

PIX/ASA: Configuratievoorbeeld van Active/active failover

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Verwante producten](#)

[Conventies](#)

[Active/active-failover](#)

[Active/active failover-Overzicht](#)

[Primaire/secundaire status en actieve/stand-by status](#)

[Synchronisatie met apparaatinitialisatie en configuratie](#)

[Opdrachtreplicatie](#)

[failover-triggers](#)

[failover-acties](#)

[Regelmatige en stateful failover](#)

[Regelmatige failover](#)

[Stateful failover](#)

[Beperkingen van configuratie van failover](#)

[Niet-ondersteunde functies](#)

[Configuratie van actieve/actieve failover op kabel](#)

[Voorwaarden](#)

[Netwerkdigram](#)

[Configuraties](#)

[LAN-gebaseerde actieve/actieve failover-configuratie](#)

[Netwerkdigram](#)

[Configuratie van primaire eenheid](#)

[Configuratie van secundaire eenheid](#)

[Configuraties](#)

[Verifiëren](#)

[Gebruik van de overnameverdracht van de show](#)

[Beeld van gemonitorde interfaces](#)

[De failover-opdrachten in de draaiende configuratie weergeven](#)

[Functionaliteitstests](#)

[Gedwongen failover](#)

[Uitgeschakeld failover](#)

[Herstel van een mislukte eenheid](#)

[Vervang de mislukte eenheid door een nieuwe eenheid](#)

[Problemen oplossen](#)

[failover-systeemmeldingen](#)

[Primaire Lost Failover communicatie met partner op interface_name](#)

[Debug Berichten](#)

[SNMP](#)

[failover](#)

[WAARSCHUWING: Ontbreken van berichtdecryptie.](#)

[Gerelateerde informatie](#)

[Inleiding](#)

De failover-configuratie vereist twee identieke security apparaten die op elkaar zijn aangesloten via een speciale failover-verbinding en, naar keuze, een stateful failover-verbinding. De gezondheid van de actieve interfaces en eenheden wordt bewaakt om te bepalen of aan de specifieke voorwaarden voor uitsterving is voldaan. Als aan deze voorwaarden wordt voldaan, treedt failover op.

Het beveiligingsapparaat ondersteunt twee failover-configuraties, **active/active failover** en **active/stand-by failover**. Elke failover-configuratie heeft zijn eigen methode om failover te bepalen en uit te voeren. Met Active/active failover kunnen beide eenheden netwerkverkeer doorgeven. Dit laat u lading-balanceren op uw netwerk configureren. Active/active failover is alleen beschikbaar voor eenheden die in meerdere context-modus werken. Met Active/STANDBY-failover geeft slechts één unit het verkeer door terwijl de andere unit in een stand-by toestand wacht. Active/stand-by failover is beschikbaar voor eenheden die in één of meerdere contextmodus werken. Beide configuraties ondersteunen stateful of stateless (reguliere) failover.

Dit document concentreert zich op de manier om een Active/Active failover te configureren in Cisco PIX/ASA security applicatie.

Raadpleeg [PIX/ASA 7.x Active/Standby-failover Configuration](#) om meer informatie te [krijgen](#) over de Active/Standby-failover-configuraties.

Opmerking: VPN-failover wordt niet ondersteund op eenheden die in meerdere context-modus draaien omdat VPN niet in meerdere context wordt ondersteund. VPN-failover is alleen beschikbaar voor **actieve/standby failover**-configuraties in één context-configuraties.

Deze configuratiehandleiding biedt een voorbeeldconfiguratie om een korte inleiding tot de PIX/ASA 7.x actieve/actieve technologie te omvatten. Raadpleeg de [handleiding voor Cisco Security Appliance, versie 7.2](#) voor een grondiger betekenis van de theorie die aan deze technologie ten grondslag ligt.

[Voorwaarden](#)

[Vereisten](#)

Hardware-eis

De twee eenheden in een overnameconfiguratie moeten dezelfde hardwareconfiguratie hebben. Ze moeten hetzelfde model hebben, hetzelfde aantal en dezelfde soorten interfaces, en hetzelfde

aantal RAM.

Opmerking: de twee eenheden hoeven niet hetzelfde formaat Flitser geheugen te hebben. Als u eenheden met verschillende Flash-geheugenformaten gebruikt in uw configuratie van de failover, zorg er dan voor dat de eenheid met het kleinere Flash-geheugen voldoende ruimte heeft om de software-beeldbestanden en de configuratiebestanden op te slaan. Als dit niet het geval is, mislukt de configuratie-synchronisatie van de eenheid met het grotere Flash-geheugen naar de eenheid met het kleinere Flash-geheugen.

Softwarevereisten

De twee eenheden in een overnameconfiguratie moeten zich in de operationele modi bevinden (routinematig of transparant, enkelvoudig of meervoudig kader). Ze moeten dezelfde belangrijke (eerste nummer) en mindere (tweede nummer) softwareversie hebben, maar u kunt verschillende versies van de software binnen een upgrade gebruiken. U kunt bijvoorbeeld één eenheid upgrade uitvoeren van versie 7.0(1) naar versie 7.0(2) en failover actief blijven. Cisco raadt u aan beide eenheden op dezelfde versie te upgraden om compatibiliteit op lange termijn te waarborgen.

Raadpleeg [Nul-downtime upgrades uitvoeren voor failover-paren](#) voor meer informatie over het upgraden van de software op een failover-paar.

Licentievereisten

Op het PIX/ASA Security Appliance platform moet ten minste één van de eenheden een **onbeperkte (UR)licentie** hebben. De andere eenheid kan een Failover Alleen Active-Active (FO_AA) licentie of een andere UR-licentie hebben. Eenheden met een beperkte licentie kunnen niet voor failover worden gebruikt, en twee eenheden met FO_AA-licenties kunnen niet samen als een failover-paar worden gebruikt.

Opmerking: u zou de licenties op een failover-paar moeten verbeteren om extra functies en voordelen te verkrijgen. Raadpleeg voor meer informatie over een upgrade de [Licentietoetsen bij een failover-paar](#)

Opmerking: de gelicentieerde functies, zoals SSL VPN-peers of security contexten, op beide security apparaten die aan failover deelnemen, moeten identiek zijn.

Opmerking: de FO-licentie ondersteunt geen actieve/actieve failover.

[Gebruikte componenten](#)

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- PIX security applicatie met 7.x versie en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

[Verwante producten](#)

Deze configuratie kan ook worden gebruikt in combinatie met deze hardware- en softwareversies:

- ASA met 7.x versie en hoger

Opmerking: Active/active failover is niet beschikbaar in de ASA 5505 Series adaptieve security applicatie.

[Conventies](#)

Raadpleeg de [Cisco Technical Tips-conventies](#) voor meer informatie-documentverdragen.

[Active/active-failover](#)

In deze sectie worden de volgende onderwerpen beschreven:

- [Active/active failover-Overzicht](#)
- [Primaire/secundaire status en actieve/stand-by status](#)
- [Synchronisatie met apparaatinitialisatie en configuratie](#)
- [Opdrachtreplicatie](#)
- [failover-triggers](#)
- [failover-acties](#)

[Active/active failover-Overzicht](#)

Active/active failover is alleen beschikbaar voor security apparaten in meerdere context-modus. In een actieve/actieve configuratie van het failliet, kunnen beide veiligheidsapparaten netwerkverkeer passeren.

Bij Active/active failover verdeelt u de beveiligingscontexten op het security apparaat in groepen met failover. Een failover-groep is simpelweg een logische groep van een of meer security contexten. U kunt op het beveiligingsapparaat maximaal twee failover-groepen maken. De admin context is altijd een lid van de failovergroep 1. Om het even welke niet toegewezen veiligheidscontexten zijn ook leden van failliet groep 1 standaard.

De failover-groep vormt de basiseenheid voor failover in actieve/actieve failover. Controle van interfacekloof, failover, en active/stand-by status zijn alle eigenschappen van een failover-groep in plaats van de unit. Wanneer een actieve failover-groep faalt, verandert deze in de stand-by status terwijl de standby failover-groep actief wordt. De interfaces in de overnamegroep die actief wordt veronderstellen de MAC en IP adressen van de interfaces in de failliet groep. De interfaces in de overnamegroep die nu in de standby staat zijn, nemen de standby MAC- en IP-adressen over.

Opmerking: een uitvalgroep die niet op een eenheid werkt, betekent niet dat de eenheid heeft gefaald. Mogelijk is er nog een andere failover-groep die het verkeer aanstuurt.

[Primaire/secundaire status en actieve/stand-by status](#)

Net als in Active/Standby-failover wordt één eenheid in een actief/actief failover-paar aangewezen als de primaire eenheid en de andere eenheid als secundaire eenheid. Anders dan Active/Standby-failover geeft deze aanwijzing niet aan welke eenheid actief wordt wanneer beide eenheden tegelijkertijd starten. In plaats daarvan doet de primaire/secundaire benaming twee dingen:

- Bepaalt welke eenheid de actieve configuratie aan het paar biedt wanneer ze tegelijkertijd opstarten.
- Bepaalt op welke eenheid elke failover-groep in de actieve status verschijnt wanneer de eenheden tegelijkertijd opstarten. Elke failover-groep in de configuratie is ingesteld met een primaire of secundaire eenheidvoorkeuren. U kunt beide overvalgroepen in de actieve status op één eenheid in het paar configureren, waarbij de andere eenheid de overvalgroepen in de stand-by status bevat. Echter, een meer typische configuratie is elke failovergroep een verschillende rolvoorkeur toe te wijzen om elke actief op een verschillende eenheid te maken, die het verkeer over de apparaten verspreidt. **Opmerking:** het security apparaat **biedt geen** taakverdeling. Het taakverdeling moet worden verwerkt door een router die verkeer naar het beveiligingsapparaat doorgeeft.

Welke eenheid elke failover-groep actief wordt, wordt bepaald zoals wordt weergegeven

- Als een unit opstart terwijl de peer unit niet beschikbaar is, worden beide failover-groepen actief op de unit.
- Wanneer een unit opstart terwijl de peer unit actief is (met beide overvalgroepen in de actieve toestand), blijven de overnamegroep in de actieve toestand op de actieve eenheid ongeacht de primaire of secundaire voorkeur van de overnamegroep tot één van de volgende: Er treedt een uitvalssituatie op. U forceert de failover-groep handmatig naar de andere eenheid met de **geen failover actieve** opdracht. U stelde de failover-groep in met de opdracht **vooruitlopen**, waardoor de failover-groep automatisch actief wordt op de favoriete eenheid wanneer de unit beschikbaar wordt.
- Wanneer beide eenheden tegelijkertijd opstarten, wordt elke failover-groep actief op de favoriete eenheid nadat de configuraties zijn gesynchroniseerd.

Synchronisatie met apparaatinitialisatie en configuratie

Configuratie-synchronisatie vindt plaats wanneer een of beide eenheden in een failover-paar worden opgestart. De configuraties zijn gesynchroniseerd zoals wordt getoond:

- Wanneer een eenheid opstart terwijl de peer unit actief is (waarbij beide overvalgroepen actief zijn), neemt de starteenheid contact op met de actieve eenheid om de actieve configuratie te verkrijgen, ongeacht de primaire of secundaire aanwijzing van de starteenheid.
- Wanneer beide eenheden tegelijkertijd starten, verkrijgt de secundaire eenheid de actieve configuratie vanuit de primaire eenheid.

Wanneer de replicatie wordt gestart, wordt met de veiligheidswasmachineconcern op de eenheid die de configuratie stuurt, het bericht "**Beginnende configuratie-replicatie**" weergegeven: **Verzenden naar partner**" en na voltooiing van het programma geeft het security apparaat het bericht "**End Configuration Reporting to maat**" weer. Tijdens replicatie kunnen opdrachten die op de eenheid zijn ingevoerd die de configuratie heeft verzonden, niet correct naar de peer-unit worden gekopieerd, en kunnen opdrachten die op de eenheid die de configuratie ontvangt, worden ingevoerd, worden overschreven door de configuratie die wordt ontvangen. Voer geen opdrachten in op een van beide eenheden in het failover-paar tijdens het configuratie-replicatieproces. Afhankelijk van de grootte van de configuratie kan het reproduceren van een paar seconden tot een aantal minuten duren.

Op de eenheid die de configuratie ontvangt, bestaat de configuratie alleen in het actieve geheugen. Om de configuratie in het geheugen van de flitser op te slaan na synchronisatie moet u het **schrijfgeheugen alle** opdracht in de ruimte van de systeemuitvoering op de eenheid inbrengen

die failovergroep 1 in de actieve staat heeft. De opdracht wordt gerepliceerd naar de peer unit, die vervolgens de configuratie naar Flash geheugen schrijft. Wanneer u het sleutelwoord met deze opdracht gebruikt, worden het systeem en alle contextconfiguraties opgeslagen.

Opmerking: Opstartconfiguraties die op externe servers zijn opgeslagen, zijn toegankelijk vanuit beide eenheden via het netwerk en hoeven niet afzonderlijk voor elke eenheid te worden opgeslagen. U kunt ook de configuratiebestanden van de configuratie van de contexten van de disk op de primaire eenheid naar een externe server kopiëren en ze vervolgens op schijf op de secundaire eenheid kopiëren, waar ze beschikbaar komen wanneer de unit opnieuw wordt geladen.

Opdrachtreplicatie

Nadat beide eenheden actief zijn, worden er opdrachten van de ene eenheid naar de andere herhaald, zoals wordt weergegeven:

- Opdrachten die binnen een beveiligingscontext zijn ingevoerd, worden overgenomen van de eenheid waarop de beveiligingscontext in de actieve toestand verschijnt naar de peer unit.**Opmerking:** context wordt in de actieve toestand van een eenheid overwogen indien de overnamegroep waartoe zij behoort in de actieve staat van die eenheid is.
- Opdrachten die in de ruimte voor systeemuitvoering zijn ingevoerd, worden nagevolgd van de eenheid waarop de failover-groep 1 in de actieve toestand is, naar de eenheid waarop de failover-groep 1 in de stand-by status staat.
- Opdrachten die in de beheercontext zijn ingevoerd, worden gerepliceerd van de eenheid waarop de failover-groep 1 in de actieve toestand is, naar de eenheid waarop de failover-groep 1 in de stand-by status staat.

Alle configuratie- en bestandsopdrachten (**kopiëren, hernoemen, verwijderen, mkdir, rmdir** enzovoort) worden gerepliceerd, met de volgende uitzonderingen. De opdrachten **voor de unit tonen, debug, mode, firewall en failover** worden niet herhaald.

Als u de opdrachten in de juiste eenheid niet invoert zodat opdrachtreplicatie kan plaatsvinden, kunnen de configuraties niet synchroniseren. Deze veranderingen kunnen de volgende keer dat de eerste configuratie-synchronisatie plaatsvindt, verloren gaan.

U kunt de opdracht **schrijfstand** gebruiken om configuraties te resynchroniseren die uit sync zijn geraakt. Voor Active/active failover gedraagt de **schrijfstandby**-opdracht zich zoals aangegeven:

- Als u de opdracht **schrijfstand** in de ruimte voor systeemuitvoering invoert, worden de systeemconfiguratie en de configuraties voor alle beveiligingscontexten op het security apparaat naar de peer unit geschreven. Dit omvat configuratieinformatie voor de veiligheidscontexten die in de standby staat zijn. U moet de opdracht in de ruimte van de systeemuitvoering invoeren op de eenheid die in de actieve staat een overnamegroep 1 heeft.**Opmerking:** Als er in de actieve toestand een beveiligingscontext op de peer unit is, veroorzaakt de opdracht **schrijfstandby** actieve verbindingen door deze contexten om te worden beëindigd. Gebruik de opdracht **actief** failover op de eenheid die de configuratie biedt, om ervoor te zorgen dat alle contexten actief zijn op die eenheid voordat u de **schrijfstandby**-opdracht invoert.
- Als u de **schrijfstandby** opdracht in een beveiligingscontext invoert, wordt alleen de configuratie voor de beveiligingscontext aan de peer unit geschreven. U moet de opdracht in de beveiligingscontext van de unit invoeren waar de beveiligingscontext in de actieve toestand

verschijnt.

Opdrachten met replicatie worden niet opgeslagen in het Flash-geheugen wanneer deze worden gekopieerd naar de peer-unit. Ze worden toegevoegd aan de lopende configuratie. Om herhaalde opdrachten in het geheugen van de flitser op beide eenheden op te slaan, gebruik het **schrijfgeheugen of kopie in werking stellen-configuratie opstartende** - configuratie opdracht op de eenheid waarop u de wijzigingen aanbracht. De opdracht wordt herhaald naar de peer unit en zorgt ervoor dat de configuratie wordt opgeslagen in Flash geheugen op de peer unit.

failover-triggers

Bij Active/active failover kan failover op het niveau van de eenheid worden geactiveerd als een van de volgende gebeurtenissen zich voordoet:

- De eenheid heeft een hardwarestoring.
- Het apparaat heeft een stroomuitval.
- De eenheid heeft een softwarestoring.
- De **geen failover actief** of de **failover actieve** opdracht wordt ingevoerd in de ruimte van de systeemuitvoering.

Failover wordt geactiveerd op het niveau van de failovergroep wanneer een van deze gebeurtenissen zich voordoet:

- Teveel gecontroleerde interfaces in de groep ontbreken.
- De **geen opdracht van de groep actief groep_id** of de **groep_id** wordt ingevoerd.

failover-acties

In een actieve/actieve configuratie van de overnamegroep, komt de overname voor op een basis van de overnamegroep, niet op een systeembasis. Als u bijvoorbeeld beide overvalgroepen aanwijst als actief op de primaire eenheid, en failover groep 1 faalt, dan blijft overnamegroep 2 actief op de primaire eenheid terwijl overnamegroep 1 actief op de secundaire eenheid wordt.

Opmerking: Zorg er bij het configureren van actieve/actieve failover voor dat het gecombineerde verkeer voor beide eenheden binnen de capaciteit van elke eenheid valt.

Deze tabel toont de overnameactie voor elke misluktingsgebeurtenis. Voor elke misluktingsgebeurtenis, wordt het beleid (of failover al dan niet optreedt), acties voor de actieve failovergroep, en acties voor de standby failover-groep gegeven.

gebeurtenis	Beleids beleid	Actie actieve groep	actie van de groep Stand by	Opmerkingen
Een eenheid heeft een stroomuitval of softwarestoring	failover	Word standby Mark als mislu	Word stand-by. Mark actief als	Wanneer een eenheid in een failoverpaar faalt, worden alle actieve overvalgroepen op die eenheid

		kt	mislukt	gemarkeerd als mislukt en worden actief op de peer unit.
Interfacefout bij actieve overnamegroep boven drempelwaarde	failover	De actieve groep Mark als mislukt	Word actief	None
Interface faalt bij standby-failover-groep boven drempelwaarde	Geen failover	Geen actie	Mark standby-groep als mislukt	Wanneer de standby failover-groep wordt gemarkeerd als gefaald, probeert de actieve failover-groep niet over te falen, zelfs als de drempel voor interfacekoudheid wordt overschreden.
Formeel actieve overnamegroep herstelt	Geen failover	Geen actie	Geen actie	Tenzij anders ingesteld met de voorproefopdracht, blijven de overnamegroepen actief op hun huidige eenheid.
failover-link mislukt bij opstarten	Geen failover	Word actief	Word actief	Als de failover link bij opstarten is, worden beide failover groepen op beide eenheden actief.
Stateful failover-link mislukt	Geen failover	Geen actie	Geen actie	De staatsinformatie wordt verouderd, en de sessies worden beëindigd als er een failover optreedt.
Een failover-verbinding is mislukt tijdens gebruik	Geen failover	n	n	Elke eenheid tekent de failover-interface als mislukt. U dient de failover-link zo snel mogelijk te herstellen omdat de unit niet in de standby-unit kan

				slagen als de failover-link is uitgevallen.
--	--	--	--	---

Regelmatige en stateful failover

Het security apparaat ondersteunt twee typen uitvalbeveiligingssystemen, regelmatig en stateful. Deze sectie omvat deze onderwerpen:

- [Regelmatige failover](#)
- [Stateful failover](#)

Regelmatige failover

Wanneer een failover optreedt, worden alle actieve verbindingen verbroken. Clients moeten opnieuw verbindingen opzetten wanneer de nieuwe actieve eenheid de overname uitvoert.

Stateful failover

Als stateful failover is ingeschakeld, geeft de actieve unit de informatie over de toestand per verbinding voortdurend door naar de stand-by unit. Na een failover is dezelfde verbindinginformatie beschikbaar in de nieuwe actieve eenheid. Ondersteunde eindgebruikerstoepassingen hoeven niet opnieuw te worden aangesloten om dezelfde communicatiesessie te behouden.

De state informatie die aan de standby unit wordt doorgegeven omvat de volgende:

- De NAT-vertaaltabel
- De TCP-verbindingstaten
- De UDP-verbindingstaten
- De ARP-tabel
- Layer 2 bridge-tabel (wanneer deze in de transparante firewallmodus draait)
- De HTTP-verbindingstaten (als HTTP-replicatie is ingeschakeld)
- De tabel ISAKMP en IPSec SA
- De GTP PDP-verbindingdatabase

De informatie die niet aan de standby unit wordt doorgegeven wanneer stateful failover is ingeschakeld, omvat onder meer:

- De HTTP-verbindingstabel (tenzij HTTP-replicatie is ingeschakeld)
- De gebruikershandleiding (Uauth)
- De routingtabellen
- Staatsinformatie voor veiligheidsservicemodules

Opmerking: Als failover optreedt binnen een actieve Cisco IP SoftPhone-sessie, blijft de oproep actief omdat de informatie over de gespreksessie wordt gerepliceerd naar de standby-unit. Wanneer de vraag wordt beëindigd, verliest de IP SoftPhone client verbinding met de Call Manager. Dit gebeurt omdat er geen sessieinformatie voor het CTIQBE hang-up bericht op de standby unit is. Wanneer de IP SoftPhone-client geen antwoord van de Call Manager binnen een bepaalde tijdsperiode ontvangt, beschouwt hij de Call Manager onbereikbaar en maakt hij zich onbekend.

Beperkingen van configuratie van failover

U kunt failover niet configureren met deze typen IP-adressen:

- IP-adressen via DHCP
- IP-adressen die via PPPoE zijn verkregen
- IPv6-adressen

Bovendien zijn deze beperkingen van toepassing:

- Stateful failover wordt niet ondersteund op het ASA 5505 adaptieve security apparaat.
- Active/active failover wordt niet ondersteund op het ASA 5505 adaptieve security apparaat.
- U kunt failover niet configureren wanneer Easy VPN Remote is ingeschakeld op het ASA 5505 adaptieve security apparaat.
- VPN-failover wordt niet ondersteund in meerdere context-modus.

Niet-ondersteunde functies

De meerdere contextmodus ondersteunt deze functies niet:

- Dynamische routingprotocollenBeveiligingscontexten ondersteunen alleen statische routes. U kunt OSPF of RIP niet in meervoudige contextmodus inschakelen.
- VPN
- Multicast

Configuratie van actieve/actieve failover op kabel

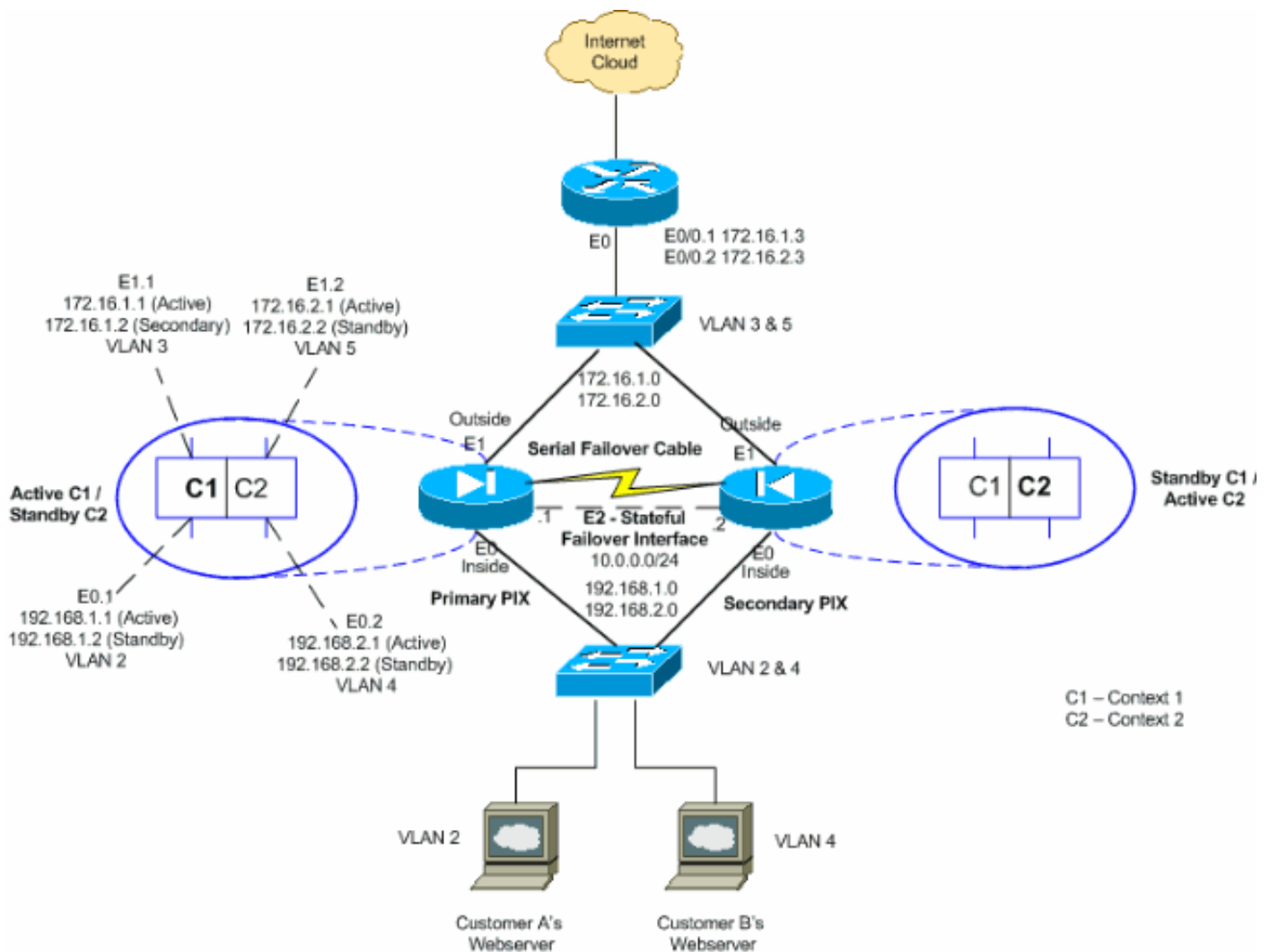
Voorwaarden

Controleer voordat u begint het volgende:

- Beide eenheden hebben dezelfde hardware-, software-configuratie en juiste licentie.
- Beide eenheden bevinden zich in dezelfde modus (enkelvoudig of meervoudig, transparant of routeerd).

Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:



Volg deze stappen om actieve/actieve failover te configureren met behulp van een seriekabel als de failover-link. De opdrachten in deze taak worden op de primaire eenheid in het failover-paar ingevoerd. De primaire eenheid is de eenheid die het uiteinde van de kabel met het label "Primair" op de kabel heeft aangesloten. Voor apparaten in meerdere context-modus worden de opdrachten in de ruimte voor systeemuitvoering ingevoerd, tenzij anders aangegeven.

U hoeft de secundaire eenheid niet te starten in het failover-paar wanneer u op kabel gebaseerde failover gebruikt. Laat de secundaire eenheid uitgeschakeld zijn tot deze is ingeschakeld.

Opmerking: Kabelgebaseerde failover is alleen beschikbaar in de PIX 500 Series security applicatie.

Voltooi deze stappen om op kabel gebaseerde, actieve/actieve failover te configureren:

1. Sluit de uitvalkabel aan op de PIX 500 Series beveiligingsapparaten. Sluit het uiteinde van de kabel met de markering "Primair" aan op de eenheid die u als primaire eenheid gebruikt, en bevestig het uiteinde van de kabel met de markering "Secundair" aan op de eenheid die u als secundaire eenheid gebruikt.
2. Schakel het primaire apparaat in.
3. Als u dit nog niet gedaan hebt, moet u de actieve en standby IP-adressen configureren voor elke gegevensinterface (Routed Mode), voor het IP-adres van het beheer (transparante modus) of voor de interface alleen-beheer. Het standby IP-adres wordt gebruikt op het security apparaat dat momenteel de stand-by unit is. Het moet in zelfde netto zoals het actieve IP adres zijn. U moet de interfaceadressen van binnen elke context configureren.

Gebruik de opdracht **Omzetten** om tussen de contexten over te schakelen. De opdracht prompt verandert in `hostname/context (configuratie-als)#`, waar context de naam van de huidige context is. U moet een IP-adres voor het beheer van elke context invoeren in een transparante firewall en meerdere contextmodi. **Opmerking:** configureer geen IP-adres voor de stateful failover-link als u een speciale stateful failover-interface wilt gebruiken. U gebruikt de **ip**-opdracht van de interface van de **failover** om in een latere stap een speciale stateful failover-interface te configureren.

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

In het voorbeeld wordt de externe interface voor context1 van de primaire PIX op deze manier geconfigureerd:

```
PIX1/context1(config)#ip address 172.16.1.1 255.255.255.0
                          standby 172.16.1.2
```

Voor context2:

```
PIX1/context2(config)#ip address 192.168.2.1 255.255.255.0
                          standby 192.168.2.2
```

In routed firewallmodus en voor de beheerinterface wordt deze opdracht ingevoerd in de interfaceconfiguratiemodus voor elke interface. In transparante firewallmodus wordt de opdracht ingevoerd in de mondiale configuratiemodus.

4. Configureer de link Stateful failover om stateful inspection mogelijk te maken. Specificeer de interface die als stateful failover-link moet worden gebruikt:

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

In dit voorbeeld wordt de Ethernet2 interface gebruikt om de stateful failover link statinformatie uit te wisselen.

```
failover link stateful Ethernet2
```

Het `if_name` argument wijst een logische naam toe aan de interface gespecificeerd door het `phy_if` argument. Het `phy_if` argument kan de fysieke havennaam zijn, zoals Ethernet1, of een eerder gecreëerd subinterface, zoals Ethernet0/2.3. Deze interface zou niet voor een ander doel moeten worden gebruikt (behalve, naar keuze, de overslagverbinding). Pas een actief en stand-by IP-adres aan de stateful failover-link toe:

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

In dit voorbeeld wordt 10.0.0.1 gebruikt als een actief en 10.0.0.2 wordt gebruikt als een standby IP-adres voor de stateful failover-link.

```
PIX1(config)#failover interface ip stateful 10.0.0.1
                          255.255.255.0 standby 10.0.0.2
```

Het standby IP-adres moet in dezelfde mate als het actieve IP-adres zijn. U hoeft het standby IP-adressubmasker niet te identificeren. Het Stateful failover-link-IP-adres en het MAC-adres veranderen niet bij failover, behalve wanneer Stateful failover een reguliere gegevensinterface gebruikt. Het actieve IP-adres blijft altijd bij de primaire eenheid, terwijl het standby IP-adres bij de secundaire eenheid blijft. Schakel de interface in:

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

5. Configuratie van de overnamegroepen. U kunt maximaal twee failovergroepen hebben. De opdracht groep maakt de gespecificeerde failover groep als deze niet bestaat en gaat de configuratie van de failovergroep in. Voor elke failovergroep moet u specificeren of de

failovergroep primaire of secundaire voorkeur heeft met de **primaire** of **secundaire** opdracht. U kunt dezelfde voorkeur aan beide groepen toewijzen. Voor taakverdeling configuraties zou u elke failover groep een verschillende eenheidspreferenties moeten toewijzen. Het volgende voorbeeld wijst overnamegroep 1 een primaire voorkeur en overvalgroep 2 een secundaire voorkeur toe:

```
hostname(config)#failover group 1
hostname(config-fover-group)#primary
hostname(config-fover-group)#exit
hostname(config)#failover group 2
hostname(config-fover-group)#secondary
hostname(config-fover-group)#exit
```

6. Wijs elke gebruikerscontext aan een failovergroep toe met behulp van de opdracht **aansluit-bij-groep** in contextconfiguratiemodus. Alle niet-toegewezen contexten worden automatisch toegewezen aan overnamegroep 1. De admin context is altijd een lid van overnamegroep 1. Voer deze opdrachten in om elke context aan een failover-groep toe te wijzen:

```
hostname(config)#context context_name
hostname(config-context)#join-failover-group {1 | 2}
hostname(config-context)#exit
```

7. Schakel failover in:

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

8. Schakel de secundaire eenheid in en schakelt de overschakeling op de eenheid in als deze nog niet is ingeschakeld:

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

De actieve eenheid stuurt de configuratie in het actieve geheugen naar de standby-unit. Terwijl de configuratie gesynchroniseerd is, worden de berichten "Beginnende configuratie replicatie: Verzenden naar partner" en "Einde configuratie replicatie om te paren" verschijnen op de primaire console. **Opmerking:** Geef eerst de **failover**-opdracht op het primaire apparaat uit en geef deze dan op het secundaire apparaat uit. Nadat u de opdracht failover op het secundaire apparaat geeft, trekt het secundaire apparaat onmiddellijk de configuratie van het primaire apparaat terug en stelt zichzelf in als *stand-by*. De primaire ASA blijft omhoog en passeert normaal verkeer en tekent zichzelf als het *actieve* apparaat. Vanaf dat punt op, wanneer een storing op het actieve apparaat optreedt, komt het stand-by apparaat op als actief.

9. Sla de configuratie op in het Flash-geheugen op de primaire eenheid. Omdat de opdrachten die op de primaire unit zijn ingevoerd, worden gerepliceerd naar de secundaire unit, slaat de secundaire unit ook de configuratie op van de unit.

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

10. Indien nodig, forceer elke overvalgroep die actief is op de primaire staat op de secundaire staat. Om een overnamegroep te dwingen actief te worden op de secundaire eenheid, geeft u deze opdracht uit in de ruimte voor systeemuitvoering op de primaire eenheid:

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

Het group_id argument specificeert de groep die u actief wilt worden op de secundaire eenheid.

Dit document gebruikt deze configuraties:

- [PIX1-systeemconfiguratie](#)
- [PIX1-configuratie - Context1](#)
- [PIX1-configuratie - Context2](#)

PIX1-systeemconfiguratie

```
PIX1#show running-config
: Saved
PIX Version 7.2(2)

!
hostname PIX1
enable password 8Ry2YjIyt7RRXU24 encrypted
no mac-address auto

!--- Enable the physical and logical interfaces in the
system execution !--- space by giving "no shutdown"
before configuring the same in the contexts ! 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 !--- of both Primary and secondary PIX.
interface Ethernet2
  description STATE Failover Interface
!
interface Ethernet3
  shutdown
!
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
```

```

!--- Command to enable the failover feature failover
!--- Command to assign the interface for stateful
failover failover link stateful Ethernet2
!--- Command to configure the active and standby IP's
for the !--- stateful failover failover interface ip
stateful 10.0.0.1 255.255.255.0 standby 10.0.0.2
!--- Configure the group 1 as primary failover group 1
!--- Configure the group 1 as secondary failover group 2
secondary
no asdm history enable
arp timeout 14400
console timeout 0

admin-context admin
context admin
  config-url flash:/admin.cfg
!
!--- Command to create a context called "context1"
context context1
!--- Command to allocate the logical interfaces to the
contexts allocate-interface Ethernet0.1 inside_context1
allocate-interface Ethernet1.1 outside_context1
config-url flash:/context1.cfg
!--- Assign this context to the failover group 1 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

```

PIX1-configuratie - Context1

```

PIX1/context1(config)#show running-config
: Saved
:
PIX Version 7.2(2)

!
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
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

```

PIX1-configuratie - Context2


```
PIX1/context2(config)#show running-config
: Saved
:
PIX Version 7.2(2)

!
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
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
```

```

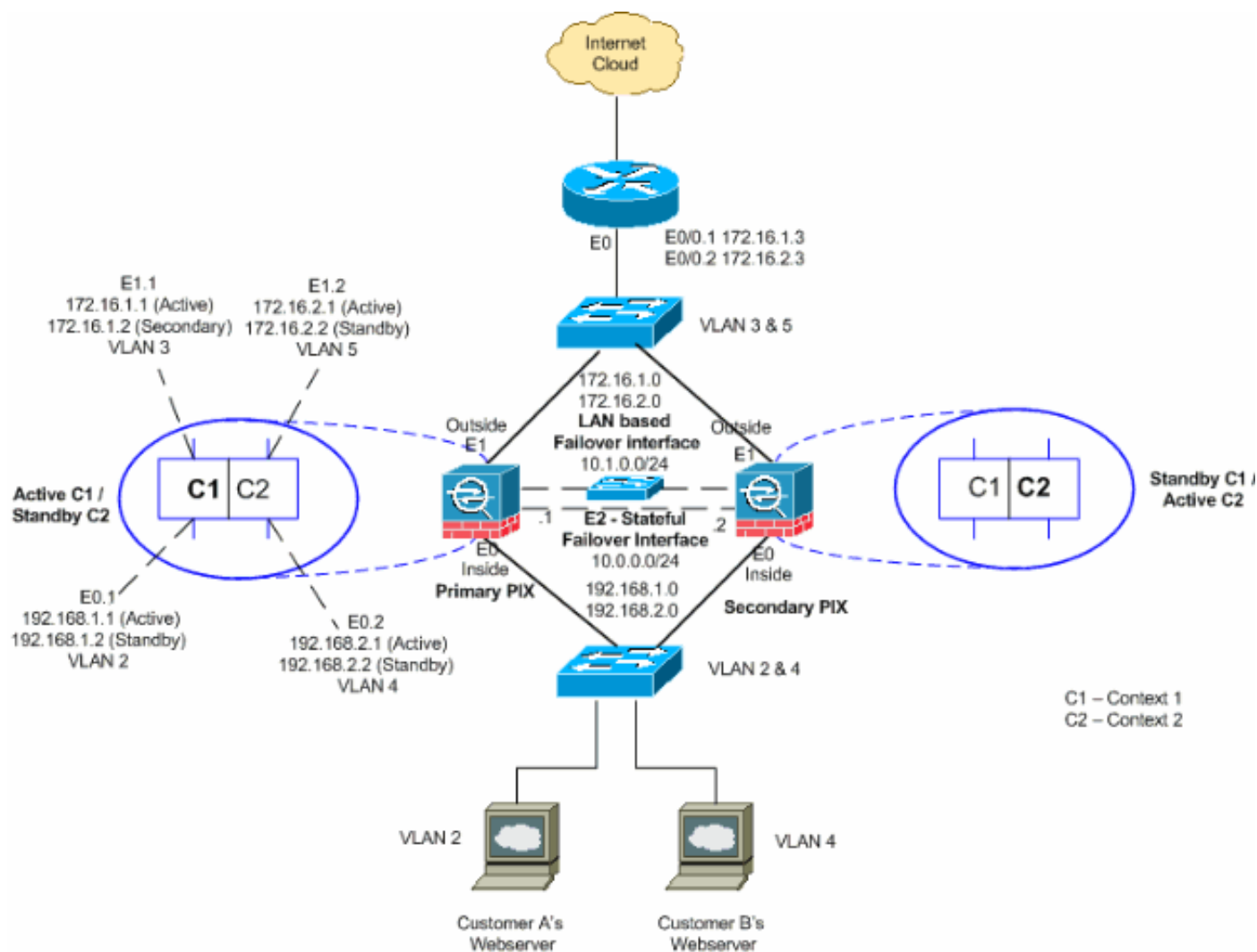
class inspection_default
 inspect dns preset_dns_map
 inspect ftp
 inspect h323 h225
 inspect h323 ras
 inspect netbios
 inspect rsh
 inspect rtsp
 inspect skinny
 inspect esmtp
 inspect sqlnet
 inspect sunrpc
 inspect tftp
 inspect sip
 inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:0000000000000000000000000000000000
: end

```

LAN-gebaseerde actieve/actieve failover-configuratie

Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:



In deze sectie wordt beschreven hoe u Active/Active failover kunt configureren met behulp van een Ethernet-failover-link. Bij het configureren van een LAN-gebaseerde failover moet u het secundaire apparaat opnieuw opstarten om de failover-link te herkennen voordat het secundaire apparaat de actieve configuratie vanaf het primaire apparaat kan verkrijgen.

Opmerking: In plaats van een cross-over Ethernet-kabel te gebruiken om de eenheden direct te verbinden, raadt Cisco u aan een specifieke schakelaar tussen de primaire en secundaire eenheden te gebruiken.

Deze sectie omvat de onderwerpen zoals getoond:

- [Configuratie van primaire eenheid](#)
- [Configuratie van secundaire eenheid](#)

Configuratie van primaire eenheid

Voltooi deze stappen om de primaire eenheid in een actieve/actieve configuratie van de failover te configureren:

1. Als u dit nog niet gedaan hebt, moet u de actieve en standby IP-adressen configureren voor elke gegevensinterface (Routed Mode), voor het IP-adres van het beheer (transparante modus) of voor de interface alleen-beheer. Het standby IP-adres wordt gebruikt op het security apparaat dat momenteel de stand-by unit is. Het moet in zelfde netto zoals het actieve IP adres zijn. U moet de interfaceadressen van binnen elke context configureren. Gebruik de opdracht **Omzetten** om tussen de contexten over te schakelen. De opdracht prompt verandert in `hostname/context (configuratie-als)#`, waar context de naam van de huidige context is. In transparante firewallmodus moet u voor elke context een IP-adres voor beheer invoeren. **Opmerking:** configureer geen IP-adres voor de stateful failover-link als u een speciale stateful failover-interface wilt gebruiken. U gebruikt de **ip**-opdracht **van de** interface van de **failover** om in een latere stap een speciale stateful failover-interface te configureren.

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

In het voorbeeld wordt de externe interface voor context1 van de primaire PIX op deze manier geconfigureerd:

```
PIX1/context1(config)#ip address 172.16.1.1 255.255.255.0  
                        standby 172.16.1.2
```

Voor context2:

```
PIX1/context2(config)#ip address 192.168.2.1 255.255.255.0  
                        standby 192.168.2.2
```

In routed firewallmodus en voor de beheerinterface wordt deze opdracht ingevoerd in de interfaceconfiguratiemodus voor elke interface. In transparante firewallmodus wordt de opdracht ingevoerd in de mondiale configuratiemodus.

2. Configureer de basisparameters voor de failover in de ruimte voor systeemuitvoering. (PIX-beveiligingsapparaat alleen) LAN-gebaseerde failover inschakelen:

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

Wijs de eenheid aan als primaire eenheid:

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

Specificeer de failover-link:

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

In dit voorbeeld gebruiken we interface Ethernet 3 als LAN-gebaseerde failover-interface.

```
PIX1(config)#failover lan interface LANFailover ethernet3
```

Het *if_name* argument wijst een logische naam toe aan de interface gespecificeerd door het *phy_if* argument. Het *phy_if* argument kan de fysieke naam van de poort zijn, zoals Ethernet1, of een eerder gemaakte subinterface, zoals Ethernet0/2.3. Op het ASA 5505 adaptieve security apparaat, specificeert *phy_if* VLAN. Deze interface moet niet voor een ander doel worden gebruikt (behalve, naar keuze, de stateful failover-link). Specificeer de failover link actief en standby IP adressen:

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

Bijvoorbeeld, gebruiken wij 10.1.0.1 als actief en 10.1.0.2 als standby IP adressen voor de interface van de failover.

```
PIX1(config)#failover interface ip LANFailover  
10.1.0.1 255.255.255.0 standby 10.1.0.2
```

Het standby IP-adres moet in dezelfde mate als het actieve IP-adres zijn. U hoeft het standby IP-adressubmasker niet te identificeren. Het IP-adres voor de failover-verbinding en het MAC-adres veranderen niet bij failover. Het actieve IP-adres blijft altijd bij de primaire eenheid, terwijl het standby IP-adres bij de secundaire eenheid blijft.

3. Configureer de koppeling Stateful failover voor stateful: Specificeer de interface die als stateful failover-link moet worden gebruikt:

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

```
PIX1(config)#failover link stateful ethernet2
```

Het *if_name* argument wijst een logische naam toe aan de interface gespecificeerd door het *phy_if* argument. Het *phy_if* argument kan de fysieke havenaam zijn, zoals Ethernet1, of een eerder gecreëerd subinterface, zoals Ethernet0/2.3. Deze interface zou niet voor een ander doel moeten worden gebruikt (behalve, naar keuze, de overslagverbinding). **Opmerking:** Als de stateful failover-link de failover-link of een reguliere data-interface gebruikt, hoeft u alleen het *if_name*-argument te leveren. Pas een actief en stand-by IP-adres aan de stateful failover-link toe. **Opmerking:** Als de stateful failover-link de failover-link of een reguliere gegevensinterface gebruikt, slaat u deze stap over. U hebt de actieve en standby IP-adressen voor de interface al gedefinieerd.

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

```
PIX1(config)#failover interface ip stateful 10.0.0.1  
255.255.255.0 standby 10.0.0.2
```

Het standby IP-adres moet in dezelfde mate als het actieve IP-adres zijn. U hoeft het standby adressubmasker niet te identificeren. Het IP-adres van de staatslink en het MAC-adres veranderen niet bij failover. Het actieve IP-adres blijft altijd bij de primaire eenheid, terwijl het standby IP-adres bij de secundaire eenheid blijft. Schakel de interface in. **Opmerking:** Als de

stateful failover-link de failover-link of de reguliere gegevensinterface gebruikt, slaat u deze stap over. U hebt de interface al ingeschakeld.

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

4. Configuratie van de overnamegroepen. U kunt maximaal twee failovergroepen hebben. De opdracht groep maakt de gespecificeerde failover groep als deze niet bestaat en gaat de configuratie van de failovergroep in. Specificeer voor elke failover-groep of de failover-groep **primaire** of **secundaire** voorkeur heeft met de primaire of secundaire opdracht. U kunt dezelfde voorkeur aan beide groepen toewijzen. Voor taakverdeling configuraties zou u elke failover groep een verschillende eenheidspreferenties moeten toewijzen. Het volgende voorbeeld wijst overnamegroep 1 een primaire voorkeur en overvalgroep 2 een secundaire voorkeur toe:

```
hostname(config)#failover group 1  
hostname(config-fover-group)#primary  
hostname(config-fover-group)#exit  
hostname(config)#failover group 2  
hostname(config-fover-group)#secondary  
hostname(config-fover-group)#exit
```

5. Wijs elke gebruikerscontext aan een failovergroep toe die de opdracht **aan**-overnamegroep in contextconfiguratiemodus gebruikt. Alle niet-toegewezen contexten worden automatisch toegewezen aan overnamegroep 1. De admin context is altijd een lid van overnamegroep 1. Voer deze opdrachten in om elke context aan een failover-groep toe te wijzen:

```
hostname(config)#context context_name  
hostname(config-context)#join-failover-group {1 | 2}  
hostname(config-context)#exit
```

6. Schakel failover in.

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

Configuratie van secundaire eenheid

Bij het configureren van een LAN-gebaseerde Active/Active failover moet u de secundaire unit opnieuw opstarten om de failover-link te herkennen. Hierdoor kan de secundaire eenheid communiceren met de basiseenheid en de configuratie ervan ontvangen.

Voltooi deze stappen om de secundaire eenheid in een actieve/actieve configuratie van de failover te starten:

1. (PIX-beveiligingsapparaat alleen) Schakel een LAN-gebaseerde failover in.

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

2. Definieert de failover-interface. Gebruik dezelfde instellingen als u voor de primaire eenheid hebt gebruikt: Specificeer de interface die als de failover-interface moet worden gebruikt.

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

```
PIX1(config)#failover lan interface LANFailover ethernet3
```

Het if_name argument wijst een logische naam toe aan de interface gespecificeerd door het phy_if argument. Het phy_if argument kan de fysieke naam van de poort zijn, zoals

Ethernet1, of een eerder gemaakte subinterface, zoals Ethernet0/2.3. Op het ASA 5505 adaptieve security apparaat, specificeert phy_if VLAN. Pas het actieve en standby IP-adres aan de failover-link toe:

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

```
PIX1(config)#failover interface ip LANFailover 10.1.0.1  
255.255.255.0 standby 10.1.0.2
```

Opmerking: Voer deze opdracht in zoals u deze op de primaire eenheid hebt ingevoerd wanneer u de failover-interface hebt ingesteld. Het standby IP-adres moet in dezelfde mate als het actieve IP-adres zijn. U hoeft het stand-by adressubmasker niet te identificeren. Schakel de interface in.

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

3. Wijs deze eenheid aan als secundaire eenheid:

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

Opmerking: Deze stap is optioneel omdat standaardinstellingen zijn aangewezen als secundair, tenzij eerder anders ingesteld.

4. Schakel failover in.

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

Nadat u failover hebt ingeschakeld, stuurt de actieve eenheid de configuratie in het actieve geheugen naar de stand-by unit. Als de configuratie gesynchroniseerd is, **beginnen de berichten met configuratie replicatie: Verzenden naar partner- en end-of-end configuratie replicatie om te paren** verschijnt op de actieve eenheidconsole. **Opmerking:** Geef eerst de **failover**-opdracht op het primaire apparaat uit en geef deze dan op het secundaire apparaat uit. Nadat u de opdracht failover op het secundaire apparaat geeft, trekt het secundaire apparaat onmiddellijk de configuratie van het primaire apparaat terug en stelt zichzelf in als *stand-by*. De primaire ASA blijft omhoog en passeert normaal verkeer en tekent zichzelf als het *actieve* apparaat. Vanaf dat punt op, wanneer een storing op het actieve apparaat optreedt, komt het stand-by apparaat op als actief.

5. Nadat de actieve configuratie replicatie heeft voltooid, voer deze opdracht in om de configuratie in Flash geheugen op te slaan:

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

6. Indien nodig, forceer elke overnamegroep die actief is op de primaire in de actieve staat op de secundaire eenheid. Om een overnamegroep te dwingen om actief te worden op de secundaire eenheid, voer deze opdracht in de ruimte van de systeemuitvoering op de primaire eenheid in:

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

Het group_id argument specificeert de groep die u actief wilt worden op de secundaire eenheid.

[Configuraties](#)

Dit document gebruikt deze configuraties:

Primaire PIX

```
PIX1(config)#show running-config
: Saved
:
PIX Version 7.2(2) <system>
!
hostname PIX1
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 PIX/ASA. 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
!--- Command to enable the LAN based failover failover
lan enable
!--- 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

```

N.B.: Raadpleeg het gedeelte **Configuration** Cable-gebaseerde failover Configuration, [PIX1 - Context1 Configuration](#) en [PIX1 - Context2 Configuration](#) voor contextconfiguratie in een LAN-gebaseerd failover-scenario.

Secundaire PIX

```

PIX2#show running-config

failover
failover lan unit secondary
failover lan interface LANFailover Ethernet3
failover lan enable
failover key *****
failover interface ip LANFailover 10.1.0.1 255.255.255.0
standby 10.1.0.2

```

Verifiëren

Gebruik van de overnameverdracht van de show

In dit gedeelte wordt de opdrachtoutput **getoond**. Op elke eenheid kunt u de overnamestatus controleren met de opdracht **failover**.

Primaire PIX

```

PIX1(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(2), Mate 7.2(2)
Group 1 last failover at: 06:12:45 UTC Apr 16 2007
Group 2 last failover at: 06:12:43 UTC Apr 16 2007

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

Secundaire PIX

PIX1(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(2), Mate 7.2(2)

Group 1 last failover at: 06:12:46 UTC Apr 16 2007
Group 2 last failover at: 06:12:41 UTC Apr 16 2007

```
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
```

Gebruik de opdracht **status** failover om de staat te controleren.

Primaire PIX

```
PIX1(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
```

Secundaire eenheid

```
PIX1(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
```

Om de IP-adressen van de failover-unit te controleren, gebruikt u de **show failover**-interface.

Primaire eenheid

```
PIX1(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
```

Secundaire eenheid

```
PIX1(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
```

[Beeld van gemonitorde interfaces](#)

Zo ziet u de status van gecontroleerde interfaces: In één contextmodus voert u de opdracht `monitor-interface` in de mondiale configuratiemodus in. In meerdere context modus, voer de `show monitor-interface` in binnen een context.

Opmerking: Gebruik de opdracht `monitor-interface` om in de configuratie van de configuratie de gezondheid op een specifieke interface te bewaken:

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

Primaire PIX

```
PIX1/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
```

Secundaire PIX

```
PIX1/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
```

Opmerking: Als u geen IP-adres voor failover invoert, geeft de opdracht **failover 0.0.0.0** voor het IP-adres weer en wordt de interface in de status "wachten" gevolgd. U moet een IP-adres voor failover instellen om te kunnen werken. Voor meer informatie over verschillende staten voor failover, raadpleeg [failover](#) te [tonen](#).

Standaard is de bewaking van fysieke interfaces ingeschakeld en is de bewaking van subinterfaces uitgeschakeld.

[De failover-opdrachten in de draaiende configuratie weergeven](#)

Ga deze opdracht in om de overvalopdrachten in de actieve configuratie te bekijken:

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

Alle **failover**-opdrachten worden weergegeven. Op eenheden die in meerdere context mode lopen, voer de **show in werking stellen-in-configuratie** opdracht in in de ruimte van de systeemuitvoering in. Voer de **show in werking stellen-configuratie alle** opdracht voor failover in om de failoveropdrachten in de actieve configuratie te tonen en neem opdrachten op waarvoor u de standaardwaarde niet hebt gewijzigd.

[Functionaliteitstests](#)

Voer de volgende stappen uit om de functionaliteit voor een failover te testen:

1. Test dat uw actieve eenheid of de failovergroep verkeer zoals verwacht met FTP overbrengt (bijvoorbeeld) om een bestand tussen hosts op verschillende interfaces te verzenden.
2. Forceer een failover naar de standby unit met deze opdracht: Voor Active/Active failover voert u de volgende opdracht in op de unit waar de failover-groep die de interface bevat die uw hosts aansluit, actief is:

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

3. Gebruik FTP om een ander bestand tussen dezelfde twee hosts te verzenden.
4. Als de test geen succes was, voer de **show failover opdracht** in om de failover status te controleren.
5. Als u klaar bent, kunt u met deze opdracht de eenheid of de failover-groep terugzetten naar de actieve status: Voor Active/Active failover voert u de volgende opdracht in op de unit waar

de failover-groep die de interface bevat die uw hosts aansluit, actief is:

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

Gedwongen failover

Voer een van deze opdrachten in om de standby-unit actief te maken:

Voer deze opdracht in de ruimte voor systeemuitleiding van de eenheid in waar de overnamegroep in de stand-by staat staat:

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

Of voer deze opdracht in de ruimte voor systeemuitleiding van de eenheid in waar de overnamegroep in de actieve staat is:

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

Het invoeren van deze opdracht in de ruimte voor systeemuitleiding zorgt ervoor dat alle overvalgroepen actief worden:

```
hostname#failover active
```

Uitgeschakeld failover

Typ deze opdracht om failover uit te schakelen:

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

Als u failover op een actief/Standby paar uitschakelt, zorgt dit ervoor dat de actieve en stand-by status van elke eenheid behouden blijft totdat u opnieuw begint. De standby-unit blijft bijvoorbeeld in de stand-by modus zodat beide eenheden niet met het verkeer beginnen te werken. Zie het gedeelte [Gedwongen failover](#) voor het actief maken van de standby-unit (zelfs met uitschakeling [van](#) failover).

Als u failover op een actief/actief paar uitschakelt, zorgt dit ervoor dat de failover-groepen in de actieve status blijven op de eenheid waarop ze momenteel actief zijn, ongeacht welke eenheid ze hebben ingesteld om er de voorkeur aan te geven. De opdracht **geen** failover kan in de ruimte voor systeemuitleiding worden ingevoerd.

Herstel van een mislukte eenheid

Om een mislukte actieve/actieve overnamegroep in een onmislukte staat te herstellen, voer deze opdracht in:

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

Als u een mislukt apparaat in een niet-geannuleerde staat herstelt, wordt het niet automatisch actief; de gerestaureerde eenheden of groepen blijven in de stand-by staat tot zij actief zijn door middel van een failover (gedwongen of natuurlijk). Een uitzondering is een failover groep gevormd met de **pre-empt** opdracht. Als eerder actief was, wordt een failover-groep actief als deze is ingesteld met de voorproefopdracht en als de unit waarvoor deze heeft gefaald zijn voorkeurseenheid is.

Vervang de mislukte eenheid door een nieuwe eenheid

Volg deze stappen om een defect apparaat te vervangen door een nieuw apparaat:

1. Start de opdracht **geen failover** op de primaire eenheid. De status van de secundaire eenheid geeft aan dat de **stand-by unit niet is gedetecteerd**.
2. Koppel de primaire eenheid los en sluit de vervangende primaire eenheid aan.
3. Controleer of de vervangende eenheid dezelfde software en ASDM versie heeft als de secundaire eenheid.
4. Start deze opdrachten op de vervangende eenheid:

```
ASA(config)#failover lan unit primary
ASA(config)#failover lan interface failover Ethernet3
ASA(config)#failover interface ip failover 10.1.0.1 255.255.255.0 standby 10.1.0.2
ASA(config)#interface Ethernet3
ASA(config-if)#no shut
ASA(config-if)#exit
```

5. Sluit de vervangende primaire eenheid aan op het netwerk en voer deze opdracht uit:

```
ASA(config)#failover
```

Problemen oplossen

Wanneer een failover optreedt, sturen beide veiligheidsapparaten systeemmeldingen uit. Deze sectie omvat deze onderwerpen:

1. [failover-systeemmeldingen](#)
2. [Debug Berichten](#)
3. [SNMP](#)

failover-systeemmeldingen

Het beveiligingsapparaat geeft een aantal systeemmeldingen uit met betrekking tot de failover op prioriteitsniveau 2, wat een kritieke toestand aangeeft. Om deze berichten te bekijken, raadpleegt u de [Cisco Security applicatie Logging Configuration en de System Log Messages](#) om vastlegging mogelijk te maken en de beschrijvingen van de systeemmeldingen te zien.

Opmerking: Binnen de overschakeling sluit de failover logischerwijs en brengt ze interfaces op, die syslog 41001 en 411002 berichten genereren. Dit is een normale activiteit.

Primaire Lost Failover communicatie met partner op interface_name

Dit failover-bericht wordt weergegeven als één eenheid van het failover-paar niet langer kan communiceren met de andere eenheid van het paar. Primair kan ook als secundair worden opgegeven voor de secundaire eenheid.

(Primair) Lost Failover communicatie met partner op interface_name

Controleer dat het netwerk dat is aangesloten op de gespecificeerde interface correct werkt.

Debug Berichten

Voer de opdracht **debug fover in** om meldingen te zien zuiveren. Raadpleeg de [handleiding voor Cisco security applicatie, versie 7.2](#) voor meer informatie.

N.B.: Omdat de debugging-uitvoer een hoge prioriteit krijgt in het CPU-proces, kan dit de systeemprestaties drastisch beïnvloeden. Om deze reden, gebruik de opdrachten **Debug over** om alleen problemen op te lossen of binnen sessies met technische ondersteuning van Cisco.

SNMP

Om SNMP syslogvallen voor failover te ontvangen, moet u de SNMP-agent configureren om SNMP-traps naar SNMP-beheerstations te verzenden, een syslog-host definiëren en de Cisco Slug MIB in uw SNMP-beheerstation compileren. Raadpleeg de opdrachten **voor en loggen** in de [Cisco Security Appliance, versie 7.2](#) voor meer informatie.

failover

Om de vraag van de de failliet unit en de houdtijden te specificeren, geeft u de opdracht **van de** overnameploeg in mondiale configuratiemodus uit.

De `unit msec [time]` van de `failover` vertegenwoordigt het tijdsinterval om het bestaan van de standby unit te controleren door hallo berichten te stemmen.

Op dezelfde manier vertegenwoordigt de `overslagaanheid msec [time]` de periode waarin een eenheid een hallo bericht moet ontvangen op de overnamekaart, waarna de peer unit gedeclareerd wordt om gefaald te hebben.

Raadpleeg de [overloopmodus](#) voor meer informatie.

WAARSCHUWING: Ontbreken van berichtdecryptie.

Foutbericht:

```
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
```

Dit probleem doet zich voor door de configuratie van de uitvaltoets. Om dit probleem op te lossen, verwijder de failover-toets en stel de nieuwe gedeelde toets in.

Gerelateerde informatie

- [Cisco 500 Series PIX-ondersteuningspagina](#)
- [Configuratie van firewall services module \(FWSM\)](#)
- [FWSM-failover-probleemoplossing](#)
- [Hoe failover werkt op Cisco Secure PIX-firewall](#)
- [Cisco 5500 Series ondersteuningspagina voor adaptieve security applicatie](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)