

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

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Zugehörige Produkte](#)

[Konventionen](#)

[Aktiv/Aktiv-Failover](#)

[Übersicht über Aktiv/Aktiv-Failover](#)

[Primär-/Sekundär- und Aktiv-/Standby-Status](#)

[Geräteinitialisierung und Konfigurationssynchronisierung](#)

[Befehlsreplikation](#)

[Failover-Trigger](#)

[Failover-Aktionen](#)

[Reguläres und Stateful Failover](#)

[Reguläres Failover](#)

[Stateful Failover](#)

[Beschränkungen der Failover-Konfiguration](#)

[Nicht unterstützte Funktionen](#)

[LAN-basierte Aktiv/Aktiv-Failover-Konfiguration](#)

[Netzwerkdiagramm](#)

[Konfiguration der primären Einheit](#)

[Sekundäre Einheitenkonfiguration](#)

[Konfigurationen](#)

[Überprüfen](#)

[Verwendung des Befehls show failover](#)

[Ansicht der überwachten Schnittstellen](#)

[Anzeige der Failover-Befehle in der laufenden Konfiguration](#)

[Failover-Funktionstests](#)

[Failover](#)

[Deaktiviertes Failover](#)

[Wiederherstellung einer fehlerhaften Einheit](#)

[Fehlerbehebung](#)

[Failover-Systemmeldungen](#)

[Primärer Verlust von Failover-Kommunikation mit Kombination auf interface\\_name](#)

[Nachrichten debuggen](#)

[SNMP](#)

[Failover-Pollzeit](#)

[WARNUNG: Entschlüsselung der Failover-Nachricht fehlgeschlagen.](#)

[Zugehörige Informationen](#)

## 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/Aktiv-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 Active/Standby-Technologie ASA/PIX 7.x. 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/Aktiv-Failover

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

- [Übersicht über Aktiv/Aktiv-Failover](#)
- [Primär-/Sekundär- und Aktiv-/Standby-Status](#)
- [Geräteinitialisierung und Konfigurationssynchronisierung](#)
- [Befehlsreplikation](#)
- [Failover-Trigger](#)
- [Failover-Aktionen](#)

## Übersicht über Aktiv/Aktiv-Failover

Aktiv/Aktiv-Failover ist nur für Security Appliances im Multiple-Context-Modus verfügbar. In einer Aktiv/Aktiv-Failover-Konfiguration können beide Security Appliances Netzwerkverkehr weiterleiten.

Bei Active/Active Failover teilen Sie die Sicherheitskontexte der Security Appliance in Failover-Gruppen auf. Eine Failover-Gruppe ist einfach eine logische Gruppe aus einem oder mehreren Sicherheitskontexten. Sie können maximal zwei Failover-Gruppen auf der Sicherheits-Appliance erstellen. Der Admin-Kontext ist immer ein Mitglied der Failover-Gruppe 1. Alle nicht zugewiesenen Sicherheitskontexte sind standardmäßig auch Mitglieder der Failover-Gruppe 1.

Die Failover-Gruppe bildet die Basiseinheit für Failover in Active/Active Failover.

Schnittstellenausfallüberwachung, Failover und Aktiv/Standby-Status sind Attribute einer Failover-Gruppe und nicht der Einheit. Wenn eine aktive Failover-Gruppe ausfällt, wechselt sie in den Standby-Status, während die Standby-Failover-Gruppe aktiv wird. Die Schnittstellen in der Failover-Gruppe, die aktiv wird, übernehmen die MAC- und IP-Adressen der Schnittstellen in der Failover-Gruppe, die ausgefallen sind. Die Schnittstellen in der Failover-Gruppe, die sich jetzt im Standby-Status befindet, übernehmen die Standby-MAC- und IP-Adressen.

**Hinweis:** Eine Failover-Gruppe, die bei einer Einheit ausfällt, bedeutet nicht, dass die Einheit ausgefallen ist. Die Einheit kann noch über eine andere Failover-Gruppe verfügen, die den Datenverkehr weiterleitet.

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

Wie beim Aktiv/Standby-Failover wird eine Einheit in einem Aktiv/Aktiv-Failover-Paar als primäre Einheit und die andere als sekundäre Einheit festgelegt. Im Gegensatz zu Active/Standby-Failover gibt diese Bezeichnung nicht an, welches Gerät aktiv wird, wenn beide Geräte gleichzeitig starten. Die primäre/sekundäre Bezeichnung hat stattdessen zwei Funktionen:

- Bestimmt, welche Einheit die aktuelle Konfiguration für das Paar bereitstellt, wenn es gleichzeitig bootet.
- Bestimmt, auf welchem Gerät die einzelnen Failover-Gruppen beim gleichzeitigen Booten der Einheiten im aktiven Zustand angezeigt werden. Jede Failover-Gruppe in der Konfiguration wird mit einer primären oder sekundären Einheitenvoreinstellung konfiguriert. Sie können beide Failover-Gruppen auf einer Einheit im Paar im aktiven Zustand konfigurieren, während die andere Einheit die Failover-Gruppen im Standby-Status enthält. Eine typischere Konfiguration besteht jedoch darin, jeder Failover-Gruppe eine andere Rollenvoreinstellung zuzuweisen, um jede Gruppe auf einer anderen Einheit aktiv zu machen und den Datenverkehr auf die Geräte zu verteilen. **Hinweis:** Die Sicherheits-Appliance bietet **keine** Services für den Lastenausgleich. Der Lastenausgleich muss von einem Router durchgeführt werden, der den Datenverkehr an die Sicherheits-Appliance weiterleitet.

Welche Einheit jede Failover-Gruppe aktiviert wird, wird wie dargestellt bestimmt

- Wenn eine Einheit gebootet wird, während die Peer-Einheit nicht verfügbar ist, werden beide Failover-Gruppen auf der Einheit aktiv.
- Wenn eine Einheit hochgefahren wird, während die Peer-Einheit aktiv ist (wobei beide Failover-Gruppen im aktiven Zustand sind), bleiben die Failover-Gruppen auf der aktiven Einheit im aktiven Zustand, unabhängig von der primären oder sekundären Präferenz der Failover-Gruppe, bis eines dieser Ereignisse eintritt: Ein Failover tritt auf. Sie erzwingen die Failover-Gruppe manuell mit dem Befehl **no failover active**. Sie haben die Failover-Gruppe mit dem Befehl **preempt** konfiguriert, wodurch die Failover-Gruppe automatisch auf der bevorzugten Einheit aktiviert wird, sobald die Einheit verfügbar ist.
- Wenn beide Einheiten gleichzeitig booten, wird jede Failover-Gruppe auf der bevorzugten Einheit aktiv, nachdem die Konfigurationen synchronisiert wurden.

## Geräteinitialisierung und Konfigurationssynchronisierung

Die Konfigurations-Synchronisierung erfolgt, wenn eine oder beide Einheiten in einem Failover-Paar gestartet werden. Die Konfigurationen werden wie folgt synchronisiert:

- Wenn eine Einheit startet, während die Peer-Einheit aktiv ist (wobei beide Failover-Gruppen aktiv sind), kontaktiert die Boot-Einheit die aktive Einheit, um die aktuelle Konfiguration abzurufen, unabhängig davon, ob die Boot-Einheit primär oder sekundär gekennzeichnet ist.
- Wenn beide Geräte gleichzeitig booten, ruft die sekundäre Einheit die aktuelle Konfiguration von der primären Einheit ab.

Wenn die Replikation gestartet wird, wird in der Security Appliance-Konsole der Einheit, die die Konfiguration sendet, die Meldung "Beginning configuration Replication: Sending to mate," und wenn der Vorgang abgeschlossen ist, zeigt die Security Appliance die Meldung "End Configuration Replication to mate" an. Während der Replikation können Befehle, die auf der Einheit eingegeben werden, die die Konfiguration sendet, nicht ordnungsgemäß an die Peer-Einheit repliziert werden, und Befehle, die auf der Einheit eingegeben wurden, die die Konfiguration empfängt, können von der empfangenen Konfiguration überschrieben werden. Während des Replikationsprozesses der Konfiguration dürfen keine Befehle auf beiden Einheiten im Failover-Paar ausgeführt werden. Die Replikation, die von der Größe der Konfiguration abhängt, kann einige Sekunden bis mehrere Minuten dauern.

Auf der Einheit, die die Konfiguration empfängt, existiert die Konfiguration nur im laufenden Speicher. Um die Konfiguration nach der Synchronisierung im Flash-Speicher zu speichern, geben Sie den Befehl **write memory all** in den Systemausführungsbereich der Einheit ein, die über die Failover-Gruppe 1 im aktiven Zustand verfügt. Der Befehl wird auf die Peer-Einheit repliziert, die die Konfiguration in den Flash-Speicher schreibt. Die Verwendung des **all**-Schlüsselworts mit diesem Befehl bewirkt, dass das System und alle Kontextualisierungen gespeichert werden.

**Hinweis:** Auf externen Servern gespeicherte Startkonfigurationen sind von beiden Einheiten über das Netzwerk zugänglich und müssen nicht für jede Einheit separat gespeichert werden. Alternativ können Sie die Contexts-Konfigurationsdateien von der Festplatte der primären Einheit auf einen externen Server kopieren und anschließend auf die Festplatte der sekundären Einheit kopieren, wo sie beim erneuten Laden der Einheit verfügbar werden.

## [Befehlsreplikation](#)

Nachdem beide Einheiten ausgeführt wurden, werden Befehle wie folgt von einer Einheit zur anderen repliziert:

- Befehle, die in einem Sicherheitskontext eingegeben werden, werden von der Einheit repliziert, auf der der Sicherheitskontext im aktiven Zustand angezeigt wird, zur Peer-Einheit. **Hinweis:** Der Kontext wird im aktiven Zustand einer Einheit betrachtet, wenn die Failover-Gruppe, zu der sie gehört, sich im aktiven Zustand dieser Einheit befindet.
- Im Systemausführungsbereich eingegebene Befehle werden von der Einheit, auf der sich die Failover-Gruppe 1 im aktiven Zustand befindet, auf die Einheit repliziert, auf der sich die Failover-Gruppe 1 im Standby-Zustand befindet.
- Im Admin-Kontext eingegebene Befehle werden von der Einheit, auf der sich die Failover-Gruppe 1 im aktiven Zustand befindet, auf die Einheit repliziert, auf der sich die Failover-Gruppe 1 im Standby-Modus befindet.

Alle Konfigurations- und Dateibefehle (**Kopieren, Umbenennen, Löschen, mkdir, rmdir** usw.) werden mit diesen Ausnahmen repliziert. Die Befehle **show, debug, mode, firewall** und **failover lan unit** werden nicht repliziert.

Wenn die Befehle auf der entsprechenden Einheit nicht eingegeben werden, um eine Befehlsreplikation durchzuführen, laufen die Konfigurationen nicht mehr synchron. Diese

Änderungen gehen möglicherweise verloren, wenn die erste Konfigurationssynchronisierung durchgeführt wird.

Sie können den Befehl **write standby** verwenden, um Konfigurationen, die nicht synchronisiert wurden, erneut zu synchronisieren. Für Active/Write StandbyActive Failover verhält sich der **Write Standby**-Befehl wie folgt:

- Wenn Sie den Befehl **write standby** im Systemausführungsbereich eingeben, werden die Systemkonfiguration und die Konfigurationen für alle Sicherheitskontexte auf der Sicherheits-Appliance auf die Peer-Einheit geschrieben. Dies umfasst Konfigurationsinformationen für Sicherheitskontexte, die sich im Standby-Zustand befinden. Sie müssen den Befehl in den Systemausführungsbereich der Einheit eingeben, deren Failover-Gruppe 1 im aktiven Zustand ist. **Hinweis:** Wenn auf der Peereinheit Sicherheitskontexte im aktiven Zustand vorhanden sind, wird der Befehl **write standby** dazu führen, dass aktive Verbindungen über diese Kontexte beendet werden. Verwenden Sie den Befehl **failover active** auf der Einheit, die die Konfiguration bereitstellt, um sicherzustellen, dass alle Kontexte auf dieser Einheit aktiv sind, bevor Sie den Befehl **write standby** eingeben.
- Wenn Sie den Befehl **write standby** in einem Sicherheitskontext eingeben, wird nur die Konfiguration für den Sicherheitskontext auf die Peer-Einheit geschrieben. Sie müssen den Befehl im Sicherheitskontext auf der Einheit eingeben, auf der der Sicherheitskontext im aktiven Zustand angezeigt wird.

Replizierte Befehle werden beim Replizieren auf die Peer-Einheit nicht im Flash-Speicher gespeichert. Sie werden der aktuellen Konfiguration hinzugefügt. Um replizierte Befehle in Flash-Speicher auf beiden Einheiten zu speichern, verwenden Sie den Befehl **write memory** oder **copy running-config startup-config** auf der Einheit, an der die Änderungen vorgenommen wurden. Der Befehl wird auf die Peer-Einheit repliziert und bewirkt, dass die Konfiguration im Flash-Speicher der Peer-Einheit gespeichert wird.

## [Failover-Trigger](#)

Bei Active/Active Failover kann Failover auf Einheitsebene ausgelöst werden, wenn eines dieser Ereignisse eintritt:

- Die Einheit weist einen Hardwarefehler auf.
- Das Gerät weist einen Stromausfall auf.
- Bei der Einheit tritt ein Softwarefehler auf.
- Der Befehl **no failover active** oder **failover active** wird in den Systemausführungsbereich eingegeben.

Failover wird auf Failover-Gruppenebene ausgelöst, wenn eines dieser Ereignisse eintritt:

- Zu viele überwachte Schnittstellen in der Gruppe schlagen fehl.
- Der Befehl **no failover active group\_id** oder **failover active group\_id** wird eingegeben.

## [Failover-Aktionen](#)

In einer Aktiv/Aktiv-Failover-Konfiguration erfolgt das Failover auf Failover-Gruppenbasis und nicht auf Systembasis. Wenn Sie z. B. beide Failover-Gruppen als aktiv für die Primäreinheit bestimmen und die Failover-Gruppe 1 ausfällt, bleibt die Failover-Gruppe 2 auf der Primäreinheit aktiv, während die Failover-Gruppe 1 auf der Sekundäreinheit aktiv wird.

**Hinweis:** Wenn Sie das Aktiv/Aktiv-Failover konfigurieren, stellen Sie sicher, dass der kombinierte Datenverkehr für beide Einheiten innerhalb der Kapazität der einzelnen Einheiten liegt.

Diese Tabelle zeigt die Failover-Aktion für jedes Fehlerereignis. Für jedes Fehlerereignis werden die Richtlinien, ob ein Failover erfolgt oder nicht, sowie Aktionen für die aktive Failover-Gruppe und Aktionen für die Standby-Failover-Gruppe angegeben.

Fehlerereignis	Richtlinie	Aktive Gruppenaktion	Standby-Gruppenaktion	Hinweise
Bei einem Gerät treten Fehler bei Stromversorgung oder Software auf.	Failover	Status als Standby-Markieren	Werden Sie Standby. Aktiv als fehlgeschlagen markieren	Wenn eine Einheit in einem Failover-Paar ausfällt, werden alle aktiven Failover-Gruppen auf dieser Einheit als ausgefallen gekennzeichnet und auf der Peer-Einheit aktiviert.
Schnittstellenausfall bei aktiver Failover-Gruppe oberhalb des Grenzwerts	Failover	Aktive Gruppe als fehlgeschlagen markieren	Aktiv werden	Keine
Schnittstellenausfall bei Standby-Failover-Gruppe oberhalb des Grenzwerts	Kein Failover	Keine Aktion	Markierung als Standby-Gruppe fehlgeschlagen	Wenn die Standby-Failover-Gruppe als ausgefallen gekennzeichnet ist, versucht die aktive Failover-Gruppe nicht, einen Failover durchzuführen

				en, selbst wenn der Grenzwert für Schnittstelle überschritten wurde.
Früher aktive Failover-Gruppenwiederherstellung	Kein Failover	Keine Aktion	Keine Aktion	Sofern der Befehl <b>preempt</b> nicht konfiguriert wurde, bleiben die Failover-Gruppen auf ihrer aktuellen Einheit aktiv.
Failover-Verbindung ist beim Start fehlgeschlagen	Kein Failover	Aktiv werden	Aktiv werden	Wenn die Failover-Verbindung beim Start nicht verfügbar ist, werden beide Failover-Gruppen auf beiden Geräten aktiv.
Stateful Failover Link fehlgeschlagen	Kein Failover	Keine Aktion	Keine Aktion	Statusinformationen sind veraltet, und Sitzungen werden beendet, wenn ein Failover auftritt.
Failover-Verbindung während des Betriebs fehlgeschlagen	Kein Failover	K/A	K/A	Jede Einheit markiert die Failover-Schnittstelle als fehlgeschla

				gen. Sie sollten die Failover-Verbindung so schnell wie möglich wiederherstellen, da bei einem Ausfall der Failover-Verbindung kein Failover auf die Standby-Einheit möglich ist.
--	--	--	--	---

## Reguläres und Stateful Failover

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

- [Reguläres Failover](#)
- [Stateful Failover](#)

### 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 (wenn sie 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 Call Manager. 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 Call Manager erhält, hält er den Call Manager für unerreichbar und registriert sich selbst.

## Beschränkungen der Failover-Konfiguration

Sie können Failover nicht mit den folgenden IP-Adressen konfigurieren:

- IP-Adressen, die über DHCP abgerufen werden
- IP-Adressen, die über PPPoE abgerufen werden
- IPv6-Adressen

Darüber hinaus gelten folgende Einschränkungen:

- Stateful Failover wird von der Adaptive Security Appliance ASA 5505 nicht unterstützt.
- Active/Active Failover wird von der Adaptive Security Appliance ASA 5505 nicht unterstützt.
- Sie können Failover nicht konfigurieren, wenn Easy VPN Remote auf der Adaptive Security Appliance ASA 5505 aktiviert ist.
- VPN-Failover wird im Multiple-Context-Modus nicht unterstützt.

## Nicht unterstützte Funktionen

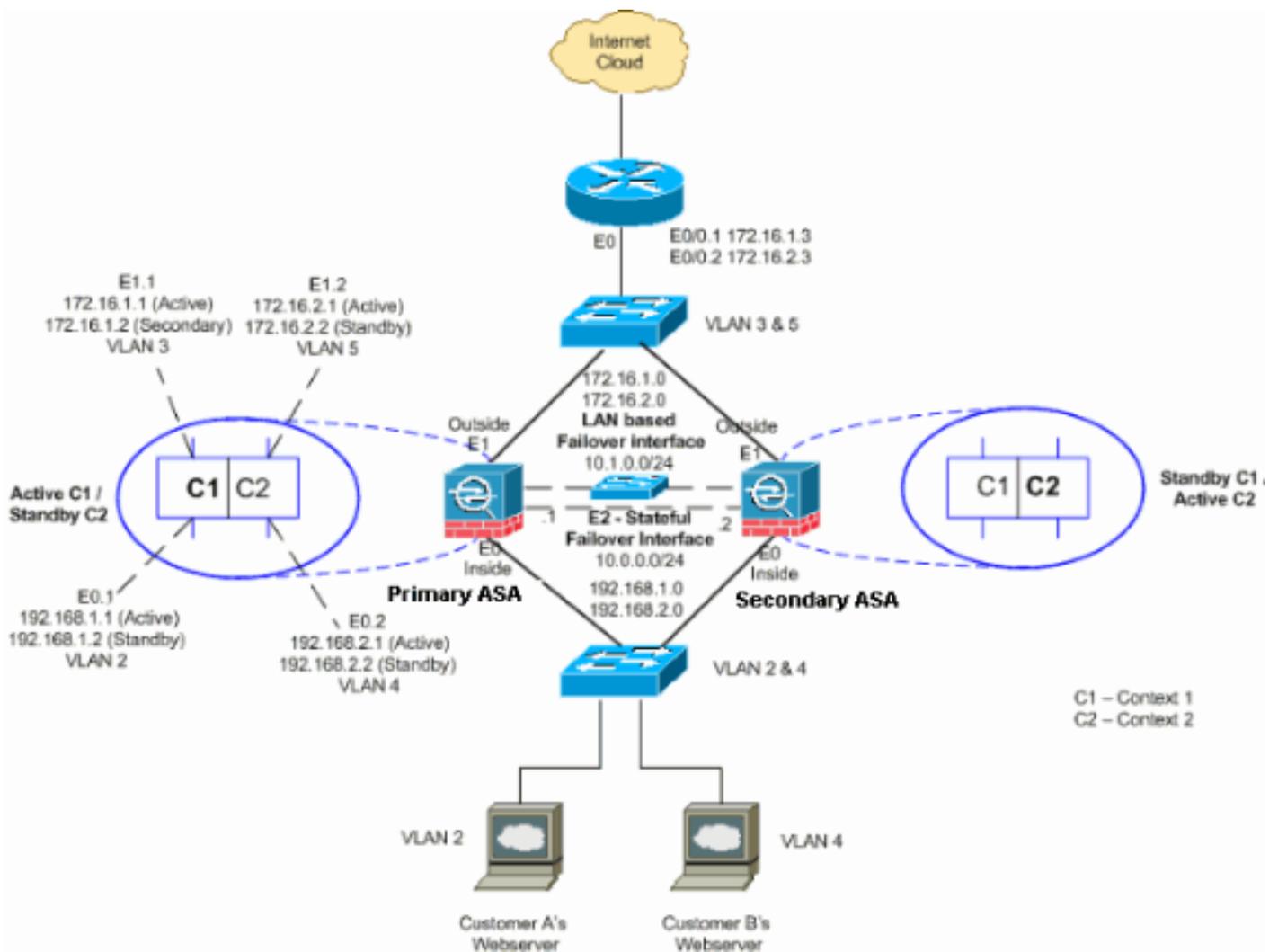
Der Multiple-Context-Modus unterstützt diese Funktionen nicht:

- Dynamische Routing-Protokolle Sicherheitskontexte unterstützen nur statische Routen. Sie können OSPF oder RIP nicht im Multiple-Context-Modus aktivieren.
- VPN
- Multicast

## LAN-basierte Aktiv/Aktiv-Failover-Konfiguration

### Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



In diesem Abschnitt wird beschrieben, wie Sie Active/Active Failover 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:** Anstelle eines Crossover-Ethernetkabels für die direkte Verbindung der Geräte empfiehlt Cisco die Verwendung eines dedizierten Switches zwischen der primären und der sekundären Einheit.

In diesem Abschnitt werden folgende Themen behandelt:

- [Konfiguration der primären Einheit](#)
- [Sekundäre Einheitenkonfiguration](#)

## [Konfiguration der primären Einheit](#)

Gehen Sie wie folgt vor, um die primäre Einheit in einer Aktiv/Aktiv-Failover-Konfiguration zu konfigurieren:

1. Falls Sie dies noch nicht getan haben, konfigurieren Sie die aktiven und Standby-IP-Adressen für jede Datenschnittstelle (gerouteter Modus), für die Management-IP-Adresse (transparenter Modus) oder für die Management-Schnittstelle. 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. Sie müssen die Schnittstellenadressen in jedem Kontext konfigurieren. Wechseln Sie mit dem **Befehl change to context** zwischen Kontexten. Die Eingabeaufforderung ändert sich in `hostname/context(config-if)#`, wobei Kontext der Name des aktuellen Kontexts ist. Im transparenten Firewall-Modus müssen Sie für jeden Kontext eine Management-IP-Adresse eingeben. **Hinweis:** Konfigurieren Sie keine IP-Adresse für die Stateful Failover-Verbindung, wenn Sie eine dedizierte Stateful Failover-Schnittstelle verwenden. Sie verwenden den **Befehl failover interface ip**, um in einem späteren Schritt eine dedizierte Stateful Failover-Schnittstelle zu konfigurieren.

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

Im Beispiel wird die externe Schnittstelle für context1 der primären ASA folgendermaßen konfiguriert:

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

Für Kontext2:

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

Im Routed Firewall-Modus und für die Management-Only-Schnittstelle wird dieser Befehl für jede Schnittstelle im Schnittstellenkonfigurationsmodus eingegeben. Im transparenten Firewall-Modus wird der Befehl im globalen Konfigurationsmodus eingegeben.

2. Konfigurieren Sie die grundlegenden Failover-Parameter im Systemausführungsbereich. (Nur PIX Security Appliance) LAN-basiertes Failover aktivieren:

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

Bestimmen Sie die Einheit als primäre Einheit:

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

Geben Sie die Failover-Verbindung an:

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

In diesem Beispiel wird das Interface Ethernet 3 als LAN-basierte Failover-Schnittstelle verwendet.

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

Das `if_name`-Argument weist der Schnittstelle, die durch das `phy_if`-Argument angegeben wurde, einen logischen Namen zu. Beim `phy_if`-Argument kann es sich um den Namen des physischen Ports, z. B. Ethernet1, oder um eine zuvor erstellte Subschnittstelle wie Ethernet0/2.3 handeln. Auf der Adaptive Security Appliance ASA 5505 gibt `phy_if` ein VLAN an. Diese Schnittstelle sollte für keinen anderen Zweck verwendet werden (mit Ausnahme der Stateful Failover-Verbindung optional). Geben Sie die aktiven und Standby-IP-Adressen der Failover-Verbindung an:

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

In diesem Beispiel wird 10.1.0.1 als aktive und 10.1.0.2 als Standby-IP-Adressen für die Failover-Schnittstelle verwendet.

```
ASA(config)#failover interface ip LANFailover  
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-IP-Adresse nicht identifizieren. Die IP-Adresse und die MAC-Adresse der Failover-Verbindung ändern sich beim Failover nicht. Die aktive IP-Adresse bleibt immer bei der primären Einheit, während die Standby-IP-Adresse bei der zweiten Einheit verbleibt.

## Sekundäre Einheitenkonfiguration

Wenn Sie ein LAN-basiertes Aktiv/Aktiv-Failover konfigurieren, müssen Sie die sekundäre Einheit bootstrap, um die Failover-Verbindung zu erkennen. Dadurch kann die Sekundäreinheit mit der laufenden Konfiguration der Primäreinheit kommunizieren und diese empfangen.

Gehen Sie wie folgt vor, um die Sekundäreinheit in einer Aktiv/Aktiv-Failover-Konfiguration zu bootstrap:

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

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

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

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

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

Das if\_name-Argument weist der Schnittstelle, die durch das phy\_if-Argument angegeben wurde, einen logischen Namen zu. Beim phy\_if-Argument kann es sich um den Namen des physischen Ports, z. B. Ethernet1, oder um eine zuvor erstellte Subschnittstelle wie Ethernet0/2.3 handeln. Auf der Adaptive Security Appliance ASA 5505 gibt phy\_if ein VLAN an. 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
```

```
ASA(config)#failover interface ip LANFailover 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. Die Standby-IP-Adresse muss sich im gleichen Subnetz wie die aktive IP-Adresse befinden. Sie müssen die Subnetzmaske der Standby-Adresse nicht identifizieren. Aktivieren Sie die Schnittstelle.

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

3. Benennen Sie diese Einheit als sekundäre Einheit:

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

**Hinweis:** Dieser Schritt ist optional, da die Einheiten standardmäßig als sekundär gekennzeichnet sind, sofern nicht zuvor anders konfiguriert.

4. Aktivieren Sie Failover.

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

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: Das Senden zur Paarung und Beendigung der Konfigurationsreplikation zur Paarung** wird auf der Konsole der aktiven Einheit angezeigt. **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.

5. Geben Sie nach Abschluss der Replikation den folgenden Befehl ein, um die Konfiguration im Flash-Speicher zu speichern:

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

6. Falls erforderlich, erzwingen Sie alle Failover-Gruppen, die auf dem primären Gerät aktiv sind, in den aktiven Status auf dem sekundären Gerät. Um zu erzwingen, dass eine Failover-Gruppe auf der Sekundäreinheit aktiv wird, geben Sie den folgenden Befehl in den Systemausführungsbereich der Primäreinheit ein:

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

Das `group_id`-Argument gibt die Gruppe an, die auf der sekundären Einheit aktiviert werden soll.

## Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

### Primäre ASA - Konfiguration von Context1

```
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

```

## Primäre ASA - Context2-Konfiguration

```
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:000000000000000000000000000000000000
: end
```

## Primäre 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

```

## Sekundäre 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
```

## 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(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

## Sekundäre 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

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

## Primäre 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
```

## Sekundäre Einheit

```
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
```

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

## Primäreinheit

```
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
```

## Sekundäre Einheit

```
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
```

## [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.

**Hinweis:** Um die Systemüberwachung auf einer bestimmten Schnittstelle zu aktivieren, verwenden Sie im globalen Konfigurationsmodus den Befehl [monitor-interface](#):

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

## Primäre 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
```

## Sekundäre 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
```

**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 Schnittstellen bleibt im `Wartezustand`. Sie müssen eine Failover-IP-Adresse festlegen, damit das Failover funktioniert. Weitere Informationen zu den verschiedenen Zuständen für Failover finden Sie unter [show failover](#).

## [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 unterschiedlichen Schnittstellen zu senden.
2. Erzwingen Sie mit dem folgenden Befehl ein Failover auf die Standby-Einheit: Geben Sie für Active/Active Failover (Aktives/Aktives Failover) den folgenden Befehl auf der Einheit ein, auf der die Failover-Gruppe installiert ist, die die Schnittstelle enthält, über die die Hosts verbunden werden, aktiv ist:

```
hostname(config)#no failover active group group_id
```

3. Verwenden Sie FTP, um eine weitere Datei zwischen den 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/Active Failover (Aktives/Aktives Failover) den folgenden Befehl auf der Einheit ein, auf der die Failover-Gruppe installiert ist, die die Schnittstelle enthält, über die die Hosts verbunden werden, aktiv ist:

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

## Failover

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

Geben Sie diesen Befehl in den Systemausführungsbereich der Einheit ein, in der sich die Failover-Gruppe im Standby-Status befindet:

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

Oder geben Sie diesen Befehl in den Systemausführungsbereich der Einheit ein, in der sich die Failover-Gruppe im aktiven Zustand befindet:

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

Wenn Sie diesen Befehl in das System eingeben, bewirkt der Ausführungsbereich, dass alle Failover-Gruppen aktiv werden:

```
hostname#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 [Forced Failover \(Erzwungene Failover-Funktion\)](#).

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 Active/Active Failover-Gruppe in einen nicht ausgefallenen Zustand wiederherzustellen:

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

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 ist 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:

1. [Failover-Systemmeldungen](#)
2. [Nachrichten debuggen](#)
3. [SNMP](#)

## [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.

## [Primärer Verlust von Failover-Kommunikation mit Kombination auf interface\\_name](#)

Diese Failover-Meldung wird angezeigt, wenn eine Einheit des Failover-Paars nicht mehr mit der anderen Einheit des Paares kommunizieren kann. Primär kann auch als Sekundäreinheit für die Sekundäreinheit aufgeführt werden.

(Primär) Verlorene Failover-Kommunikation mit Kombination auf `interface_name`

Überprüfen Sie, ob das Netzwerk, das mit der angegebenen Schnittstelle verbunden ist, ordnungsgemäß funktioniert.

## Nachrichten debuggen

Um Debugmeldungen anzuzeigen, geben Sie den Befehl **debug fover ein**. Weitere Informationen finden Sie unter [Cisco Security Appliance Command Reference, Version 7.2](#).

**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. [Version 7.2](#) enthält weitere Informationen zu den Befehlen **snmp-server** und **logging** in der [Befehlsreferenz für die Cisco Security Appliance](#).

## Failover-Pollzeit

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

Die `Failover Polltime Unit msec [time]` stellt das Zeitintervall dar, in dem das Vorhandensein der Standby-Einheit durch Abruf von Hello-Nachrichten überprüft wird.

Entsprechend stellt die `Failover-Haltezeiteinheit msec [time]` den Zeitraum dar, in dem ein Gerät eine Hello-Nachricht auf der Failover-Verbindung erhalten muss, nach der die Peer-Einheit als ausgefallen deklariert wird.

Weitere Informationen finden Sie unter [Failover Polltime](#).

## 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.

## 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](#)