ASA/PIX: Aktiv/Standby-Failover im transparenten Modus konfigurieren

Inhalt

Einführung

Für die Failover-Konfiguration sind zwei identische Security Appliances erforderlich, die über eine dedizierte Failover-Verbindung und optional über eine Stateful Failover-Verbindung miteinander verbunden sind. Der Zustand der aktiven Schnittstellen und Einheiten wird überwacht, um festzustellen, ob bestimmte Failover-Bedingungen erfüllt sind. Wenn diese Bedingungen erfüllt sind, tritt ein Failover auf.

Die Sicherheits-Appliance unterstützt zwei Failover-Konfigurationen:

- Aktiv/Aktiv-Failover
- Aktiv/Standby-Failover

Für jede Failover-Konfiguration gibt es eine eigene Methode zum Bestimmen und Ausführen von Failover. Mit Active/Active Failover können beide Einheiten den Netzwerkverkehr weiterleiten. So können Sie den Lastenausgleich in Ihrem Netzwerk konfigurieren. Active/Active Failover ist nur auf Einheiten verfügbar, die im Multiple-Context-Modus ausgeführt werden. Bei einem Aktiv/Standby-Failover leitet nur ein Gerät den Datenverkehr weiter, während das andere Gerät im Standby-Modus wartet. Aktiv/Standby-Failover ist für Geräte verfügbar, die im Single- oder Multiple-Context-Modus ausgeführt werden. Beide Failover-Konfigurationen unterstützen Stateful- oder Stateless (reguläres Failover).

Eine transparente Firewall ist eine Layer-2-Firewall, die wie ein *Bump im Kabel* oder eine *versteckte Firewall* funktioniert und nicht als Router-Hop auf verbundene Geräte angesehen wird. Die Sicherheits-Appliance verbindet dasselbe Netzwerk mit den internen und externen Ports. Da die Firewall kein gerouteter Hop ist, können Sie problemlos eine transparente Firewall in ein bestehendes Netzwerk einführen. Es ist nicht erforderlich, IP erneut zu komprimieren. Sie können die Adaptive Security Appliance so einstellen, dass sie im standardmäßigen Routing-Firewall-Modus oder im transparenten Firewall-Modus ausgeführt wird. Wenn Sie den Modus ändern, löscht die Adaptive Security Appliance die Konfiguration, da viele Befehle in beiden Modi nicht unterstützt werden. Wenn Sie bereits über eine ausgefüllte Konfiguration verfügen, sichern Sie diese Konfiguration, bevor Sie den Modus ändern. Sie können diese Sicherungskonfiguration als Referenz verwenden, wenn Sie eine neue Konfiguration erstellen. Weitere Informationen zur Konfiguration der Firewall-Appliance im transparenten Modus finden Sie im Konfigurationsbeispiel für eine transparente Firewall.

In diesem Dokument wird erläutert, wie ein Aktiv/Standby-Failover im transparenten Modus auf der ASA Security Appliance konfiguriert wird.

Hinweis: VPN-Failover wird bei Einheiten, die im Multiple-Context-Modus ausgeführt werden, nicht

unterstützt. VPN-Failover ist nur für **Active/Standby-Failover-**Konfigurationen verfügbar.

Cisco empfiehlt, die Verwaltungsschnittstelle nicht für Failover zu verwenden, insbesondere nicht für Stateful Failover, bei dem die Sicherheits-Appliance die Verbindungsinformationen kontinuierlich von einer Sicherheitslösung zur anderen sendet. Die Failover-Schnittstelle muss mindestens die gleiche Kapazität wie die Schnittstellen aufweisen, die regulären Datenverkehr weiterleiten. Während die Schnittstellen auf der ASA 5540 Gigabit sind, ist die Management-Schnittstelle nur FastEthernet. Die Management-Schnittstelle ist nur für den Management-Datenverkehr vorgesehen und als management0/0 festgelegt. Sie können jedoch den Befehl **nur für die Verwaltung** verwenden, um jede Schnittstelle als Nur-Management-Schnittstelle zu konfigurieren. Für Management 0/0 können Sie auch den Nur-Management-Modus deaktivieren, sodass die Schnittstelle wie jede andere Schnittstelle Datenverkehr durchlaufen kann. Weitere Informationen zum **Befehl** "Nur **Verwaltung**" finden Sie unter Cisco Security Appliance Command Reference, Version 8.0.

Dieser Konfigurationsleitfaden enthält eine Beispielkonfiguration mit einer kurzen Einführung in die PIX/ASA 7.x Active/Standby-Technologie. Im ASA/PIX-Befehlsreferenz finden Sie weitere Informationen zur Theorie, die dieser Technologie zugrunde liegt.

Voraussetzungen

Anforderungen

Hardware-Anforderungen

Die Hardwarekonfiguration der beiden Einheiten in einer Failover-Konfiguration muss identisch sein. Sie müssen das gleiche Modell und dieselbe Anzahl an Schnittstellen und dieselbe Anzahl an RAM-Modulen aufweisen.

Hinweis: Die beiden Einheiten müssen nicht denselben Flash-Speicher haben. Wenn Sie Einheiten mit unterschiedlichen Flash-Speichergrößen in Ihrer Failover-Konfiguration verwenden, sollten Sie sicherstellen, dass das Gerät mit dem kleineren Flash-Speicher über genügend Speicherplatz verfügt, um die Software-Image-Dateien und die Konfigurationsdateien aufnehmen zu können. Ist dies nicht der Fall, schlägt die Synchronisierung der Konfiguration vom Gerät mit dem größeren Flash-Speicher zum Gerät mit dem kleineren Flash-Speicher fehl.

Softwareanforderungen

Die beiden Einheiten in einer Failover-Konfiguration müssen im Betriebsmodus (geroutet oder transparent, ein oder mehrere Kontexte) sein. Sie müssen über dieselbe Haupt- (Erste-) und Nebenversion (zweite Nummer) verfügen, Sie können jedoch im Rahmen eines Upgrade-Prozesses verschiedene Versionen der Software verwenden. Sie können beispielsweise eine Einheit von Version 7.0(1) auf Version 7.0(2) aktualisieren und verfügen über ein aktives Failover. Cisco empfiehlt, beide Einheiten auf die gleiche Version zu aktualisieren, um eine langfristige Kompatibilität zu gewährleisten.

Weitere Informationen zum Aktualisieren der Software auf einem Failover-Paar finden Sie im Abschnitt Durchführen von Upgrades ohne Ausfallzeiten für Failover-Paare im *Cisco Security Appliance Command Line Configuration Guide, Version 8.0*.

Lizenzanforderungen

Auf der ASA Security Appliance-Plattform muss mindestens eine Einheit über eine **uneingeschränkte (UR)-Lizenz** verfügen.

Hinweis: Möglicherweise müssen die Lizenzen für ein Failover-Paar aktualisiert werden, um zusätzliche Funktionen und Vorteile zu erhalten. Weitere Informationen finden Sie unter Lizenzschlüssel-Upgrade auf einem Failover-Paar.

Hinweis: Die lizenzierten Funktionen (z. B. SSL VPN-Peers oder Sicherheitskontexte) auf beiden an der Ausfallsicherung beteiligten Security Appliances müssen identisch sein.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- ASA Security Appliance ab Version 7.x

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Zugehörige Produkte

Diese Konfiguration kann auch mit den folgenden Hardware- und Softwareversionen verwendet werden:

- PIX Security Appliance ab Version 7.x

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Aktiv/Standby-Failover

In diesem Abschnitt wird Active/Standby-Failover beschrieben. Dabei werden folgende Themen behandelt:

- Aktiv/Standby-Failover - Übersicht
- Primär-/Sekundär- und Aktiv-/Standby-Status
- Geräteinitialisierung und Konfigurationssynchronisierung
- Befehlsreplikation
- Failover-Trigger
- Failover-Aktionen

Aktiv/Standby-Failover - Übersicht

Mit Active/Standby-Failover können Sie die Funktionen einer ausgefallenen Einheit mithilfe einer Standby-Sicherheits-Appliance übernehmen. Wenn das aktive Gerät ausfällt, wechselt es in den

Standby-Status, während das Standby-Gerät in den aktiven Status wechselt. Die aktive Einheit übernimmt die IP-Adressen oder, bei einer transparenten Firewall, die Management-IP-Adresse und die MAC-Adressen der ausgefallenen Einheit und beginnt mit der Weiterleitung des Datenverkehrs. Das Gerät, das sich jetzt im Standby-Modus befindet, übernimmt die Standby-IP-Adressen und -MAC-Adressen. Da die MAC-IP-Adressenpaarung für Netzwerkgeräte unverändert bleibt, werden im Netzwerk keine ARP-Einträge geändert oder die Zeitüberschreitung wurde verhindert.

Hinweis: Im Multiple-Context-Modus kann die Sicherheits-Appliance über die gesamte Einheit (einschließlich aller Kontexte) ausfallen, jedoch nicht über einzelne Kontexte hinweg ausfallen.

Primär-/Sekundär- und Aktiv-/Standby-Status

Die Hauptunterschiede zwischen den beiden Einheiten in einem Failover-Paar hängen davon ab, welches Gerät aktiv ist und welches Gerät im Standby-Modus ist, d. h. welche IP-Adressen verwendet werden sollen und welches Gerät der primäre ist und den Datenverkehr aktiv weiterleitet.

Es gibt einige Unterschiede zwischen den Einheiten, die, wie in der Konfiguration angegeben, auf der primären Einheit und auf der sekundären Einheit basieren:

- Die Primäreinheit wird immer dann zur aktiven Einheit, wenn beide Einheiten gleichzeitig hochfahren (und die Betriebsfähigkeit der Geräte gleich ist).
- Die MAC-Adresse der primären Einheit wird immer mit den aktiven IP-Adressen gekoppelt. Die Ausnahme zu dieser Regel tritt auf, wenn die Sekundäreinheit aktiv ist und die primäre MAC-Adresse nicht über die Failover-Verbindung abgerufen werden kann. In diesem Fall wird die sekundäre MAC-Adresse verwendet.

Geräteinitialisierung und Konfigurationssynchronisierung

Die Konfigurations-Synchronisierung erfolgt, wenn ein oder beide Geräte im Failover-Paar gestartet werden. Konfigurationen werden immer vom aktiven Gerät zum Standby-Gerät synchronisiert. Wenn die Standby-Einheit ihren ersten Start abgeschlossen hat, löscht sie ihre laufende Konfiguration, mit Ausnahme der für die Kommunikation mit der aktiven Einheit erforderlichen Failover-Befehle, und die aktive Einheit sendet ihre gesamte Konfiguration an die Standby-Einheit.

Die aktive Einheit wird wie folgt bestimmt:

- Wenn ein Gerät startet und erkennt, dass ein Peer bereits aktiv ist, wird es zur Standby-Einheit.
- Wenn ein Gerät bootet und keinen Peer erkennt, wird es zur aktiven Einheit.
- Wenn beide Geräte gleichzeitig booten, wird die primäre Einheit zur aktiven Einheit, und die sekundäre Einheit wird zur Standby-Einheit.

Hinweis: Wenn die Sekundäreinheit startet und die Primäreinheit nicht erkennt, wird sie zur aktiven Einheit. Es verwendet eigene MAC-Adressen für die aktiven IP-Adressen. Sobald die Primäreinheit verfügbar ist, ändert die Sekundäreinheit die MAC-Adressen in die Adressen der Primäreinheit, wodurch der Netzwerkverkehr unterbrochen werden kann. Um dies zu vermeiden, konfigurieren Sie das Failover-Paar mit virtuellen MAC-Adressen. Weitere Informationen finden Sie im Abschnitt Konfigurieren von Aktiv/Standby-Failover in diesem Dokument.

Wenn die Replikation gestartet wird, wird in der Security Appliance-Konsole der aktiven Einheit die Meldung `beginnende Konfigurationsreplikation` angezeigt: `Sending to mate`, und wenn es abgeschlossen ist, zeigt die Sicherheits-Appliance die Meldung `End Configuration Replication to mate an.` Innerhalb der Replikation können auf der aktiven Einheit eingegebene Befehle nicht ordnungsgemäß auf die Standby-Einheit repliziert werden. Außerdem können auf der Standby-Einheit eingegebene Befehle von der Konfiguration überschrieben werden, die von der aktiven Einheit repliziert wird. Geben Sie keine Befehle auf einer der Komponenten im Failover-Paar im Rahmen des Konfigurationsreplikationsprozesses ein. Abhängig von der Größe der Konfiguration kann die Replikation einige Sekunden bis mehrere Minuten dauern.

Von der Sekundäreinheit aus können Sie die Replikationsmeldung beim Synchronisieren von der Primäreinheit beobachten:

```
ASA> .

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

ASA>
```

Auf der Standby-Einheit existiert die Konfiguration nur im laufenden Speicher. Geben Sie die folgenden Befehle ein, um die Konfiguration nach der Synchronisierung im Flash-Speicher zu speichern:

- Geben Sie im Einzelkontextmodus den Befehl **copy running-config startup-config** auf der aktiven Einheit ein. Der Befehl wird auf die Standby-Einheit repliziert, die dann die Konfiguration in den Flash-Speicher schreibt.
- Geben Sie im Multiple-Context-Modus den Befehl **copy running-config startup-config** auf der aktiven Einheit aus dem Systemausführungsspeicherplatz und in jedem Kontext auf der Festplatte ein. Der Befehl wird auf die Standby-Einheit repliziert, die dann die Konfiguration in den Flash-Speicher schreibt. Kontexte mit Startkonfigurationen auf externen Servern sind von beiden Einheiten über das Netzwerk zugänglich und müssen nicht für jede Einheit separat gespeichert werden. Alternativ können Sie die Kontexte auf der Festplatte von der aktiven Einheit auf einen externen Server kopieren und sie anschließend auf die Festplatte des Standby-Geräts kopieren, wo sie verfügbar werden, wenn das Gerät neu geladen wird.

Befehlsreplikation

Die Befehlsreplikation verläuft immer vom aktiven zum Standby-Gerät. Wenn Befehle auf der aktiven Einheit eingegeben werden, werden sie über die Failover-Verbindung an die Standby-Einheit gesendet. Sie müssen die aktive Konfiguration nicht im Flash-Speicher speichern, um die Befehle zu replizieren.

Hinweis: Änderungen am Standby-Gerät werden nicht auf die aktive Einheit repliziert. Wenn Sie einen Befehl auf der Standby-Einheit eingeben, zeigt die Sicherheits-Appliance die Meldung `*** WARNING **** Konfigurationsreplikation NICHT von der Standby-Einheit zur aktiven Einheit durchgeführt.` Konfigurationen sind nicht mehr synchronisiert. Diese Meldung wird auch angezeigt, wenn Sie Befehle eingeben, die sich nicht auf die Konfiguration auswirken.

Wenn Sie den Befehl **write standby** (**Write Standby**) auf der aktiven Einheit eingeben, löscht die Standby-Einheit die aktuelle Konfiguration, mit Ausnahme der für die Kommunikation mit der

aktiven Einheit verwendeten Failover-Befehle, und die aktive Einheit sendet die gesamte Konfiguration an die Standby-Einheit.

Wenn Sie im Systemausführungsbereich den **Write Standby-**Befehl eingeben, werden alle Kontexte repliziert. Wenn Sie den Write Standby-Befehl in einem Kontext eingeben, repliziert der Befehl nur die Kontextinformationen.

Replizierte Befehle werden in der aktuellen Konfiguration gespeichert. Geben Sie die folgenden Befehle ein, um die replizierten Befehle im Flash-Speicher der Standby-Einheit zu speichern:

- Geben Sie im Einzelkontextmodus den Befehl **copy running-config startup-config** auf der aktiven Einheit ein. Der Befehl wird auf die Standby-Einheit repliziert, die dann die Konfiguration in den Flash-Speicher schreibt.
- Geben Sie im Multiple-Context-Modus den Befehl **copy running-config startup-config** auf der aktiven Einheit aus dem Systemausführungsspeicherplatz und in jedem Kontext auf der Festplatte ein. Der Befehl wird auf die Standby-Einheit repliziert, die dann die Konfiguration in den Flash-Speicher schreibt. Kontexte mit Startkonfigurationen auf externen Servern sind von beiden Einheiten über das Netzwerk zugänglich und müssen nicht für jede Einheit separat gespeichert werden. Alternativ können Sie die Kontexte auf der Festplatte von der aktiven Einheit auf einen externen Server kopieren und dann auf die Festplatte der Standby-Einheit kopieren.

Failover-Trigger

Das Gerät kann ausfallen, wenn eines der folgenden Ereignisse eintritt:

- Die Einheit weist einen Hardwarefehler oder einen Stromausfall auf.
- Bei der Einheit tritt ein Softwarefehler auf.
- Zu viele überwachte Schnittstellen schlagen fehl.
- Der Befehl **no failover active** wird auf der aktiven Einheit eingegeben, oder der Befehl **failover active** wird auf der Standby-Einheit eingegeben.

Failover-Aktionen

Bei einem Aktiv/Standby-Failover erfolgt das Failover auf Gerätebasis. Selbst bei Systemen, die im Mehrfachkontextmodus ausgeführt werden, können Sie keine Failover-Vorgänge für einzelne oder Gruppen von Kontexten durchführen.

Diese Tabelle zeigt die Failover-Aktion für jedes Fehlerereignis. Für jedes Fehlerereignis werden in der Tabelle die Failover-Richtlinie (Failover oder kein Failover), die von der aktiven Einheit durchgeführten Aktionen, die vom Standby-Gerät durchgeführten Aktionen und spezielle Hinweise zum Failover-Zustand und zu den entsprechenden Aktionen aufgeführt. Die Tabelle zeigt das Failover-Verhalten.

Fehlerereignis	Richtlinie	Aktive Aktion	Standby-Aktion	Hinweise
Aktive Einheit ausgefallen (Stromversor	Failover	K/A	Werden Sie aktiv; markieren aktiv als	An einer überwachten Schnittstell

gung oder Hardware)			fehlgeschlagen	e oder der Failover-Verbindung werden keine Hello-Nachrichten empfangen.
Früher aktive Gerätewiederherstellung	Kein Failover	Werden Sie Standby	Keine Aktion	Keine
Standby-Einheit ausgefallen (Stromversorgung oder Hardware)	Kein Failover	Mark Standby als fehlgeschlagen	K/A	Wenn die Standby-Einheit als ausgefallen gekennzeichnet ist, versucht die aktive Einheit nicht, ein Failover durchzuführen, selbst wenn der Grenzwert für Schnittstellenausfälle überschritten wird.
Failover-Verbindung ist in Betrieb	Kein Failover	Markierung der Failover-Schnittstelle als fehlgeschlagen	Markierung der Failover-Schnittstelle als fehlgeschlagen	Sie müssen die Failover-Verbindung so schnell wie möglich wiederherstellen, da das Gerät bei Ausfall der Failover-Verbindung nicht auf die Standby-

				Einheit umschalten kann.
Failover-Verbindung ist beim Start fehlgeschlagen	Kein Failover	Markierung der Failover-Schnittstelle als fehlgeschlagen	Aktiv werden	Wenn die Failover-Verbindung beim Start nicht verfügbar ist, werden beide Einheiten aktiv.
Stateful Failover Link fehlgeschlagen	Kein Failover	Keine Aktion	Keine Aktion	Statusinformationen sind veraltet, und Sitzungen werden beendet, wenn ein Failover auftritt.
Schnittstellenausfall bei aktiver Einheit oberhalb des Grenzwerts	Failover	Aktiv als fehlgeschlagen markieren	Aktiv werden	Keine
Schnittstellenausfall im Standby-Gerät oberhalb des Grenzwerts	Kein Failover	Keine Aktion	Mark Standby als fehlgeschlagen	Wenn das Standby-Gerät als ausgefallen gekennzeichnet ist, versucht das aktive Gerät nicht, einen Failover durchzuführen, selbst wenn der Grenzwert für Schnittstellenausfälle überschritten wurde.

Reguläres und Stateful Failover

Die Sicherheits-Appliance unterstützt zwei Arten von Failover: regulär und Stateful. Dieser Abschnitt behandelt folgende Themen:

Reguläres Failover

Wenn ein Failover auftritt, werden alle aktiven Verbindungen verworfen. Clients müssen Verbindungen wiederherstellen, wenn die neue aktive Einheit die Kontrolle übernimmt.

Stateful Failover

Wenn Stateful Failover aktiviert ist, leitet die aktive Einheit kontinuierlich Informationen zum Verbindungsstatus an die Standby-Einheit weiter. Nach einem Failover stehen die gleichen Verbindungsinformationen auf der neuen aktiven Einheit zur Verfügung. Unterstützte Endbenutzeranwendungen müssen nicht erneut verbunden werden, um dieselbe Kommunikationssitzung zu behalten.

Folgende Statusinformationen werden an den Standby-Switch weitergeleitet:

- Die NAT-Übersetzungstabelle
- Die TCP-Verbindungsstatus
- UDP-Verbindungsstatus
- Die ARP-Tabelle
- Die Layer 2 Bridge-Tabelle (nur wenn die Firewall im **transparenten Firewall-**Modus ausgeführt wird)
- HTTP-Verbindungsstatus (wenn HTTP-Replikation aktiviert ist)
- Die Tabelle ISAKMP und IPSec SA
- Die GTP PDP-Verbindungsdatenbank

Folgende Informationen werden bei Aktivierung des Stateful Failover nicht an die Standby-Einheit weitergeleitet:

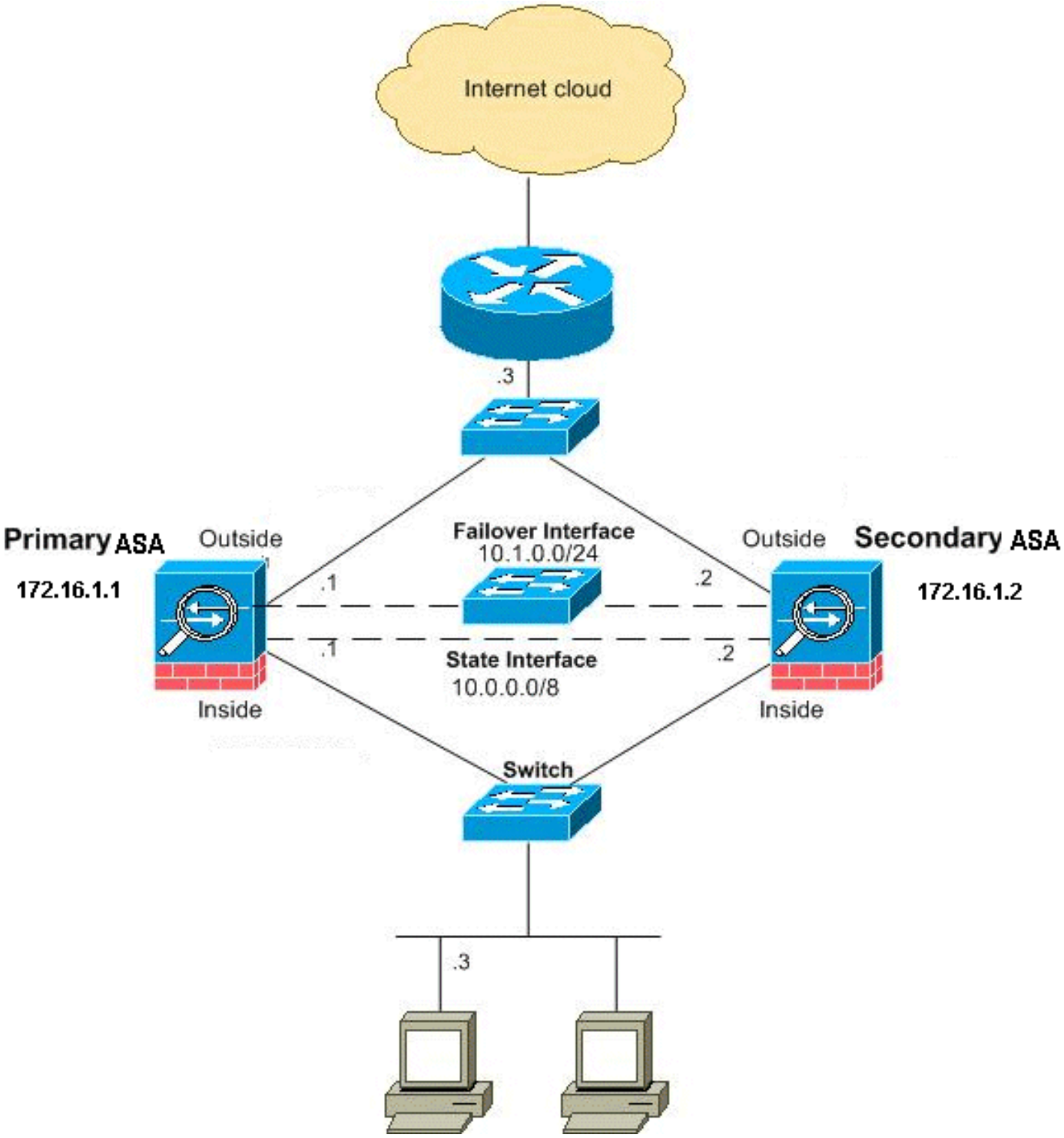
- Die HTTP-Verbindungstabelle (sofern die HTTP-Replikation nicht aktiviert ist)
- Die Benutzerauthentifizierungstabelle (uauth)
- Die Routing-Tabellen
- Statusinformationen zu Sicherheitsdienstmodulen

Hinweis: Wenn innerhalb einer aktiven Cisco IP SoftPhone-Sitzung ein Failover erfolgt, bleibt der Anruf aktiv, da die Informationen zum Anrufsitzungsstatus auf die Standby-Einheit repliziert werden. Wenn der Anruf beendet wird, verliert der IP SoftPhone-Client die Verbindung mit dem Cisco CallManager. Dies liegt daran, dass auf der Standby-Einheit keine Sitzungsinformationen für die CTIQBE-Abbruchmeldung vorliegen. Wenn der IP SoftPhone-Client innerhalb eines bestimmten Zeitraums keine Antwort vom Cisco CallManager erhält, wird der Cisco CallManager als nicht erreichbar betrachtet und die Registrierung selbst aufgehoben.

LAN-basierte Aktiv/Standby-Failover-Konfiguration

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



In diesem Abschnitt wird beschrieben, wie Sie Active/Standby Failover im transparenten Modus mit einer Ethernet-Failover-Verbindung konfigurieren. Wenn Sie ein LAN-basiertes Failover konfigurieren, müssen Sie das sekundäre Gerät mit einem Bootstrap versehen, um die Failover-Verbindung zu erkennen, bevor das sekundäre Gerät die aktuelle Konfiguration vom primären Gerät beziehen kann.

Hinweis: Wenn Sie von kabelbasiertem Failover zu LAN-basiertem Failover wechseln, können Sie viele Schritte überspringen, z. B. die Zuweisung der aktiven und Standby-IP-Adressen für jede Schnittstelle, die Sie für die kabelbasierte Failover-Konfiguration abgeschlossen haben.

Konfiguration der primären Einheit

Führen Sie diese Schritte aus, um die primäre Einheit in einer LAN-basierten Aktiv/Standby-Failover-Konfiguration zu konfigurieren. Diese Schritte stellen die Mindestkonfiguration bereit, die erforderlich ist, um Failover auf der primären Einheit zu aktivieren. Im Multiple-Context-Modus werden alle Schritte im Systemausführungsbereich ausgeführt, sofern nicht anders angegeben.

Gehen Sie wie folgt vor, um die primäre Einheit in einem Aktiv/Standby-Failover-Paar zu konfigurieren:

1. Falls Sie dies noch nicht getan haben, konfigurieren Sie die aktiven und Standby-IP-Adressen für die Verwaltungsschnittstelle (transparenter Modus). Die Standby-IP-Adresse wird auf der Sicherheitslösung verwendet, die derzeit als Standby-Einheit fungiert. Sie muss sich im gleichen Subnetz wie die aktive IP-Adresse befinden.**Hinweis:** Konfigurieren Sie keine IP-Adresse für die Stateful Failover-Verbindung, wenn Sie eine dedizierte Stateful Failover-Schnittstelle verwenden. Mit dem Befehl **failover interface ip** konfigurieren Sie in einem späteren Schritt eine dedizierte Stateful Failover-Schnittstelle.
   ```
   hostname(config-if)#ip address active_addr netmask
                          standby standby_addr
   ```

   Im Gegensatz zum gerouteten Modus, der für jede Schnittstelle eine IP-Adresse erfordert, verfügt eine transparente Firewall über eine dem gesamten Gerät zugewiesene IP-Adresse. Die Sicherheits-Appliance verwendet diese IP-Adresse als Quelladresse für Pakete, die von der Sicherheits-Appliance ausgehen, z. B. Systemmeldungen oder AAA-Kommunikation. Im Beispiel wird die IP-Adresse für die primäre ASA wie folgt konfiguriert:
   ```
   hostname(config)#ip address 172.16.1.1 255.255.0.0 standby 172.16.1.2
   ```

   Hier wird 172.16.1.1 für die Primäreinheit und 172.16.1.2 für die Sekundäreinheit (Standby) verwendet.**Hinweis:** Im Multiple-Context-Modus müssen Sie die Schnittstellenadressen in jedem Kontext konfigurieren. Verwenden Sie den Befehl **change to context**, um zwischen Kontexten zu wechseln. Die Eingabeaufforderung ändert sich in `hostname/context(config-if)#`, wobei Kontext der Name des aktuellen Kontexts ist.
2. (Nur PIX Security Appliance-Plattform) Aktivieren Sie das LAN-basierte Failover.
   ```
   hostname(config)#failover lan enable
   ```

3. Bestimmen Sie die Einheit als primäre Einheit.
   ```
   hostname(config)#failover lan unit primary
   ```

4. Definieren Sie die Failover-Schnittstelle.Geben Sie die Schnittstelle an, die als Failover-Schnittstelle verwendet werden soll.
   ```
   hostname(config)#failover lan interface if_name phy_if
   ```

   In dieser Dokumentation wird der "Failover" (Schnittstellenname für Ethernet0) für eine Failover-Schnittstelle verwendet.
   ```
   hostname(config)#failover lan interface failover Ethernet3
   ```

   Das *if_name*-Argument weist der Schnittstelle, die durch das *phy_if*-Argument angegeben wurde, einen Namen zu. Das *phy_if*-Argument kann der physische Portname sein, z. B. Ethernet1, oder eine zuvor erstellte Subschnittstelle, z. B. Ethernet0/2.3.Weisen Sie der Failover-Verbindung die aktive und die Standby-IP-Adresse zu.

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

In dieser Dokumentation wird für die Konfiguration der Failover-Verbindung 10.1.0.1 für den aktiven Switch, 10.1.0.2 für den Standby-Switch und "Failover" für den Schnittstellennamen Ethernet0 verwendet.

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

Die Standby-IP-Adresse muss sich im gleichen Subnetz wie die aktive IP-Adresse befinden. Sie müssen die Subnetzmaske der Standby-Adresse nicht identifizieren.Die IP-Adresse und die MAC-Adresse der Failover-Verbindung ändern sich beim Failover nicht. Die aktive IP-Adresse für die Failover-Verbindung verbleibt immer bei der primären Einheit, während die Standby-IP-Adresse bei der zweiten Einheit verbleibt.Aktivieren der Schnittstelle

```
hostname(config)#interface phy_if

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

Im Beispiel wird Ethernet3 für Failover verwendet:

```
hostname(config)#interface ethernet3

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

5. (Optional) Um Stateful Failover zu aktivieren, konfigurieren Sie die Stateful Failover-Verbindung.Geben Sie die Schnittstelle an, die als Stateful Failover-Verbindung verwendet werden soll.

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

In diesem Beispiel wurde "state" (Status) als Schnittstellenname für Ethernet2 verwendet, um Informationen zum Status der Failover-Verbindung auszutauschen:

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

Hinweis: Wenn die Stateful Failover-Verbindung die Failover-Verbindung oder eine Datenschnittstelle verwendet, müssen Sie nur das **Argument *if_name angeben***.Das *if_name-**Argument weist der Schnittstelle, die durch das** phy_if-**Argument*** angegeben wird, einen logischen Namen zu. Das *phy_if-**Argument kann der physische Portname, z. B. Ethernet1, oder eine zuvor erstellte Subschnittstelle, z. B. Ethernet0/2.3, sein.*** Diese Schnittstelle darf für keinen anderen Zweck verwendet werden, mit Ausnahme der Failover-Verbindung (optional).Weisen Sie der Stateful Failover-Verbindung eine aktive und Standby-IP-Adresse zu.**Hinweis:** Wenn die Stateful Failover-Verbindung die Failover-Verbindung oder die Datenschnittstelle verwendet, überspringen Sie diesen Schritt. Sie haben bereits die aktiven und Standby-IP-Adressen für die Schnittstelle definiert.

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

Der 10.0.0.1 wird als aktive und der 10.0.0.2 als Standby-IP-Adresse für die Stateful Failover-Verbindung in diesem Beispiel verwendet.

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

Die Standby-IP-Adresse muss sich im gleichen Subnetz wie die aktive IP-Adresse befinden. Sie müssen die Subnetzmaske der Standby-Adresse nicht identifizieren.Die IP-Adresse und die MAC-Adresse der Stateful Failover-Verbindung ändern sich beim Failover nur, wenn sie

eine Datenschnittstelle verwenden. Die aktive IP-Adresse bleibt immer bei der primären Einheit, während die Standby-IP-Adresse bei der zweiten Einheit verbleibt.Aktivieren Sie die Schnittstelle.**Hinweis:** Wenn die Stateful Failover-Verbindung die Failover-Verbindung oder die Datenschnittstelle verwendet, überspringen Sie diesen Schritt. Sie haben die Schnittstelle bereits aktiviert.

```
hostname(config)#interface phy_if

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

Hinweis: In diesem Szenario wird beispielsweise Ethernet2 für die Stateful-Failover-Verbindung verwendet:

```
hostname(config)#interface ethernet2

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

6. Aktivieren Sie Failover.

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

Hinweis: Geben Sie den **Failover-**Befehl zuerst auf dem primären Gerät aus, und geben Sie ihn dann auf dem sekundären Gerät aus. Nachdem Sie den **Failover-**Befehl für das sekundäre Gerät ausgegeben haben, wird die Konfiguration sofort vom primären Gerät entfernt und als *Standby-Gerät* festgelegt. Die primäre ASA bleibt erhalten, leitet den Datenverkehr normal weiter und markiert sich selbst als *aktives* Gerät. Ab diesem Zeitpunkt wird das Standby-Gerät bei jedem Ausfall des aktiven Geräts als aktiv angezeigt.

7. Speichern Sie die Systemkonfiguration im Flash-Speicher.

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

Sekundäre Einheitenkonfiguration

Die einzige erforderliche Konfiguration für die Sekundäreinheit ist die Failover-Schnittstelle. Bei der Sekundäreinheit müssen diese Befehle zunächst mit der Primäreinheit kommunizieren. Nachdem die Primäreinheit ihre Konfiguration an die Sekundäreinheit gesendet hat, besteht der einzige permanente Unterschied zwischen den beiden Konfigurationen im Befehl **Failover LAN Unit**, der jede Einheit als Primär- oder Sekundäreinheit identifiziert.

Im Mehrfachkontextmodus werden alle Schritte im Systemausführungsbereich ausgeführt, sofern nicht anders angegeben.

Gehen Sie wie folgt vor, um die Sekundäreinheit zu konfigurieren:

1. (Nur PIX Security Appliance-Plattform) LAN-basiertes Failover aktivieren

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

2. Definieren Sie die Failover-Schnittstelle. Verwenden Sie die gleichen Einstellungen, die Sie für die Primäreinheit verwendet haben.Geben Sie die Schnittstelle an, die als Failover-Schnittstelle verwendet werden soll.

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

In dieser Dokumentation wird Ethernet0 für eine LAN-Failover-Schnittstelle verwendet.

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

Das *if_name*-Argument weist der Schnittstelle, die durch das *phy_if*-Argument angegeben wurde, einen Namen zu.Weisen Sie der Failover-Verbindung die aktive und die Standby-IP-Adresse zu.

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

In dieser Dokumentation wird für die Konfiguration der Failover-Verbindung 10.1.0.1 für den aktiven Switch, 10.1.0.2 für den Standby-Switch und "Failover" für den Schnittstellennamen Ethernet0 verwendet.

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

Hinweis: Geben Sie diesen Befehl genau so ein, wie Sie ihn bei der Konfiguration der Failover-Schnittstelle auf der primären Einheit eingegeben haben.Aktivieren Sie die Schnittstelle.

```
hostname(config)#interface phy_if

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

In diesem Szenario wird beispielsweise Ethernet0 für Failover verwendet.

```
hostname(config)#interface ethernet3

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

3. (Optional) Benennen Sie diese Einheit als Sekundäreinheit.

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

Hinweis: Dieser Schritt ist optional, da Einheiten standardmäßig als sekundär gekennzeichnet sind, sofern sie nicht zuvor konfiguriert wurden.

4. Aktivieren Sie Failover.

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

Hinweis: Nachdem Sie die Failover-Funktion aktiviert haben, sendet die aktive Einheit die Konfiguration im laufenden Speicher an die Standby-Einheit. Während die Konfiguration synchronisiert wird, erhalten Sie folgende Meldungen: *Beginning configuration Replication: Senden zur Paarung* und *Beendigung der Konfigurationsreplikation zur Paarung* auf der Konsole der aktiven Einheit.

5. Speichern Sie die Konfiguration nach Abschluss der Replikation im Flash-Speicher.

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

Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

Primäre 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
```

Sekundäre 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
```

Überprüfen

Verwendung des Befehls show failover

In diesem Abschnitt wird die Ausgabe des Befehls **show failover** beschrieben. Für jede Einheit können Sie den Failover-Status mit dem Befehl **show failover** überprüfen.

Primäre 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
```

Sekundäre 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
```

Verwenden Sie den Befehl **show failover state** (Failover-Status anzeigen), um den Zustand zu überprüfen.

Primäre 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
```

Sekundäre Einheit

```
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
```

Um die IP-Adressen der Failover-Einheit zu überprüfen, verwenden Sie den Befehl **show failover interface**.

Primäreinheit

```
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
```

Sekundäre Einheit

```
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
```

Ansicht der überwachten Schnittstellen

So zeigen Sie den Status der überwachten Schnittstellen an: Geben Sie im Einzelkontextmodus den **Befehl show monitor-interface im globalen Konfigurationsmodus ein.** Geben Sie im Multiple-Context-Modus die **Monitor-Schnittstelle** in einem Kontext ein.

Primäre 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
```

Sekundäre 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
```

Hinweis: Wenn Sie keine Failover-IP-Adresse eingeben, zeigt der Befehl **show failover** 0.0.0.0 für die IP-Adresse an, und die Überwachung der Schnittstelle bleibt *warten*. Weitere Informationen zu

den verschiedenen Failover-Zuständen finden Sie im Abschnitt show failover der *Cisco Security Appliance Command Reference, Version 7.2*.

Anzeige der Failover-Befehle in der laufenden Konfiguration

Geben Sie den folgenden Befehl ein, um die Failover-Befehle in der aktuellen Konfiguration anzuzeigen:

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

Alle Failover-Befehle werden angezeigt. Geben Sie bei Einheiten, die im Mehrfachkontextmodus ausgeführt werden, den Befehl **show running-config failover** im Systemausführungsbereich ein. Geben Sie den Befehl **show running-config all failover** ein, um die Failover-Befehle in der aktuellen Konfiguration anzuzeigen und Befehle einzuschließen, für die Sie den Standardwert nicht geändert haben.

Failover-Funktionstests

Gehen Sie wie folgt vor, um die Failover-Funktion zu testen:

1. Testen Sie, dass Ihr aktives Gerät oder Ihre Failover-Gruppe den Datenverkehr wie erwartet über FTP weiterleitet (z. B.), um eine Datei zwischen Hosts an verschiedenen Schnittstellen zu senden.
2. Erzwingen Sie mit dem folgenden Befehl ein Failover auf die Standby-Einheit:Geben Sie für Active/Standby Failover (Aktiv/Standby-Failover) den folgenden Befehl auf der aktiven Einheit ein:
   ```
   hostname(config)#no failover active
   ```
3. Verwenden Sie FTP, um eine andere Datei zwischen denselben beiden Hosts zu senden.
4. Wenn der Test nicht erfolgreich war, geben Sie den **Befehl show failover ein**, um den Failover-Status zu überprüfen.
5. Mit dem folgenden Befehl können Sie die Einheit oder die Failover-Gruppe wieder in den aktiven Status zurücksetzen:Geben Sie für Active/Standby Failover (Aktiv/Standby-Failover) den folgenden Befehl auf der aktiven Einheit ein:
   ```
   hostname(config)#failover active
   ```

Failover

Geben Sie einen der folgenden Befehle ein, um die Aktivierung des Standby-Geräts zu erzwingen:

Geben Sie den folgenden Befehl auf der Standby-Einheit ein:

```
hostname#failover active
```

Geben Sie den folgenden Befehl auf der aktiven Einheit ein:

```
hostname#no failover active
```

Deaktiviertes Failover

Geben Sie den folgenden Befehl ein, um Failover zu deaktivieren:

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

Wenn Sie die Failover-Funktion in einem Aktiv/Standby-Paar deaktivieren, wird der Aktiv- und Standby-Status jedes Geräts beibehalten, bis Sie neu starten. So bleibt die Standby-Einheit beispielsweise im Standby-Modus, sodass beide Geräte nicht anfangen, Datenverkehr zu übergeben. Informationen zum Aktivieren der Standby-Einheit (auch wenn die Failover-Funktion deaktiviert ist) finden Sie im Abschnitt Forcing Failover (Failover erzwingen).

Wenn Sie die Failover-Funktion für ein Aktiv/Aktiv-Paar deaktivieren, bleiben die Failover-Gruppen auf der aktiven Einheit, auf der sie momentan aktiv sind, unabhängig davon, für welche Einheit sie konfiguriert sind. Der Befehl **no failover** kann im Systemausführungsbereich eingegeben werden.

Wiederherstellung einer fehlerhaften Einheit

Geben Sie den folgenden Befehl ein, um eine ausgefallene Einheit in einen nicht ausgefallenen Zustand wiederherzustellen:

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

Wenn Sie eine ausgefallene Einheit in einen nicht ausgefallenen Zustand zurücksetzen, wird sie nicht automatisch aktiviert. wiederhergestellte Einheiten oder Gruppen bleiben im Standby-Status, bis sie durch Failover (erzwungen oder natürlich) aktiviert werden. Eine Ausnahme ist eine mit dem Befehl preempt konfigurierte Failover-Gruppe. Wenn zuvor aktiv, wird eine Failover-Gruppe aktiviert, wenn sie mit dem Befehl "preempt" konfiguriert wird und die Einheit, bei der sie ausgefallen ist, die bevorzugte Einheit ist.

Fehlerbehebung

Wenn ein Failover auftritt, senden beide Security-Appliances Systemmeldungen aus. Dieser Abschnitt behandelt folgende Themen

- Failover-Überwachung
- Einheitenfehler
- %ASA-3-210005: LU-Zuweisungsverbindung fehlgeschlagen
- Failover-Systemmeldungen
- Nachrichten debuggen
- SNMP
- Bekannte Probleme

Failover-Überwachung

Dieses Beispiel veranschaulicht, was geschieht, wenn das Failover nicht begonnen hat, die

Netzwerkschnittstellen zu überwachen. Das Failover überwacht die Netzwerkschnittstellen erst, wenn das zweite `Hello-`Paket von der anderen Einheit auf dieser Schnittstelle gehört wurde. Dies dauert etwa 30 Sekunden. Wenn die Einheit an einen Netzwerk-Switch angeschlossen ist, der das Spanning Tree Protocol (STP) ausführt, dauert dies doppelt so lange wie die `Vorwärtsverzögerung`, die im Switch konfiguriert wurde, der normalerweise als 15 Sekunden konfiguriert ist, plus diese 30 Sekunden Verzögerung. Dies liegt daran, dass der Netzwerk-Switch beim ASA-Start und unmittelbar nach einem Failover-Ereignis eine temporäre Bridge-Schleife erkennt. Nach Erkennung dieser Schleife wird die Weiterleitung von Paketen an diesen Schnittstellen für die `Weiterleitungsverzögerungszeit` beendet. Er wechselt dann für eine zusätzliche `Weiterleitungsverzögerungszeit in den Listen-`Modus, in der der Switch auf Bridge-Schleifen wartet, jedoch keinen Datenverkehr weiterleitet oder Failover-`Hello-`Pakete weiterleitet. Nach der zweifachen Vorwärtsverzögerung (30 Sekunden) wird der Datenverkehrsfluss wieder aufgenommen. Jede ASA verbleibt im `Wartemodus`, bis `Hello-`Pakete im Wert von 30 Sekunden von der anderen Einheit `abgerufen` werden. Innerhalb der Zeit, in der die ASA den Datenverkehr weiterleitet, fällt die andere Einheit nicht aus, da die `Hello-`Pakete nicht abgerufen werden. Alle anderen Failover-Überwachungsfunktionen, d. h. Stromversorgung, Schnittstellenverlust und Failover Cable `hello`.

Für Failover empfiehlt Cisco dringend, dass Kunden PortFast auf allen Switch-Ports aktivieren, die mit ASA-Schnittstellen verbunden sind. Darüber hinaus müssen Channeling und Trunking an diesen Ports deaktiviert werden. Wenn die Schnittstelle der ASA innerhalb eines Failovers ausfällt, muss der Switch keine 30 Sekunden warten, während der Port von einem Status des Zuhörens zu Weiterleitung wechselt.

```
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)
```

Führen Sie die folgenden Schritte aus, um Failover-Probleme einzugrenzen:

- Prüfen Sie die Netzwerkkabel, die mit der Schnittstelle im Warte-/Fehlzustand verbunden sind, und ersetzen Sie sie, wenn möglich, durch diese.
- Wenn zwischen den beiden Einheiten ein Switch angeschlossen ist, überprüfen Sie, ob die Netzwerke, die mit der Schnittstelle verbunden sind, im Status Warten/Fehlschlagen ordnungsgemäß funktionieren.
- Überprüfen Sie den Switch-Port, der mit der Schnittstelle im Warte-/Fehlfunktion-Status verbunden ist, und verwenden Sie, falls möglich, den anderen FE-Port am Switch.
- Stellen Sie sicher, dass Sie Port fast aktiviert und sowohl Trunking als auch Channeling für die Switch-Ports deaktiviert haben, die mit der Schnittstelle verbunden sind.

Einheitenfehler

In diesem Beispiel hat das Failover einen Fehler erkannt. Beachten Sie, dass die Fehlerquelle Schnittstelle 1 auf der primären Einheit ist. Die Einheiten befinden sich aufgrund des Fehlers

wieder im `Wartemodus`. Die ausgefallene Einheit hat sich aus dem Netzwerk entfernt (die Schnittstellen sind ausgefallen) und keine `Hello`-Pakete mehr im Netzwerk sendet. Die aktive Einheit bleibt so lange `warten`, bis die ausgefallene Einheit ausgetauscht wird und die Failover-Kommunikation wieder beginnt.

```
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-Zuweisungsverbindung fehlgeschlagen

Wenn Sie die folgende Fehlermeldung erhalten, liegt möglicherweise ein Speicherproblem vor:

```
LU-Zuweisungsverbindung fehlgeschlagen
```

Dieses Problem ist im Cisco Bug ID CSCte80027 dokumentiert (nur registrierte Kunden). Um dieses Problem zu beheben, aktualisieren Sie Ihre Firewall auf eine Softwareversion, in der dieser Fehler behoben ist. Einige der ASA-Softwareversionen, unter denen dieser Fehler behoben wurde, sind 8.2(4), 8.3(2), 8.4(2).

Failover-Systemmeldungen

Die Sicherheits-Appliance gibt eine Reihe von Systemmeldungen bezüglich Failover auf Prioritätsstufe 2 aus, was auf einen kritischen Zustand hinweist. Um diese Meldungen anzuzeigen, können Sie die Protokollierungskonfiguration der Cisco Security Appliance sowie die Systemprotokollmeldungen lesen, um die Protokollierung zu aktivieren und Systemmeldungen anzuzeigen. Außerdem finden Sie dort Beschreibungen der Systemmeldungen.

Hinweis: Beim Switchover wird das Failover logisch heruntergefahren und dann die Schnittstellen hochgefahren, wodurch Syslog-Meldungen **411001** und **411002** generiert werden. Dies ist eine normale Aktivität.

Nachrichten debuggen

Um Debugmeldungen anzuzeigen, geben Sie den Befehl **debug fover ein**. Weitere Informationen finden Sie in der Cisco Security Appliance Command Reference.

Hinweis: Da der Debugausgabe im CPU-Prozess eine hohe Priorität zugewiesen wird, kann dies die Systemleistung erheblich beeinträchtigen. Verwenden Sie deshalb die Befehle **debug fover** nur zur Fehlerbehebung oder zur Fehlerbehebung in Sitzungen mit dem technischen Support von Cisco.

SNMP

Um SNMP-Syslog-Traps für Failover zu empfangen, konfigurieren Sie den SNMP-Agent so, dass

SNMP-Traps an SNMP-Managementstationen gesendet werden, definieren Sie einen Syslog-Host, und kompilieren Sie die Cisco Syslog-MIB in Ihre SNMP-Managementstation. Weitere Informationen finden Sie unter **snmp-server** und **logging-**Befehle in der Cisco Security Appliance-Befehlsreferenz.

Failover-Pollzeit

Um die Polling- und Haltezeiten der Failover-Einheit anzugeben, verwenden Sie den Befehl **failover polltime** im globalen Konfigurationsmodus.

Der `Failover Polltime Unit msec [time]` fragt Hello-Nachrichten ab, um das Zeitintervall darzustellen, um das Vorhandensein der Standby-Einheit zu überprüfen.

Entsprechend stellt die `Failover Holdtime Unit msec [time]` die Zeitspanne dar, in der ein Gerät eine Hello-Nachricht auf der Failover-Verbindung empfangen muss, nach der die Peer-Einheit als fehlerhaft deklariert wird.

Um die Polll- und Haltezeiten der Datenschnittstellen in einer Aktiv/Standby-Failover-Konfiguration anzugeben, verwenden Sie den Befehl **failover polltime interface** im globalen Konfigurationsmodus. Um die Standardabfrage und die Haltezeiten wiederherzustellen, verwenden Sie die **no-**Form dieses Befehls.

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

Mit dem Befehl **Failover polltime interface** können Sie die Häufigkeit ändern, mit der Hello-Pakete an Datenschnittstellen gesendet werden. Dieser Befehl ist nur für Active/Standby-Failover verfügbar. Verwenden Sie für Active/Active Failover den Befehl **polltime interface** im Konfigurationsmodus für die Failover-Gruppe anstelle des Befehls **failover polltime interface**.

Sie können keinen *Holdtime-**Wert*** eingeben, der weniger als das Fünffache der Interfaces-Abfragezeit beträgt. Mit einer schnelleren Abfragezeit kann die Sicherheits-Appliance Fehler erkennen und Failover schneller auslösen. Eine schnellere Erkennung kann jedoch zu unnötigen Switchovers führen, wenn das Netzwerk vorübergehend überlastet ist. Die Schnittstellentests beginnen, wenn ein Hello-Paket mehr als die Hälfte der Haltezeit auf der Schnittstelle nicht hörbar ist.

Sie können in die Konfiguration sowohl Befehle für Failover Polltime Unit als auch für Failover Polltime einschließen.

In diesem Beispiel wird die Zeitfrequenz für die Schnittstellenabfrage auf 500 Millisekunden und die Haltezeit auf 5 Sekunden festgelegt:

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

Weitere Informationen finden Sie im Abschnitt Failover Polltime der *Cisco Security Appliance Command Reference, Version 7.2*.

Zertifikat/Privater Schlüssel in Failover-Konfiguration exportieren

Das primäre Gerät repliziert automatisch den privaten Schlüssel/das private Zertifikat auf die sekundäre Einheit. Geben Sie den Befehl **write memory** (**Schreibspeicher**) in der aktiven Einheit ein, um die Konfiguration, die das Zertifikat/den privaten Schlüssel enthält, auf die Standby-Einheit zu replizieren. Alle Schlüssel/Zertifikate auf der Standby-Einheit werden gelöscht und durch die Konfiguration der aktiven Einheit repliziert.

Hinweis: Sie dürfen Zertifikate, Schlüssel und Vertrauenspunkte nicht manuell vom aktiven Gerät importieren und anschließend in das Standby-Gerät exportieren.

WARNUNG: Entschlüsselung der Failover-Nachricht fehlgeschlagen.

Fehlermeldung:

```
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
```

Dieses Problem tritt aufgrund der Failover-Schlüsselkonfiguration auf. Um dieses Problem zu beheben, entfernen Sie den Failover-Schlüssel, und konfigurieren Sie den neuen gemeinsamen Schlüssel.

Problem: Nach der Konfiguration eines transparenten Aktiv/Standby-Failovers im Mehrfachmodus "Failover" fällt immer das Failover auf.

Das Failover ist konstant, wenn die internen Schnittstellen beider ASAs direkt verbunden sind und die externen Schnittstellen beider ASAs direkt verbunden sind. Wenn ein Switch zwischen den Switches verwendet wird, flapping das Failover.

Lösung: Deaktivieren Sie die BPDU an den ASA-Schnittstellen, um dieses Problem zu beheben.

ASA-Module Failover

Wenn Advanced Inspection and Prevention Security Services Module (AIP-SSM) oder Content Security and Control Security Services Module (CSC-SSM) in Aktiv- und Standby-Einheiten eingesetzt werden, wird die Lösung als Failover unabhängig von der ASA betrieben. **Die Module müssen manuell in aktiven und Standby-Einheiten konfiguriert werden. Das Failover repliziert die Modulkonfiguration nicht.**

Hinsichtlich des Failovers müssen beide ASA-Einheiten, die über AIP-SSM- oder CSC-SSM-Module verfügen, denselben Hardwaretyp aufweisen. Wenn die Primäreinheit beispielsweise über das ASA-SSM-10-Modul verfügt, muss die Sekundäreinheit über das ASA-SSM-10-Modul verfügen.

Failover-Nachrichtenblock fehlerhaft

Fehlermeldung `%PIX|ASA-3-105010: (Primär) Failover-Nachrichtenblock fehlerhaft`

Erläuterung: Der Speicher des Blocks wurde erschöpft. Dies ist eine transiente Nachricht, und die Sicherheits-Appliance sollte sich wiederherstellen. *Primär* kann auch als *Sekundäreinheit* für die Sekundäreinheit aufgeführt werden.

Empfohlene Aktion: Überwachen des aktuellen Blockspeichers mithilfe des Befehls **show blocks**

Failover-Problem des AIP-Moduls

Wenn sich zwei ASAs in einer Failover-Konfiguration befinden und beide über ein AIP-SSM verfügen, müssen Sie die Konfiguration der AIP-SSMs manuell replizieren. Nur die Konfiguration der ASA wird vom Failover-Mechanismus repliziert. Das AIP-SSM ist nicht im Failover enthalten.

Erstens wird das AIP-SSM in Bezug auf Failover unabhängig von der ASA betrieben. Für Failover ist aus ASA-Sicht lediglich die Tatsache erforderlich, dass die AIP-Module denselben Hardwaretyp aufweisen. Darüber hinaus muss die Konfiguration der ASA zwischen dem aktiven und dem Standby-Gerät wie bei allen anderen Teilen des Failovers synchronisiert werden.

Bei der Einrichtung der AIP handelt es sich im Grunde genommen um unabhängige Sensoren. Zwischen den beiden gibt es kein Failover, und sie kennen einander nicht. Sie können unabhängige Codeversionen ausführen. Das heißt, sie müssen nicht übereinstimmen, und der ASA ist die Codeversion des AIP in Bezug auf Failover egal.

ASDM initiiert eine Verbindung mit dem AIP über die IP-Management-Schnittstelle, die Sie auf dem AIP konfiguriert haben. Anders ausgedrückt: Die Verbindung zum Sensor erfolgt in der Regel über HTTPS, was von der Einrichtung des Sensors abhängt.

Sie können ein Failover der ASA unabhängig von den IPS-Modulen (AIP) einrichten. Sie sind immer noch mit dem gleichen verbunden, weil Sie eine Verbindung zu seiner Management-IP herstellen. Um eine Verbindung mit dem anderen AIP herzustellen, müssen Sie erneut eine Verbindung zu seiner Verwaltungs-IP herstellen, um diese zu konfigurieren und darauf zuzugreifen.

Weitere Informationen finden Sie unter ASA: Senden Sie Netzwerkverkehr von der ASA an das AIP SSM-Konfigurationsbeispiel für weitere Informationen und Beispielkonfigurationen zum Senden von Netzwerkverkehr, der über die Cisco Adaptive Security Appliance (ASA) der Serie ASA 550 an das Advanced Inspection and Prevention Security Services Module (AIP-SSM) (IPS) geleitet wird.

Bekannte Probleme

Wenn Sie versuchen, auf das ASDM auf der sekundären ASA mit der Software Version 8.x und der ASDM-Version 6.x für die Failover-Konfiguration zuzugreifen, wird folgender Fehler ausgegeben:

```
Fehler: Der Name im Sicherheitszertifikat ist ungültig oder entspricht nicht dem Namen der Site
```

Im Zertifikat ist der Emittent und der Betreffname die IP-Adresse der *aktiven* Einheit, nicht die IP-Adresse der *Standby*-Einheit.

In ASA Version 8.x wird das interne (ASDM)-Zertifikat vom aktiven Gerät auf das Standby-Gerät repliziert, was die Fehlermeldung verursacht. Wenn jedoch dieselbe Firewall auf Version 7.x-Code mit 5.x-ASDM ausgeführt wird und Sie versuchen, auf ASDM zuzugreifen, erhalten Sie die folgende regelmäßige Sicherheitswarnung:

```
Das Sicherheitszertifikat hat einen gültigen Namen, der mit dem Namen der Seite übereinstimmt,
die Sie anzeigen möchten.
```

Wenn Sie das Zertifikat überprüfen, ist der Aussteller und der Betreffname die IP-Adresse der Standby-Einheit.

Zugehörige Informationen

- Cisco Adaptive Security Appliances der Serie ASA 5500
- Cisco PIX Firewall-Software
- FWSM-Failover-Konfiguration (Firewall Services Module)
- FWSM Failover Troubleshooting
- Funktionsweise von Failover auf der Cisco Secure PIX Firewall
- Technischer Support und Dokumentation - Cisco Systems