在活動裝置上輸入**copy running-config startup-config**命令。該命令被複製到備用單元，備用單元繼續將其配置寫入快閃記憶體。
- 對於多情景模式，請從系統執行空間在活動裝置上以及磁碟上的每個情景中輸入**copy running-config startup-config**命令。該命令被複製到備用單元，備用單元繼續將其配置寫入快閃記憶體。可通過網路從任一裝置訪問外部伺服器上具有啟動配置的情景，無需為每個裝置單獨儲存。或者，您可以將磁碟上的上下文從活動單元複製到外部伺服器，然後將其複製到備用單元上的磁碟上。

故障轉移觸發器

如果發生以下事件之一，裝置可能會失敗：

- 裝置出現硬體故障或電源故障。
- 裝置出現軟體故障。
- 太多的受監控介面出現故障。
- 在主用裝置上輸入**no failover active**命令，或在備用裝置上輸入**failover active**命令。

故障切換操作

在主用/備用故障切換中，故障切換以裝置為單位。即使是在多情景模式下運行的系統上，也不能對單個或組情景進行故障切換。

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，該表顯示了故障切換策略（故障切換或不故障切換）、活動單元執行的操作、備用單元執行的操作，以及有關故障切換條件和操作的任何特殊說明。該表顯示了故障切換行為。

故障事件	政策	活動操作	備用操作	備註
活動單元出現故障（電源或硬體）	容錯移轉	不適用	啟用；將活動標籤為失敗	任何受監控的介面或故障切換鏈路上均未收到hello消息。
以前的活動單元恢復	無故障切換	成為待命	無操作	無
備用裝置出現故障（電源或硬體）	無故障切換	將待機標籤為失敗	不適用	當備用裝置標籤為發生故障時，主用裝置不會嘗試進行故障轉移，即使已超過介面故障閾值也是如此。
故障切換鏈路在操作過程中失敗	無故障切換	將故障切換介面標籤為發生故障	將故障切換介面標籤為發生故障	您必須儘快恢復故障切換鏈路，因為在故障切換鏈路關閉時，裝置無法故障切換到備用裝置。
故障轉移鏈路在啟動時失敗	無故障切換	將故障切換介面標籤為發生故障	啟用	如果故障切換鏈路在啟動時關閉，則兩台裝置均會變為活動狀態。
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。

活動裝置上的介面故障超過閾值	容錯移轉	將活動標籤為失敗	啟用	無
備用裝置上的介面故障超過閾值	無故障切換	無操作	將待機標籤為失敗	當備用裝置標籤為發生故障時，即使超過介面故障閾值，主用裝置也不會嘗試進行故障轉移。

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
- 狀態容錯移轉

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(僅當防火牆在透明防火牆**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

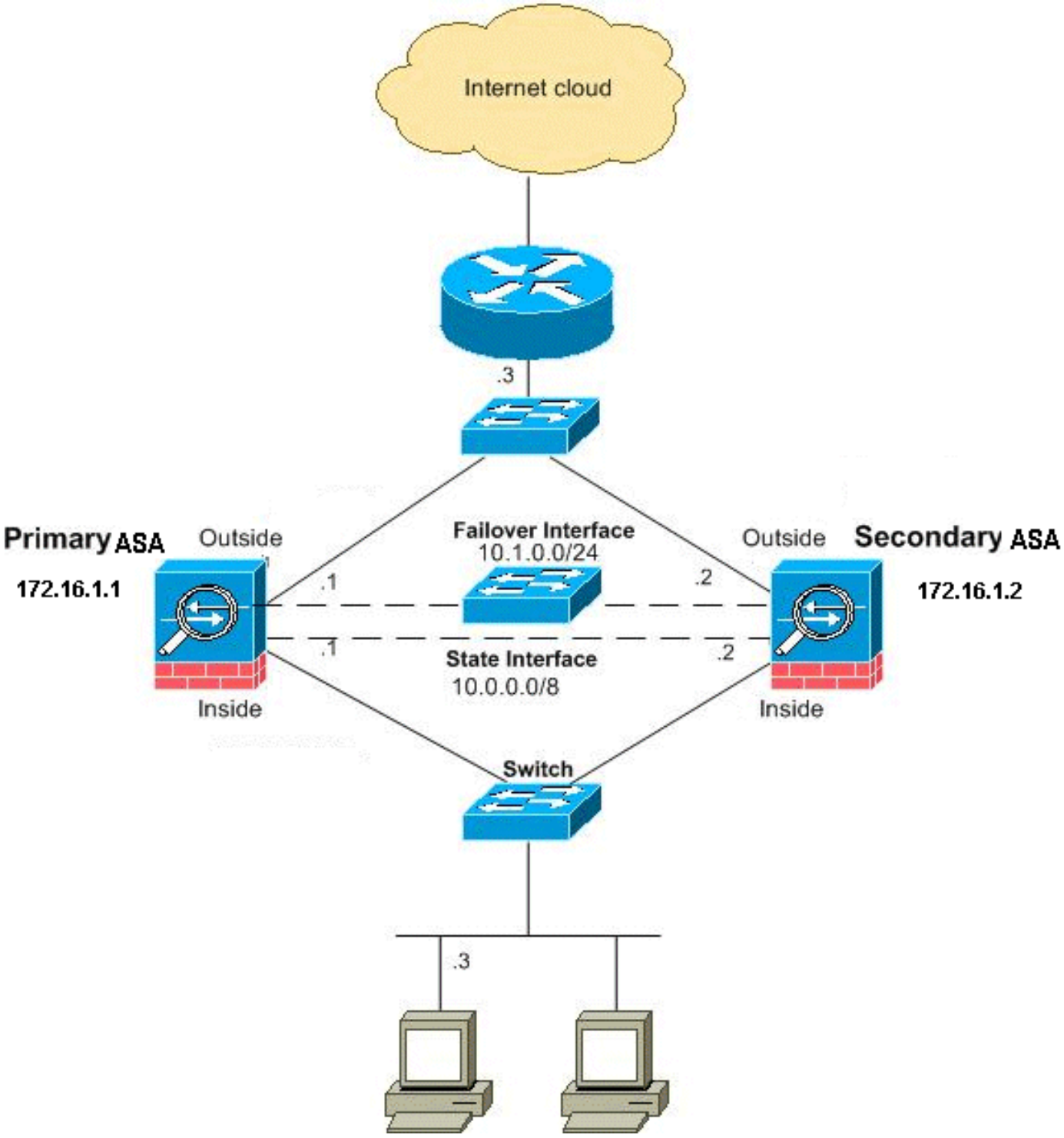
附註： 如果在活動Cisco IP SoftPhone會話中發生故障切換，呼叫將保持活動狀態，因為呼叫會話狀態資訊會複製到備用裝置。當呼叫終止時，IP SoftPhone客戶端將失去與Cisco CallManager的連線。之所以會出現這種情況，是因為備用裝置上沒有CTIQBE掛斷消息的會話資訊。當IP SoftPhone客戶端在某個時間段內未收到來自Cisco CallManager的響應時，它會認為Cisco

CallManager不可達並自行註銷。

基於LAN的主用/備用故障切換配置

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在透明模式下配置主用/備用故障切換。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：如果您從基於電纜的故障切換更改為基於區域網的故障切換，則可以跳過許多步驟，例如為

基於電纜的故障切換配置完成的每個介面分配主用和備用IP地址。

主裝置配置

完成這些步驟，在基於LAN的主用/備用故障切換配置中配置主裝置。這些步驟提供了在主裝置上啟用故障切換所需的最低配置。對於多情景模式，除非另有說明，否則所有步驟都將在系統執行空間中執行。

要在主用/備用故障轉移對中配置主裝置，請完成以下步驟：

1. 如果尚未配置管理介面的活動和備用IP地址（透明模式）。 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。**注意：如**果您使用專用有狀態故障切換介面，請勿為有狀態故障切換鏈路配置IP地址。在後面的步驟中，使用**failover interface ip**命令配置專用有狀態故障切換介面。
   ```
   hostname(config-if)#ip address active_addr netmask
                          standby standby_addr
   ```

   與路由模式（要求每個介面都有一個IP地址）不同，透明防火牆將IP地址分配給整個裝置。安全裝置將此IP地址用作源自安全裝置的資料包（如系統消息或AAA通訊）的源地址。在本示例中，主ASA的IP地址配置如下：
   ```
   hostname(config)#ip address 172.16.1.1 255.255.0.0 standby 172.16.1.2
   ```

   這裡，172.16.1.1用於主裝置，172.16.1.2分配給輔助（備用）裝置。**注意：在**多情景模式下，您必須從每個情景中配置介面地址。使用**changeto context**命令可在上下文之間切換。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。
2. （僅限PIX安全裝置平台）啟用基於LAN的故障切換。
   ```
   hostname(config)#failover lan enable
   ```

3. 將該單位指定為主要單位。
   ```
   hostname(config)#failover lan unit primary
   ```

4. 定義故障切換介面。指定要用作故障轉移介面的介面。
   ```
   hostname(config)#failover lan interface if_name phy_if
   ```

   在本文檔中，「failover」（乙太網介面0的介面名稱）用於故障切換介面。
   ```
   hostname(config)#failover lan interface failover Ethernet3
   ```

   *if_name*引數為由*phy_if*引數指定的介面指定一個名稱。*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）。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
   ```

   在本文檔中，為了配置故障切換鏈路，10.1.0.1用於主用裝置，10.1.0.2用於備用裝置，而「failover」是Ethernet0的介面名稱。
   ```
   hostname(config)#failover interface ip failover 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。故障切換鏈路的主用IP地址始終位於主裝置上，而備用IP地址始終位於輔助裝置上。啟用介面
   ```
   hostname(config)#interface phy_if
   ```

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

在本示例中，Ethernet3用於故障切換：

```
hostname(config)#interface ethernet3

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

5. （可選）要啟用狀態故障切換，請配置狀態故障切換鏈路。指定要用作有狀態故障切換鏈路的介面。

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

此示例使用「state」作為Ethernet2的介面名稱來交換故障切換鏈路狀態資訊：

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

注意：如果狀態故障切換鏈路使用故障切換鏈路或資料介面，則只需提供*if_name*參數。*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）。此介面不得用於任何其他目的，但可選擇用作故障切換鏈路。為有狀態故障切換鏈路分配一個活動和備用IP地址。**注意：如**果有狀態故障切換鏈路使用故障切換鏈路或資料介面，請跳過此步驟。您已經定義了介面的活動和備用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用作活動地址，10.0.0.2用作有狀態故障切換鏈路的備用IP地址。

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

備用IP地址必須與活動IP地址位於同一子網中。您無需標識備用地址子網掩碼。有狀態故障切換鏈路IP地址和MAC地址不會在故障切換時更改，除非它們使用資料介面。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。啟用介面。**注意：如**果有狀態故障切換鏈路使用故障切換鏈路或資料介面，請跳過此步驟。您已啟用該介面。

```
hostname(config)#interface phy_if

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

注意：例如，在此場景中，Ethernet2用於有狀態故障切換鏈路：

```
hostname(config)#interface ethernet2

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

6. 啟用故障轉移。

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

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。

7. 將系統配置儲存到快閃記憶體。

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

輔助裝置配置

輔助裝置上需要的唯一配置是故障切換介面。輔助裝置需要這些命令來最初與主裝置通訊。主裝置將其配置傳送到輔助裝置後，兩種配置之間的唯一永久差異是**failover lan unit**命令，該命令將每台裝置標識為主裝置或輔助裝置。

對於多情景模式，除非另有說明，否則所有步驟都將在系統執行空間中執行。

要配置輔助裝置，請完成以下步驟：

1. （僅限PIX安全裝置平台）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
   ```

   在本文檔中，Ethernet0用於LAN故障切換介面。
   ```
   hostname(config)#failover lan interface failover Ethernet3
   ```

   *if_name*引數為*phy_*if引數指定的介面指定名稱。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
   ```

   在本文檔中，為了配置故障切換鏈路，10.1.0.1用於主用裝置，10.1.0.2用於備用裝置，而「failover」是Ethernet0的介面名稱。
   ```
   hostname(config)#failover interface ip failover 10.1.0.1
                         255.255.255.0 standby 10.1.0.2
   ```

   注意：輸入此命令與您在主裝置上配置故障切換介面時輸入該命令完全相同。啟用介面。
   ```
   hostname(config)#interface phy_if

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

   例如，在此案例中，Ethernet0用於故障切換。
   ```
   hostname(config)#interface ethernet3

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

3. （可選）將此單位指定為輔助單位。
   ```
   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，除非事先進行了配置。
4. 啟用故障轉移。
   ```
   hostname(config)#failover
   ```

   注意：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*顯示在活動裝置控制檯上。
5. 運行配置完成複製後，將配置儲存到快閃記憶體。
   ```
   hostname(config)#copy running-config startup-config
   ```

組態

本檔案會使用以下設定：

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
```

輔助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
```

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#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
```

輔助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 命令驗證狀態。

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
```

輔助裝置

```
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
```

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

主裝置

```
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
```

輔助裝置

```
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
```

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**。

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
```

輔助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
```

註：如果不輸入故障切換IP地址，則**show failover**命令會顯示IP地址的0.0.0.0，並且介面監控仍保持等待*狀*態。請參閱*思科安全裝置命令參考7.2版*中的show failover部分，瞭解有關不同故障切換狀態的詳細資訊。

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），以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/備用故障轉移，請在主用裝置上輸入以下命令：
   ```
   hostname(config)#no failover active
   ```
3. 使用FTP在相同的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/備用故障轉移，請在主用裝置上輸入以下命令：
   ```
   hostname(config)#failover active
   ```

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：

在備用裝置上輸入以下命令：

```
hostname#failover active
```

在活動裝置上輸入以下命令：

```
hostname#no 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

要將故障裝置恢復為未故障狀態，請輸入以下命令：

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

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，並且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。本節包含以下主題

- 故障轉移監控
- 裝置故障
- %ASA-3-210005:LU分配連線失敗
- 故障切換系統消息
- 調試消息
- SNMP
- 已知的問題

故障轉移監控

此示例演示當故障切換尚未啟動以監控網路介面時會發生的情況。故障切換不會開始監控網路介面，直到它收到來自該介面上另一裝置的第二個hello資料包。大約需要30秒。如果裝置連線到執行跨距樹狀目錄通訊協定(STP)的網路交換器，則需要兩倍於交換器上設定的時間（通常設定為15秒），加上此30秒延遲。這是因為在ASA啟動時和故障轉移事件後立即檢測到臨時網橋環路。檢測到此環路後，它會在轉發延遲時間停止在這些介面包包。然後進入listen模式，等待額外的時間，在此時間內，交換機偵聽橋接器環路，但不會轉發流量或轉發故障轉移hello資料包。經過兩次轉發延遲時間（30秒）後，流量將恢復。每個ASA都保持等待，直到它收到來自另一裝置的30的hello資料包。在ASA傳遞流量的時間內，它不會因為未聽到hello資料包而導致其它裝置故障。所有其他故障切換監控仍會發生，即電源、鏈路介面丟失和故障切換電纜hello。

對於故障切換，思科強烈建議客戶在連線到ASA介面的所有交換機埠上啟用portfast。此外，必須在這些埠上禁用通道化和中繼。如果ASA的介面在故障切換過程中關閉，則當埠從偵聽狀態轉換到學

習狀態到轉發狀態時，交換機不必等待30秒。

```
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)
```

總而言之，請檢查以下步驟，以縮小故障切換問題的範圍：

- 檢查連線到介面的網路電纜是否處於等待/故障狀態，如果可能，請更換這些電纜。
- 如果兩台裝置之間連線有交換機，請驗證連線到處於等待/失敗狀態的介面的網路是否正常工作。
- 檢查連線到處於等待/失敗狀態的介面的交換機埠，如果可能，使用交換機上的另一個FE埠。
- 檢查是否已快速啟用連線埠，並停用連線到介面的交換器連線埠上的主幹和通道化。

裝置故障

在本示例中，故障切換檢測到故障。請注意，主裝置上的介面1是故障的來源。由於故障，裝置已重新處於模式。故障裝置已從網路中自行刪除（介面關閉），並且不再在網路上傳送`hello`資料包。在更換故障裝置並再次啟動故障切換通訊之前，主用裝置一直處於`waiting`狀態。

```
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分配連線失敗

如果收到以下錯誤消息，則可能存在記憶體問題：

```
LU
```

此問題已記錄在Cisco錯誤ID CSCte80027(僅限註冊客戶)。 若要解決此問題，請將防火牆升級為修正此錯誤的軟體版本。修正此錯誤的一些ASA軟體版本為8.2(4)、8.3(2)和8.4(2)。

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。

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。

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使用**failover polltime**命令。

`failover polltime unit msec [time]`輪詢hello消息以表示時間間隔，以便檢查備用單元的存在。

同樣，`failover holdtime unit msec [time]`表示設定一個時間段，在該時間段內，裝置必須在故障轉移鏈路上接收hello消息，在此時間段後，對等裝置會宣告出現故障。

要在主用/備用故障切換配置中指定資料介面輪詢和保持時間，請在全域性配置模式下使用**failover polltime interface**命令。若要恢復預設輪詢和保持時間，請使用此命令的**no**形式。

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

使用**failover polltime interface**命令更改在資料介面上傳送hello資料包的頻率。此命令僅適用於主用/備用故障切換。對於主用/主用故障切換，請在故障切換組配置模式下使用**polltime interface**命令，而不是**failover polltime interface**命令。

不能輸入小於介面輪詢時間5倍的*holdtime*值。藉助更快的輪詢時間，安全裝置可以更快地檢測故障並觸發故障切換。但是，在網路臨時擁塞時，更快的檢測會導致不必要的切換。當超過一半的保持時間在介面上未聽到hello資料包時，介面測試開始。

您可以在配置中包括failover polltime unit和failover polltime interface命令。

此示例將介面輪詢時間頻率設定為500毫秒，將保持時間設定為5秒：

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

有關詳細資訊，請參閱*思科安全裝置命令參考7.2版*中的failover polltime部分。

匯出故障轉移配置中的證書/私鑰

主裝置自動將私鑰/證書複製到輔助裝置。在作用中裝置發出**write memory**指令，將組態（包括憑證/私人金鑰）複製到備用裝置。備用裝置上的所有金鑰/證書都將被主用裝置配置清除並重新填充。

注意：不能手動從活動裝置匯入證書、金鑰和信任點，然後匯出到備用裝置。

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。

問題：配置透明主用/備用多模式故障切換後，故障切換始終處於擺動狀態

當兩個ASA的內部介面直接連線且兩個ASA的外部介面都直接連線時，故障轉移是穩定的。但是，當交換機在中之間使用時，故障切換將搖擺。

解決方案：在ASA介面上禁用BPDU以解決此問題。

ASA模組故障轉移

如果在主用和備用單元中使用高級檢測和防禦安全服務模組(AIP-SSM)或內容安全和控制安全服務模組(CSC-SSM)，則在故障轉移方面，它將獨立於ASA運行。**必須在主用和備用裝置中手動配置模組，故障切換不會複製模組配置。**

在故障切換方面，具有AIP-SSM或CSC-SSM模組的兩個ASA裝置必須屬於同一硬體型別。例如，如果主裝置具有ASA-SSM-10模組，則輔助裝置必須具有ASA-SSM-10模組。

故障轉移消息塊分配失敗

錯誤消息 `%PIX|ASA-3-105010:`

說明:塊記憶體已耗盡。這是一個臨時消息，安全裝置應進行恢復。主裝置也可以列為輔助裝置。

建議的操作：使用**show blocks**命令以監控目前的區塊記憶體。

AIP模組故障轉移問題

如果您有兩個ASA處於故障切換配置中，並且每個都有一個AIP-SSM，則必須手動複製AIP-SSM的配置。故障切換機制只複製ASA的配置。故障切換中不包括AIP-SSM。

首先，AIP-SSM在故障轉移方面獨立於ASA運行。對於故障切換，從ASA的角度來看，只需要確保AIP模組具有相同的硬體型別。除此之外，與故障切換的任何其他部分一樣，活動與備用之間的ASA配置必須同步。

對於AIP的設定，它們實際上是獨立的感測器。兩者之間沒有故障切換，而且它們彼此沒有意識。它們可以運行獨立版本的代碼。也就是說，它們不必匹配，並且ASA不關心AIP上與故障切換相關的代碼版本。

ASDM通過您在AIP上配置的管理介面IP啟動與AIP的連線。換句話說，它通常通過HTTPS連線到感測器，這取決於您如何設定感測器。

您可以讓ASA進行獨立於IPS(AIP)模組的故障切換。您仍連線到同一個，因為您已連線到其管理IP。要連線到另一個AIP，您必須重新連線到其管理IP以配置並訪問它。

請參閱ASA:將網路流量從ASA傳送到AIP SSM配置示例，瞭解有關如何將通過Cisco ASA 5500系列自適應安全裝置(ASA)的網路流量傳送到高級檢測和防禦安全服務模組(AIP-SSM)(IPS)的更多資訊和配置示例

已知的問題

當您嘗試使用版本8.x軟體和ASDM 6.x版進行故障切換配置的輔助ASA上訪問ASDM時，收到以下錯誤：

在證書中，頒發者和使用者名稱是活動單元的IP地址，*而*不是備用單元的*IP地*址。

在ASA 8.x版中，內部(ASDM)證書從活動裝置複製到備用裝置，這會導致錯誤消息。但是，如果相同的防火牆在版本7.x代碼上運行並使用5.x ASDM，而您嘗試訪問ASDM，則會收到此常規安全警告：

檢查證書時，頒發者和使用者名稱是備用裝置的IP地址。

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