ASA/PIX: Active/stand-by failover in doorzichtige modus configureren

Inhoud

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.

De security applicatie ondersteunt twee failover-configuraties:

- Active/active-failover
- 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.

Een transparante firewall, is een Layer 2-firewall die werkt als een *bump in de draad*, of een *onzichtbare firewall*, en wordt niet gezien als een router op aangesloten apparaten. Dit security apparaat sluit hetzelfde netwerk aan op de binnen- en buitenkant van het apparaat. Omdat de firewall geen routed hop is, kunt u gemakkelijk een transparante firewall in een bestaand netwerk introduceren; het is niet nodig IP opnieuw aan te passen . U kunt het adaptieve security apparaat instellen om in de standaard routed firewallmodus of de transparante firewallmodus te werken. Wanneer u de modi verandert, wordt de configuratie van het adaptieve security apparaat geannuleerd omdat veel opdrachten in beide modi niet worden ondersteund. Als u al een dichtbevolkte configuratie hebt, dient u een back-up van deze configuratie te maken voordat u de modus wijzigt. u kunt deze back-upconfiguratie gebruiken als referentie wanneer u een nieuwe configuratie maakt. Raadpleeg het voorbeeld Transparent Firewall Configuration voor meer informatie over de configuratie van het firewallapparaat in Transparent-modus.

Dit document concentreert zich op de manier waarop u een actieve/Standby failover in Transparent Mode op de ASA Security Appliance kunt configureren.

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

Cisco raadt u aan de beheerinterface niet te gebruiken voor failover, vooral voor stateful failover waarin het security apparaat voortdurend de verbindingsinformatie van het ene security apparaat naar het andere stuurt. De interface voor failover moet minstens van de zelfde capaciteit zijn als de interfaces die geregeld verkeer passeren, en terwijl de interfaces op de ASA 5540 gigabit zijn, is de beheersinterface slechts FastEthernet. De beheerinterface is alleen ontworpen voor beheerverkeer en wordt gespecificeerd als Management 0/0. Maar u kunt de **alleen-beheeropdracht** gebruiken om elke interface te configureren als een alleen-beheerinterface. Bovendien kunt u voor Management 0/0 de beheermodus alleen uitschakelen zodat de interface net als elke andere interface door het verkeer kan bladeren. Raadpleeg de handleiding voor Cisco security applicatie, versie 8.0 voor meer informatie over de opdracht **alleen** voor **beheer**.

Deze configuratiehandleiding biedt een voorbeeldconfiguratie die een korte introductie in de PIX/ASA 7.x Active/Standby technologie moet bevatten. Raadpleeg de ASA/PIX-opdrachtreferentie voor een grondiger betekenis van de theorie achter deze technologie.

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 het gedeelte Downloads op nul voor failover's van *Cisco Security Appliance Opdracht Line Guide, versie 8.0* voor meer informatie over het upgraden van de software op een failover-paar.

Licentievereisten

Op het ASA security apparaat platform moet ten minste één van de eenheden een **onbeperkte (UR) licentie** hebben.

Opmerking: het kan nodig zijn om de licenties op een failover-paar te verbeteren om extra functies en voordelen te verkrijgen. Raadpleeg Licentietoetsen op een failover-paneel voor meer

informatie.

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

Gebruikte componenten

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

- ASA security applicatie, versie 7.x 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:

- PIX security applicatie met 7.x versie en hoger

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Active/stand-by failover

In deze sectie worden de volgende onderwerpen beschreven:

Active/stand-by failover-Overzicht

Met Active/Standby Failover kunt u een stand-by security apparaat gebruiken om de functionaliteit van een defecte unit over te nemen. Als de actieve eenheid faalt, verandert deze in de stand-by status terwijl de stand-by unit in de actieve toestand verandert. De eenheid die actief wordt veronderstelt de IP adressen, of, voor een transparante firewall, het beheer IP adres, en MAC adressen van de mislukte eenheid en begint verkeer door te geven. De eenheid die nu in standby staat is neemt de standby IP-adressen en MAC-adressen over. Omdat netwerkapparaten geen verandering in de MAC aan IP adresbedrading zien, veranderen geen ARP ingangen of tijd overal in het netwerk.

N.B.: Voor de multi-context-modus kan het security apparaat niet functioneren in de gehele eenheid, waartoe alle contexten behoren, maar kan het niet afzonderlijk bij afzonderlijke contexten

afleveren.

Primaire/secundaire status en actieve/stand-by status

De belangrijkste verschillen tussen de twee eenheden in een failover-paar zijn gerelateerd aan welke eenheid actief is en welke eenheid stand-by is, namelijk welke IP-adressen moet worden gebruikt en welke eenheid primair is en actief verkeer doorgeeft.

Er zijn een paar verschillen tussen de eenheden op basis waarvan de unit primair is, zoals gespecificeerd in de configuratie, en de eenheid secundair is:

- De primaire eenheid wordt altijd de actieve eenheid als beide eenheden tegelijkertijd starten (en dezelfde operationele gezondheid hebben).
- Het primaire adres van eenheid MAC is altijd gekoppeld aan de actieve IP adressen. De uitzondering op deze regel komt voor wanneer de secundaire eenheid actief is en niet het primaire adres van MAC over de failover verbinding kan verkrijgen. In dit geval, wordt het secundaire adres van MAC gebruikt.

Synchronisatie met apparaatinitialisatie en configuratie

De synchronisatie van de configuratie vindt plaats wanneer een of beide apparaten in de failover paar worden opgestart. Configuraties worden altijd gesynchroniseerd vanaf de actieve eenheid naar de standby-unit. Wanneer de standby-unit zijn eerste start heeft voltooid, wordt de actieve configuratie gewist, behalve de failover-opdrachten die nodig zijn om met de actieve unit te communiceren, en de actieve unit de gehele configuratie naar de standby-unit stuurt.

De actieve eenheid wordt bepaald door:

- Als een unit start en een peer die al actief is herkent, wordt deze de stand-by unit.
- Als een unit opstart en geen peer detecteert, wordt deze de actieve eenheid.
- Als beide eenheden tegelijkertijd starten, wordt de primaire eenheid de actieve eenheid en wordt de secundaire eenheid de stand-by eenheid.

Opmerking: Als de secundaire eenheid opstart en de primaire eenheid niet detecteert, wordt deze de actieve eenheid. Het gebruikt zijn eigen MAC-adressen voor de actieve IP-adressen. Wanneer de primaire eenheid beschikbaar wordt, verandert de secundaire eenheid de MAC adressen aan die van de primaire eenheid, die een verstoring in uw netwerkverkeer kan veroorzaken. Om dit te vermijden, moet u het failoverpaar met virtuele MAC-adressen configureren. Zie het gedeelte Active/Standby-failover van dit document configureren voor meer informatie.

Wanneer de replicatie wordt gestart, wordt met de veiligheidswasmachineconnector op de actieve eenheid de bericht `beginconfiguratie-replicatie` weergegeven: `Verzenden naar paren`, en na voltooiing van het programma, geeft het security apparaat de bericht-`end configuratie replicatie weer om te paren.` Binnen de replicatie kunnen opdrachten die op de actieve unit zijn ingevoerd, niet correct naar de standby-unit worden gerepliceerd, en kunnen opdrachten die op de standby-unit zijn ingevoerd, worden overschreven door de configuratie die vanuit de actieve unit wordt gerepliceerd. Voer geen opdrachten in op een van beide eenheden in het failover-paar in het configuratie-replicatieproces. Afhankelijk van de grootte van de configuratie kan het reproduceren van een paar seconden tot een aantal minuten duren.

Vanuit de secundaire eenheid kunt u het replicatiebericht observeren naarmate het synchroniseert vanaf de primaire eenheid:

```
ASA> .

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

ASA>
```

Op de standby-unit bestaat de configuratie alleen in actief geheugen. Om de configuratie in het geheugen van Flash op te slaan na synchronisatie, voert u deze opdrachten in:

- Voor één contextmodus, voer de **kopie in in werking gestelde-configuratie opstartende-**configuratie opdracht op de actieve eenheid. De opdracht wordt gerepliceerd naar de standby-unit, die vervolgens de configuratie naar Flash-geheugen schrijft.
- Voor de meerdere contextmodus, voer het **van in werking stellen-beslist-in-**diskette **exemplaar** op de actieve eenheid van de ruimte van de systeemuitvoering en van binnen elke context op schijf in. De opdracht wordt gerepliceerd naar de standby-unit, die vervolgens de configuratie naar Flash-geheugen schrijft. Contacten met opstartconfiguraties op externe servers zijn toegankelijk vanuit beide eenheden via het netwerk en hoeven niet afzonderlijk te worden opgeslagen voor elke eenheid. U kunt de contexten op schijf ook kopiëren van de actieve eenheid naar een externe server en ze vervolgens kopiëren naar schijf op de standby-unit, waar ze beschikbaar komen wanneer de unit opnieuw wordt geladen.

Opdrachtreplicatie

Opdrachtreplicatie stroomt altijd van de actieve eenheid naar de stand-by eenheid. Aangezien er opdrachten op de actieve eenheid worden ingevoerd, worden deze via de failover-link naar de standby-unit verzonden. U hoeft de actieve configuratie niet in het Flash-geheugen op te slaan om de opdrachten te herhalen.

Opmerking: Wijzigingen die op de standby-unit zijn aangebracht, worden niet overgenomen in de actieve unit. Als u een opdracht op de standby-unit invoert, geeft het beveiligingsapparaat het bericht `*** WAARSCHUWING *** Configuration-replicatie NIET uit de standby-unit naar de actieve unit.` Configuraties worden niet langer gesynchroniseerd. Dit bericht wordt weergegeven zelfs als u opdrachten invoert die de configuratie niet beïnvloeden.

Als u de opdracht **schrijfstand** op de actieve eenheid invoert, wordt de standby-unit uitgeschakeld, behalve de standaardinstellingen voor de failover die worden gebruikt om met de actieve eenheid te communiceren, en de actieve eenheid stuurt de gehele configuratie naar de standby-unit.

In de modus voor meerdere context worden alle contexten, wanneer u de opdracht **schrijfstand** in de ruimte voor systeemuitvoering invoert, herhaald. Als u de schrijfstandby opdracht binnen een context invoert, repliceert de opdracht alleen de contextconfiguratie.

Opdrachten met replicatie worden opgeslagen in de actieve configuratie. Voer de volgende opdrachten in om de vervolgde opdrachten in het Flash-geheugen op de standby-unit op te slaan:

- Voor één contextmodus, voer de **kopie in in werking gestelde-configuratie opstartende-**configuratie opdracht op de actieve eenheid. De opdracht wordt gerepliceerd naar de standby-unit, die vervolgens de configuratie naar Flash-geheugen schrijft.
- Voor de meerdere contextmodus, voer het **van in werking stellen-beslist-in-**diskette **exemplaar** op de actieve eenheid van de ruimte van de systeemuitvoering en binnen elke context op

schijf in. De opdracht wordt gerepliceerd naar de standby-unit, die vervolgens de configuratie naar Flash-geheugen schrijft. Contacten met opstartconfiguraties op externe servers zijn toegankelijk vanuit beide eenheden via het netwerk en hoeven niet afzonderlijk te worden opgeslagen voor elke eenheid. U kunt de contexten op schijf ook van de actieve eenheid naar een externe server kopiëren en ze vervolgens op schijf op de standby-unit kopiëren.

failover-triggers

De eenheid kan falen als een van deze gebeurtenissen optreedt:

- De eenheid heeft een hardwarestoring of een stroomuitval.
- De eenheid heeft een softwarestoring.
- Teveel gecontroleerde interfaces falen.
- De opdracht **no failover actief** is in de actieve eenheid ingevoerd, of de opdracht **failover actief** wordt ingevoerd in de standby unit.

failover-acties

Bij Active/Standby Failover doet zich failover voor op basis van een eenheid. Zelfs op systemen die in meerdere context mode lopen, kunt u geen individuele of groepen van contexten overslaan.

Deze tabel toont de overnameactie voor elke mislukkingsgebeurtenis. Voor elke mislukkingsgebeurtenis toont de tabel het overnamebeleid (failover of geen failover), de actie die door de actieve eenheid is ondernomen, de actie die door de standby-eenheid is ondernomen en alle speciale opmerkingen over de overnametoestand en de acties. De tabel toont het overnamegedrag.

gebeurtenis	Beleidsbeleid	Actief optreden	Standby Actie	Opmerkingen
Actieve eenheid mislukt (stroom of hardware)	failover	N.v.t.	Word actief; markering actief als mislukt	Geen hallo-berichten worden ontvangen op om het even welke gemonitorde interface of de overvalverbinding.
Voorheen actieve eenheid herstelt	Geen failover	Word stand-by	Geen actie	None
Standby-eenheid mislukt (stroom of hardware)	Geen failover	Mark standby is mislukt	N.v.t.	Wanneer de standby-unit is gemarkeerd als faalt, probeert de actieve unit geen failover,

				zelfs als de drempel voor interfacestoorn is wordt overschreden.
Een failover-link is niet actief	Geen failover	Fout bij opnemen van failover-interface	Fout bij opnemen van failover-interface	U moet de failover-link zo snel mogelijk herstellen omdat de unit niet kan uitvallen op de standby-unit terwijl de failover-link is uitgevallen.
failover-link mislukt bij opstarten	Geen failover	Fout bij opnemen van failover-interface	Word actief	Als de failover link bij opstarten is, worden 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.
Interfacefout actieve eenheid boven drempelwaarde	failover	Mark actief als mislukt	Word actief	None
Interfacefout bij standby-eenheid boven drempelwaarde	Geen failover	Geen actie	Mark standby is mislukt	Wanneer de standby-unit is gemarkeerd als defect, probeert de actieve unit niet te falen, zelfs niet als de interface-storingsdrempel is overschreden.

Regelmatige en stateful failover

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

Regelmatige failover

Wanneer een failover optreedt, worden alle actieve verbindingen verbroken. Clients moeten de verbindingen herstellen 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 verbindingsinformatie 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-verbindingsstaten
- De UDP-verbindingsstaten
- De ARP-tabel
- De Layer 2-bridge-tabel (alleen wanneer de Firewall in de **transparante** firewallmodus draait)
- De HTTP-verbindingsstaten (als HTTP-replicatie is ingeschakeld)
- De tabel ISAKMP en IPSec SA
- De GTP PDP-verbindingsdatabase

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

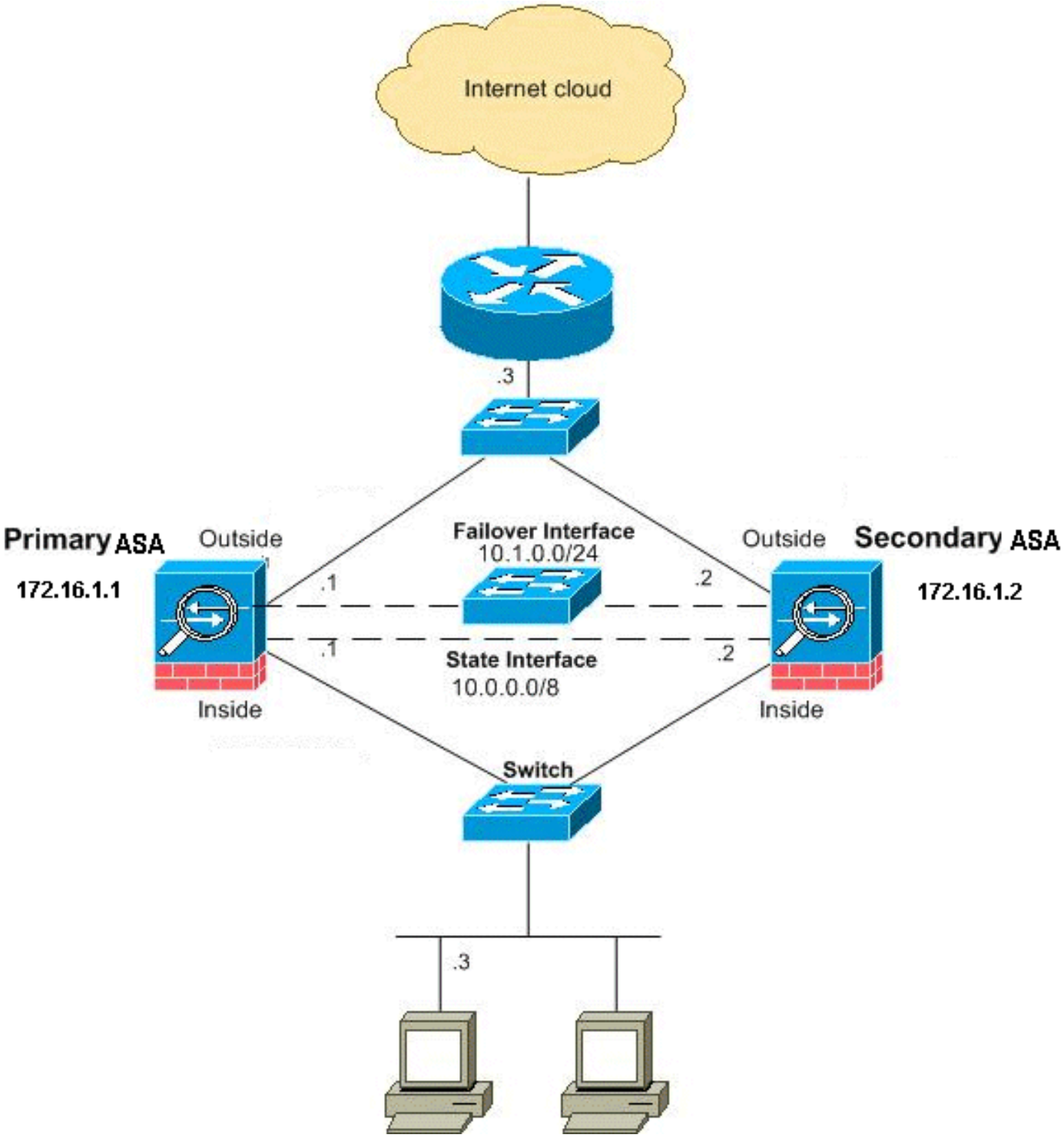
- De HTTP-verbindingstabel (tenzij HTTP-replicatie is ingeschakeld)
- De gebruikershandleiding (Uauth)
- De routingtabellen
- Staatsinformatie voor veiligheidsservicemodules

OPMERKING: Als failover optreedt binnen een actieve Cisco IP SoftPhone-sessie, blijft de oproep actief omdat de informatie over de gesprekssessie wordt gerepliceerd naar de standby-unit. Wanneer de vraag wordt beëindigd, verliest de IP SoftPhone client verbinding met Cisco CallManager. 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 Cisco CallManager binnen een bepaalde tijdsperiode ontvangt, beschouwt de client Cisco CallManager als onbereikbaar en ongeregistreerd zelf.

LAN-gebaseerde actieve/standby-failover-configuratie

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



In dit gedeelte wordt beschreven hoe u Active/Standby failover in Transparent-modus kunt configureren met een Ethernet-overnameverbinding. Wanneer u LAN-gebaseerde failover configureren 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.

N.B.: Als u van op kabel gebaseerde failover naar op LAN gebaseerde failover verandert, kunt u veel stappen overslaan, zoals de toewijzing van de actieve en standby IP adressen voor elke interface, die u voor de op kabel gebaseerde configuratie van failover hebt ingevuld.

Configuratie van primaire eenheid

Voltooi deze stappen om de primaire eenheid te configureren in een op LAN gebaseerde, actieve/STANDBY-configuratie. Deze stappen bieden de minimale configuratie die nodig is om failover op de primaire eenheid mogelijk te maken. Voor de multi-context-modus worden alle stappen uitgevoerd in de ruimte voor de uitvoering van het systeem, tenzij anders aangegeven.

Voltooi de volgende stappen om de primaire eenheid in een Active/Standby failover-paar te configureren:

1. Als u dit nog niet gedaan hebt, moet u de actieve en standby IP-adressen van de beheerinterface (transparante modus) configureren. 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.**N.B.:** Configureer geen IP-adres voor de stateful failover-link als u een speciale stateful failover-interface gebruikt. U gebruikt de opdracht **IP-interface voor** failover om in een latere stap een speciale stateful failover-interface te configureren.
   ```
   hostname(config-if)#ip address active_addr netmask
                          standby standby_addr
   ```

   In tegenstelling tot routed Mode, dat een IP-adres voor elke interface vereist, heeft een transparante firewall een IP-adres dat aan het gehele apparaat is toegewezen. Het security apparaat gebruikt dit IP-adres als het bronadres voor pakketten die op het security apparaat worden geleverd, zoals systeemmeldingen of AAA-communicatie. In het voorbeeld wordt het IP-adres voor de primaire ASA geconfigureerd zoals hieronder wordt getoond:
   ```
   hostname(config)#ip address 172.16.1.1 255.255.0.0 standby 172.16.1.2
   ```

   Hier wordt 172.16.1.1 gebruikt voor de primaire eenheid en 172.16.1.2 wijst de secundaire (standby) eenheid aan.**Opmerking:** In de multi-context modus, moet u de interface-adressen vanuit elke context configureren. Gebruik de opdracht Omzetten context om tussen de contexten te switches. De opdracht prompt verandert in `hostname/context (configuratie-als)#`, waar context de naam van de huidige context is.
2. (PIX-beveiligingsapparaat alleen) Schakel de LAN-gebaseerde failover in.
   ```
   hostname(config)#failover lan enable
   ```

3. Wijs de eenheid als primaire eenheid aan.
   ```
   hostname(config)#failover lan unit primary
   ```

4. Defineert de failover-interface.Specificeer de interface die als de failover-interface moet worden gebruikt.
   ```
   hostname(config)#failover lan interface if_name phy_if
   ```

   In deze documentatie, wordt "failover" (interfacenaam voor Ethernet0) gebruikt voor een overnameninterface.
   ```
   hostname(config)#failover lan interface failover Ethernet3
   ```

   Het *if_name* argument wijst een naam toe aan de interface opgegeven door het *phy_if* argument. Het *phy_if* argument kan de fysieke port naam zijn, zoals Ethernet1, of een eerder gecreëerd subinterface, zoals Ethernet0/2.3.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
   ```

In deze documentatie, om de failover link te configureren wordt 10.1.0.1 gebruikt voor active, 10.1.0.2 voor de standby unit, en "failover" is een interfacenaam van Ethernet0.

```
hostname(config)#failover interface ip failover 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 adressubmasker niet te identificeren.Het IP-adres voor de failover-verbinding en het MAC-adres veranderen niet bij failover. Het actieve IP-adres voor de failover-verbinding blijft altijd bij de primaire eenheid, terwijl het standby IP-adres bij de secundaire eenheid blijft.De interface inschakelen

```
hostname(config)#interface phy_if

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

In het voorbeeld wordt Ethernet3 gebruikt voor failover:

```
hostname(config)#interface ethernet3

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

5. (Optioneel) configureren de stateful failover-verbinding om stateful inspection in te schakelen.Specificeer de interface die als stateful failover-link moet worden gebruikt.

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

Dit voorbeeld gebruikte "state" als een interfacenaam voor Ethernet2 om de informatie van de de staat van de failoverlink te ruilen:

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

Opmerking: Als de stateful failover link de failover link of een data interface gebruikt, hoeft u alleen het *if_name* ***argument*** te leveren.Het argument *if_name* wijst een logische naam toe aan de interface opgegeven 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 moet niet voor een ander doel gebruikt worden, behalve, optioneel, als de failover verbinding.Wijs een actief en standby IP-adres aan de stateful failover-link toe.**Opmerking:** Als de stateful failover link de failover-link of de data-interface gebruikt, sla deze stap dan 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
```

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

```
hostname(config)#failover interface ip state 10.0.0.1 255.0.0.0
                        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.De stateful failover link IP adres en MAC adres veranderen niet bij failover tenzij ze een data interface gebruiken. 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 data-interface gebruikt, sla deze stap dan over. U hebt de interface al ingeschakeld.

```
hostname(config)#interface phy_if
```

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

Opmerking: In dit scenario wordt Ethernet2 bijvoorbeeld gebruikt voor de stateful failover-link:
```
hostname(config)#interface ethernet2

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

6. Schakel failover in.
```
hostname(config)#failover
```

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.
7. Sla de systeemconfiguratie op in het Flash-geheugen.
```
hostname(config)#copy running-config startup-config
```

Configuratie van secundaire eenheid

De enige configuratie die op de secundaire eenheid vereist is, is voor de failover-interface. De secundaire eenheid vereist dat deze opdrachten in eerste instantie met de primaire eenheid communiceren. Nadat de primaire eenheid zijn configuratie naar de secundaire eenheid stuurt, is het enige permanente verschil tussen de twee configuraties de opdracht **eenheid** voor **failover LAN**, die elke eenheid als primair of secundair identificeert.

Voor de multi-context-modus worden alle stappen uitgevoerd in de ruimte voor de uitvoering van het systeem, tenzij anders vermeld.

Voltooi de volgende stappen om de secundaire eenheid te configureren:

1. (PIX-beveiligingsapparaat alleen) Schakel een LAN-gebaseerde failover in.
```
hostname(config)#failover lan enable
```

2. Defineert de failover-interface. Gebruik dezelfde instellingen als die 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
```

   In deze documentatie, wordt Ethernet0 gebruikt voor een LAN failoverinterface.
```
hostname(config)#failover lan interface failover Ethernet3
```

   Het *if_name* argument wijst een naam toe aan de interface opgegeven door het *phy_if* argument.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
```

   In deze documentatie, om de failover link te configureren wordt 10.1.0.1 gebruikt voor active, 10.1.0.2 voor de standby unit, en "failover" is een interfacenaam van Ethernet0.
```
hostname(config)#failover interface ip failover 10.1.0.1
```

```
255.255.255.0 standby 10.1.0.2
```

N.B.: Voer deze opdracht in zoals u deze op de primaire eenheid had ingevoerd toen u de failover-interface op de primaire eenheid instelde.Schakel de interface in.

```
hostname(config)#interface phy_if

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

In dit scenario wordt bijvoorbeeld Ethernet0 gebruikt voor failover.

```
hostname(config)#interface ethernet3

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

3. (Optioneel) Wijs deze eenheid aan als secundaire eenheid.

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

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

4. Schakel failover in.

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

Opmerking: Nadat u failover hebt ingeschakeld, stuurt de actieve unit de configuratie in het actieve geheugen naar de standby-unit. Als de configuratie gesynchroniseerd is, *beginnen* de berichten *met configuratie replicatie: Verzenden naar maat-* en *end-configuratiescherm* verschijnt op de actieve console van de eenheid.

5. Nadat de actieve configuratie replicatie heeft voltooid, slaat u de configuratie op in het Flash-geheugen.

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

Configuraties

Dit document gebruikt deze configuraties:

Primaire ASA

```
ASA#show running-config
 ASA Version 7.2(3)
!
!--- To set the firewall mode to transparent mode, !---
use the firewall transparent command !--- in global
configuration mode.

firewall transparent
hostname ASA
domain-name default.domain.invalid
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0
 nameif failover

  description LAN Failover Interface
!
```

```
interface Ethernet1
 nameif inside
 security-level 100
!
interface Ethernet2
 nameif outside
 security-level 0

!--- Configure no shutdown in the stateful failover
interface !--- of both Primary and secondary ASA.

interface Ethernet3
 nameif state
 description STATE Failover Interface
!
interface Ethernet4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet5
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain.invalid
access-list 100 extended permit ip any any
pager lines 24
mtu outside 1500
mtu inside 1500

!--- Assign the IP address to the Primary and !---
Seconday ASA Security Appliance. ip address 172.16.1.1
255.255.255.0 standby 172.16.1.2

failover
failover lan unit primary
failover lan interface failover Ethernet0
failover lan enable
failover key ******
failover link state Ethernet3
failover interface ip failover 10.1.0.1 255.255.255.0
standby 10.1.0.2
failover interface ip state 10.0.0.1 255.0.0.0 standby
10.0.0.2

asdm image flash:/asdm-522.bin
no asdm history enable
arp timeout 14400
access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.3 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
```

```
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

Secundaire ASA

```
ASA#show running-config
ASA Version 7.2(3)
!
hostname ASA
domain-name default.domain.invalid
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
failover
failover lan unit secondary
failover lan interface failover Ethernet0
failover lan enable
failover key ******
failover interface ip failover 10.1.0.1 255.255.255.0
standby 10.1.0.2
```

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 ASA

```
ASA#show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: failover Ethernet0 (up)
Unit Poll frequency 200 milliseconds, holdtime 800 milliseconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 7.2(3), Mate 7.2(3)
Last Failover at: 00:08:03 UTC Jan 1 1993
        This host: Primary - Active
                Active time: 1820 (sec)
                  Interface inside (172.16.1.1): Normal
                  Interface outside (172.16.1.1): Normal
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                  Interface inside (172.16.1.2): Normal
                  Interface outside (172.16.1.2): Normal

Stateful Failover Logical Update Statistics
        Link : state Ethernet3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         185        0          183        0
        sys cmd         183        0          183        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        L2BRIDGE Tbl    2          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       7012
        Xmit Q:         0       1       185
```

Secundaire ASA

```
ASA(config)#show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Secondary
Failover LAN Interface: failover Ethernet0 (up)
Unit Poll frequency 200 milliseconds, holdtime 800 milliseconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 7.2(3), Mate 7.2(3)
Last Failover at: 16:39:12 UTC Aug 9 2009
        This host: Secondary - Standby Ready
                Active time: 0 (sec)
                  Interface inside (172.16.1.2): Normal
                  Interface outside (172.16.1.2): Normal
        Other host: Primary - Active
                Active time: 1871 (sec)
```

```
                Interface inside (172.16.1.1): Normal
                Interface outside (172.16.1.1): Normal

Stateful Failover Logical Update Statistics
        Link : state Ethernet3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         183        0          183        0
        sys cmd         183        0          183        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        L2BRIDGE Tbl    0          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       7043
        Xmit Q:         0       1       183
```

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

Primaire ASA

```
ASA#show failover state
               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  Comm Failure            00:02:36 UTC Jan 1 1993

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

Secundaire eenheid

```
ASA#show failover state
               State          Last Failure Reason      Date/Time
This host  -   Secondary
               Standby Ready  None
Other host -   Primary
               Active         None

====Configuration State===
        Sync Done - STANDBY
====Communication State===
        Mac set
```

Om de IP-adressen van de failover-unit te controleren, gebruikt u de opdracht **faalinterface**.

Primaire eenheid

```
ASA#show failover interface
        interface failover Ethernet0
                System IP Address: 10.1.0.1 255.255.255.0
                My IP Address    : 10.1.0.1
                Other IP Address : 10.1.0.2
        interface state Ethernet3
```

```
                System IP Address: 10.0.0.1 255.255.255.0
                My IP Address    : 10.0.0.1
                Other IP Address : 10.0.0.2
```

Secundaire eenheid

```
ASA#show failover interface
        interface failover Ethernet0
                System IP Address: 10.1.0.1 255.255.255.0
                My IP Address    : 10.1.0.2
                Other IP Address : 10.1.0.1
        interface state Ethernet3
                System IP Address: 10.0.0.1 255.255.255.0
                My IP Address    : 10.0.0.2
                Other IP Address : 10.0.0.1
```

Beeld van gemonitorde interfaces

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

Primaire ASA

```
ASA(config)#show monitor-interface
        This host: Primary - Active
                Interface inside (172.16.1.1): Normal
                Interface outside (172.16.1.1): Normal
        Other host: Secondary - Standby Ready
                Interface inside (172.16.1.2): Normal
                Interface outside (172.16.1.2): Normal
```

Secundaire ASA

```
ASA(config)#show monitor-interface
        This host: Secondary - Standby Ready
                Interface inside (172.16.1.2): Normal
                Interface outside (172.16.1.2): Normal
        Other host: Primary - Active
                Interface inside (172.16.1.1): Normal
                Interface outside (172.16.1.1): Normal
```

Opmerking: Als u geen IP-adres voor failover invoert, blijft de opdracht **failover** 0.0.0.0 voor het IP-adres en de interface-controle in de *wachtstand* aanwezig. Raadpleeg het gedeelte Show failover van de *Cisco Security Appliance Opdracht Referentie, versie 7.2* voor meer informatie over de verschillende failover-staten.

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 het **tonen in werking-in werking stellen-in alle** bevel **om** de failoverbevelen in de actieve

configuratie te tonen en omvat opdrachten waarvoor u de standaardwaarde niet hebt gewijzigd.

Functionaliteitstests

Voltooi deze stappen 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:Typ deze opdracht voor Active/Standby Failover in de actieve eenheid:
   ```
   hostname(config)#no failover active
   ```
3. Gebruik FTP om een ander bestand tussen dezelfde twee hosts te verzenden.
4. Als de test geen succes had, 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:Typ deze opdracht voor Active/Standby Failover in de actieve eenheid:
   ```
   hostname(config)#failover active
   ```

Gedwongen failover

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

Typ deze opdracht in de standby-unit:

```
hostname#failover active
```

Typ deze opdracht op de actieve eenheid:

```
hostname#no 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 Forcing Failover om de standby-unit actief te maken (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 systeemuitvoering worden ingevoerd.

Herstel van een mislukte eenheid

Typ deze opdracht om een mislukte eenheid in een niet-mislukte staat te herstellen:

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

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. Indien eerder actief, wordt een overnamegroep actief als deze ingesteld is met de voorproefopdracht en als de eenheid waarop deze faalt zijn voorkeurseenheid is.

Problemen oplossen

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

- failover-bewaking
- Eenheid
- %ASA-3-210005: LU wijst de verbinding niet toe
- failover-systeemmeldingen
- Debug Berichten
- SNMP
- Bekende problemen

failover-bewaking

Dit voorbeeld laat zien wat er gebeurt wanneer de failover niet is begonnen de netwerkinterfaces te controleren. Failover begint de netwerkinterfaces niet te bewaken totdat hij het tweede `hallo` pakket van de andere unit op die interface heeft gehoord. Dit duurt ongeveer 30 seconden. Als de unit is aangesloten op een netwerk-switch met Spanning Tree Protocol (STP), duurt dit twee keer de voorwaartse vertragingstijd die in de switch is ingesteld, doorgaans ingesteld op 15 seconden, plus deze 30 seconden. Dit komt doordat bij de opstart van ASA en onmiddellijk na een overvalgebeurtenis, de switch van het netwerk een tijdelijke brug lus detecteert. Bij detectie van deze lus, houdt het op om pakketten op deze interfaces voor de `voorwaartse` vertragingstijd door te sturen. Het `luistert` dan de modus voor een `voorwaartse vertragingstijd in`, waarin de switch naar bruggen luistert maar geen verkeer doorstuurt of failover `hallo` pakketten doorsturen. Na tweemaal de voorwaartse vertragingstijd (30 seconden) hervat de verkeersstroom. Elke ASA blijft in een `wachtmodus` totdat hij 30 seconden `hallo-`pakketten van de andere eenheid verneemt. Binnen de tijd dat de ASA het verkeer overdraagt, faalt het niet de andere eenheid op basis van het niet horen van de `hallo-`pakketten. Alle andere controle op failover komt nog voor, dat wil zeggen, Power, Interface Loss of Link en Failover Cable `hallo`.

Voor failover raadt Cisco sterk aan dat klanten portfast op alle switch poorten mogelijk maken die aan ASA interfaces verbinden. Bovendien moeten kanalisatie- en trunking in deze havens worden verboden. Als de interface van de ASA daalt binnen de failover, hoeft de switch niet 30 seconden te wachten terwijl de port overschakelt van een staat van luisteren naar het verzenden.

```
Failover On
Cable status: Normal
Reconnect timeout 0:00:00
This host: Primary - Active
Active time: 6930 (sec)
Interface inside (172.16.1.1): Normal (Waiting)
Interface outside (172.16.1.1): Normal (Waiting)
Other host: Secondary - Standby
Active time: 15 (sec)
Interface inside (172.16.1.2): Normal (Waiting)
Interface outside (172.16.1.2): Normal (Waiting)
```

In samenvatting, controleer deze stappen om de overnameproblemen te verminderen:

- Controleer de netwerkkabels die op de interface zijn aangesloten in de wachtende/mislukte toestand en vervang ze als het mogelijk is.
- Als er een switch is aangesloten tussen de twee eenheden, controleer of de netwerken die zijn aangesloten op de interface in de wachtende/mislukte status correct functioneren.
- Controleer de poort van de switch die op de interface is aangesloten in de wachtende/mislukte toestand en gebruik, als dit mogelijk is, de andere FE-poort op de switch.
- Controleer of u poort hebt ingeschakeld en zowel trunking als channeling op de switch poorten hebt ingeschakeld die op de interface zijn aangesloten.

Eenheid

In dit voorbeeld heeft failover een mislukking gedetecteerd. Merk op dat interface 1 op de primaire eenheid de bron van de storing is. De eenheden zitten weer in de `wachtmodus` vanwege de storing. De mislukte eenheid heeft zichzelf uit het netwerk verwijderd (de interfaces zijn ingedrukt) en stuurt niet langer `hallo-`pakketten op het netwerk. De actieve eenheid blijft in een `wachtstaat` tot de mislukte eenheid wordt vervangen en de overvalcommunicatie opnieuw begint.

```
Failover On
Cable status: Normal
Reconnect timeout 0:00:00
This host: Primary - Standby (Failed)
Active time: 7140 (sec)
Interface inside (172.16.1.2): Normal (Waiting)
Interface outside (172.16.1.2): Failed (Waiting)
Other host: Secondary - Active
Active time: 30 (sec)
Interface inside (172.16.1.1): Normal (Waiting)
Interface outside (172.16.1.1): Normal (Waiting)
```

LU wijst de verbinding niet toe

Een geheugenprobleem bestaat mogelijk als u deze foutmelding ontvangt:

```
LU wijst de verbinding niet toe
```

Dit probleem is gedocumenteerd in Cisco bug-ID CSCte80027 (alleen geregistreerde klanten). Voer een upgrade uit van de firewall op een softwareversie waarin dit probleem is opgelost. Een aantal van de ASA-softwareversies waaronder dit bug werd gerepareerd zijn 8.2(4), 8.3(2) en 8.4(2).

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.

Debug Berichten

Voer de opdracht **debug fover in** om meldingen te zien zuiveren. Raadpleeg de Cisco Security Appliance Opdracht 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 SNMP-server** en **vastlegging** in de Cisco Security Appliance Opdracht voor meer informatie.

failover

Om de de vraag van de de failovereenheid en de houdtijden te specificeren, gebruik de opdracht **van de** overnameploeg in mondiale configuratiemodus.

De `unit msec [time]` polltime van de `failover` polltime unit msec poleert hallo-berichten om het tijdsinterval weer te geven om het bestaan van de standby-unit te controleren.

Op dezelfde manier vertegenwoordigt de `overslageenheid msec [time]` de instelling van een tijdperiode waarin een eenheid een hallo bericht moet ontvangen op de overnamekaart, waarna de peer unit wordt gefaald verklaard.

Om de opiniepeiling van de gegevensinterface te specificeren en de tijden in een Active/Standby failover-configuratie te bewaren, gebruikt u de opdracht **voor** de **failover-polltime interface** in de mondiale configuratiemodus. Om de standaardinstelling te herstellen en de houdtijden te bewaren, gebruikt u de **geen** vorm van deze opdracht.

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

Gebruik de opdracht van de **de** interface van de overvalpollinginterface om de frequentie te veranderen waarmee de hallo pakketten op gegevensinterfaces worden verzonden. Deze opdracht is alleen beschikbaar voor actieve/standby-failover. Gebruik voor actieve/actieve failover de opdracht van de **polltime interface** in de configuratie van de failovergroep in plaats van de

opdracht **van de** interface **van de** failover.

U kunt geen waarde voor **holdtime** invoeren die minder dan 5 keer de tijd voor de interfaceenquête is. Met een snellere verkiezingstijd kan het beveiligingsapparaat storingen detecteren en failover sneller activeren. Een snellere detectie kan echter onnodige overgangen veroorzaken wanneer het netwerk tijdelijk wordt geblokkeerd. Interfacetests beginnen wanneer een hallo pakket niet op de interface wordt gehoord voor meer dan de helft van de houdtijd.

U kunt in de configuratie zowel de opdrachten van de backup-peers als de interface van de failover-polltime opnemen.

Dit voorbeeld stelt de tijdfrequentie van de interfacevraag in op 500 milliseconden en de houdtijd in op 5 seconden:

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

Raadpleeg het gedeelte over uitvalopties van de *Cisco Security Appliance Opdracht Referentie, versie 7.2* voor meer informatie.

Exportcertificaat/particuliere sleutel in failover-configuratie

Het primaire apparaat repliceert automatisch de private sleutel/het certificaat aan de secundaire eenheid. Geef de opdracht **schrijfgeheugen** uit in de actieve eenheid om de configuratie, die de certificaat/privé-toets bevat, te repliceren naar de stand-by unit. Alle toetsen/certificaten op de standby-unit worden gewist en opnieuw ingevuld door de actieve eenheidsconfiguratie.

Opmerking: U mag de certificaten, sleutels en rustpunten niet handmatig importeren van het actieve apparaat en vervolgens naar het standby apparaat exporteren.

WAARSCHUWING: Ontbreken van berichtdecryptie.

Fout:

```
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.

Probleem: Failover is altijd gefaald nadat u de transparante actieve/standby meerdere modi-failover hebt geconfigureren

Failover is stabiel wanneer de interne interfaces van beide ASA's rechtstreeks zijn verbonden en externe interfaces van beide ASA rechtstreeks zijn verbonden. Maar failover is flapping wanneer een switch tussen wordt gebruikt.

Oplossing: Schakel de BPDU op de ASA interfaces uit om dit probleem op te lossen.

ASA-modules met failover

Als geavanceerde inspectie en preventie security servicesmodule (AIP-SSM) of Content Security and Control Services Module (CSC-SSM) wordt gebruikt in actieve en standby-eenheden, werkt deze onafhankelijk van de ASA in termen van failover. **De modules moeten handmatig worden geconfigureerd in actieve en standby eenheden, de failover geeft de moduleconfiguratie niet opnieuw.**

In termen van failover moeten beide ASA-eenheden die AIP-SSM of CSC-SSM-modules hebben van hetzelfde hardwaretype zijn. Bijvoorbeeld, als de primaire eenheid de ASA-SSM-10 module heeft, moet de secundaire eenheid de ASA-SSM-10 module hebben.

BF-blokkering mislukt

Fout `%PIX|ASA-3-105010: (Primair) failover-berichtblokkering mislukt`

Uitleg: Blokgeheugen was uitgeput. Dit is een tijdelijk bericht en het beveiligingsapparaat moet herstellen. *Primair* kan ook als *secundair* worden vermeld voor de secundaire eenheid.

Aanbevolen actie: Gebruik de opdracht **Show blocks** om het huidige blokgeheugen te bewaken.

Probleem met failover voor AIP-module

Als u twee ASA's in een failover-configuratie hebt en elk een AIP-SSM heeft, moet u de configuratie van AIP-SSM's handmatig repliceren. Alleen de configuratie van de ASA wordt gerepliceerd door het overnamemechanisme. AIP-SSM is niet in de failover opgenomen.

Ten eerste functioneert het AIP-SSM onafhankelijk van de ASA in termen van failover. Voor failover is alles wat nodig is vanuit een ASA-perspectief dat de AIP-modules van hetzelfde hardwaretype zijn. Verder, zoals bij een ander deel van de failover, moet de configuratie van de ASA tussen de actieve en standby sync's zijn.

De AIP's zijn in feite onafhankelijke sensoren. Er is geen uitvalmechanisme tussen de twee en ze hebben geen kennis van elkaar. Ze kunnen onafhankelijke codeversies uitvoeren. Dat wil zeggen dat ze niet hoeven te matchen, en de ASA geeft niet om de versie van code op AIP met betrekking tot failover.

ASDM start een verbinding met de AIP via de IP-beheerinterface die u in de AIP hebt ingesteld. Met andere woorden, het verbindt met de sensor, doorgaans door middel van HTTPS, wat afhangt van hoe je de sensor instelt.

U zou een failover van de ASA onafhankelijk van de IPS (AIP) modules kunnen hebben. U bent nog steeds verbonden met dezelfde applicatie omdat u verbinding maakt met de IP-beheersoftware. Om aan te sluiten op andere AIP, moet u opnieuw aan zijn beheer IP verbinden om het te configureren en er toegang toe te hebben.

Raadpleeg ASA: Verzend netwerkverkeer van de ASA naar het AIP SSM-configuratievoorbeeld voor meer informatie en voorbeeldconfiguraties op hoe u netwerkverkeer verzenden dat door de Cisco ASA 5500 Series adaptieve security applicatie (ASA) doorgaat naar de geavanceerde inspectie en preventie security servicesmodule (AIP-SSM) (IPS)

Bekende problemen

Wanneer u probeert om toegang te krijgen tot ASDM op de secundaire ASA met versie 8.x-software en ASDM versie 6.x voor de configuratie van failover, wordt deze fout ontvangen:

```
Fout: De naam op het beveiligingscertificaat is ongeldig of komt niet overeen met de naam van de site
```

In het certificaat zijn de uitgevende instelling en de onderwerpregel het IP-adres van de *actieve* eenheid en niet het IP-adres van de *stand-by* eenheid.

In ASA versie 8.x, wordt het interne (ASDM) certificaat gerepliceerd van de actieve unit naar de standby-unit, wat de foutmelding veroorzaakt. Maar als dezelfde firewall op versie 7.x-code met 5.x ASDM draait en u probeert om toegang te krijgen tot ASDM, ontvangt u deze regelmatige veiligheidswaarschuwing:

```
Het beveiligingscertificaat heeft een geldige naam die overeenkomt met de naam van de pagina die u probeert te bekijken
```

Wanneer u het certificaat controleert, zijn de emittent en de onderwerpregel het IP-adres van de stand-by unit.

Gerelateerde informatie

- Adaptieve security applicaties van Cisco ASA 5500 Series
- Cisco PIX-firewallsoftware
- Configuratie van firewallservicesmodule (FWSM)
- FWSM-failover-probleemoplossing
- Hoe failover werkt op Cisco Secure PIX-firewall
- Technische ondersteuning en documentatie – Cisco Systems