Hoge beschikbaarheid van ZBFW configureren en probleemoplossing

Inhoud

Inleiding

Deze handleiding biedt de basisconfiguratie voor de hoge beschikbaarheid van Zone Firewall (HA) voor een actieve/stand-by instelling, evenals opdrachten voor het oplossen van problemen en gemeenschappelijke problemen die bij de functie worden gezien.

Cisco IOS® Zone-Based Firewall (ZBFW) ondersteunt HA zodat twee Cisco IOS-routers kunnen worden geconfigureerd in een actieve/standby of actieve/actieve instelling. Dit maakt redundantie mogelijk om één punt van mislukking te voorkomen.

Voorwaarden

Vereisten

U moet een release later hebben dan Cisco IOS-softwarerelease 15.2(3)T.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

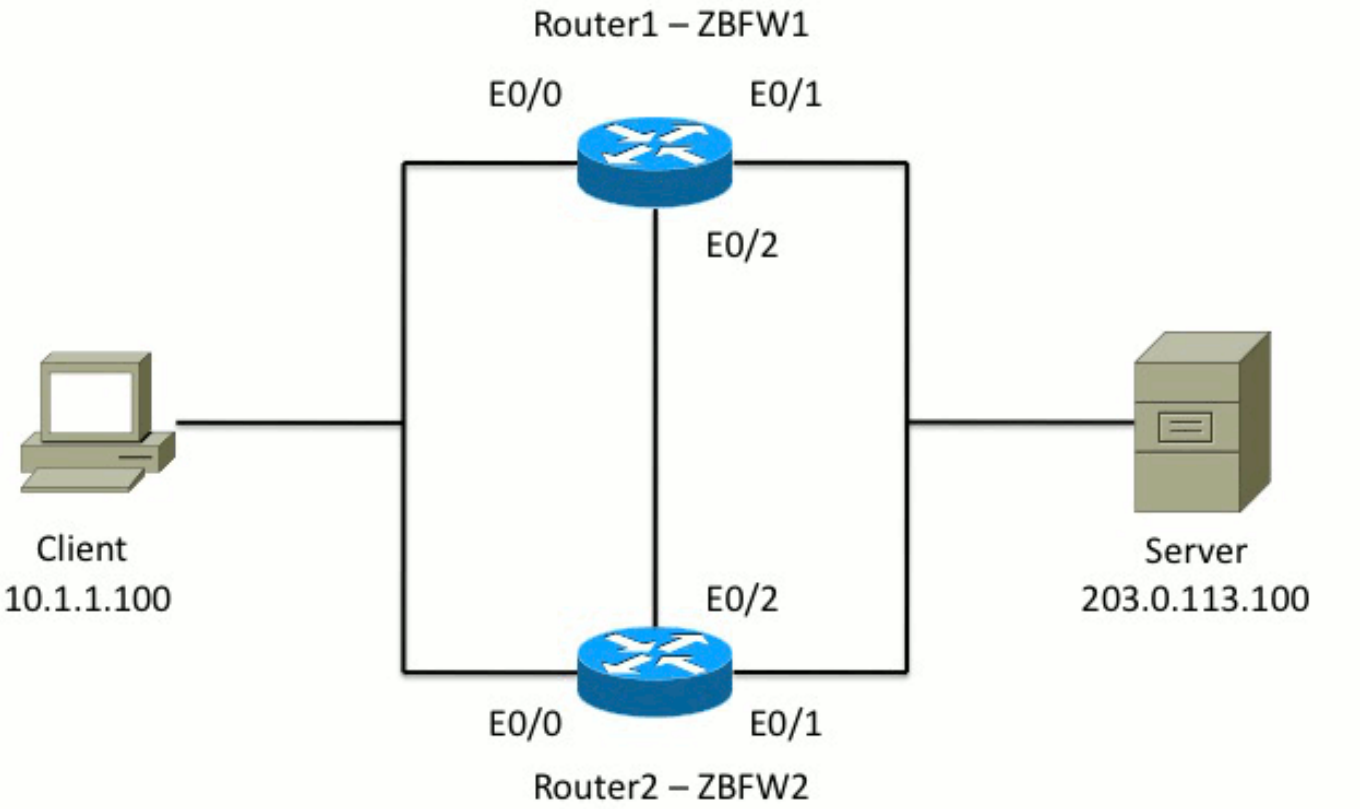
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Configureren

Dit diagram toont de topologie die in de configuratievoorbeelden wordt gebruikt.



In de configuratie die in Voorbeeld 1 wordt getoond, wordt ZBFW ingesteld om TCP-, UDP- en Internet Control Message Protocol (ICMP)-verkeer van binnenuit naar buiten te inspecteren. De in vet weergegeven configuratie stelt de HA-functie in. In Cisco IOS routers, wordt HA gevormd via de opdracht **redundantie** subconfiguratie. Om redundantie te configureren is de eerste stap redundantie in te schakelen in de global inspection parameter map.

Nadat u overtolligheid toelaat, de **toepassing** van de **overtolligheid** in subfig ingaat, en de interfaces selecteert die voor **controle** en **gegevens** worden gebruikt. De controle interface wordt gebruikt om informatie over de staat van elke router uit te wisselen. De gegevensinterface wordt gebruikt om informatie uit te wisselen over de verbindingen die moeten worden gerepliceerd.

In Voorbeeld 2, wordt de **prioriteit** opdracht ook ingesteld om router 1 de actieve eenheid in het paar te maken als zowel router 1 als router 2 operationeel zijn. De opdracht vooruitlopen (ook nader besproken in dit document) wordt gebruikt om ervoor te zorgen dat er een storing optreedt wanneer de prioriteit verandert.

De laatste stap is om de **Redundant Interface Identifier (RII)** en **Redundancy Group (RG)** aan elke interface toe te wijzen. Het **RII** groepsnummer moet uniek zijn voor elke interface, maar het moet over apparaten voor interfaces in hetzelfde net passen. De RII wordt alleen gebruikt voor de bulksync-procedure wanneer de twee routers de configuratie synchroniseren. Dit is hoe de twee routers redundante interfaces synchroniseren. De **RG** wordt gebruikt om aan te geven dat verbindingen door die interface worden gerepliceerd in de HA-verbindingstabel.

In voorbeeld 2 wordt de opdracht **redundantiegroep 1** gebruikt om een virtueel IP-adres (VIP) op de binneninterface te maken. Dit waarborgt HA, omdat alle interne gebruikers alleen met de VIP communiceren, waarvoor de actieve eenheid verwerkt.

De externe interface heeft geen RG-configuratie omdat dit de WAN-interface is. De externe interface van zowel router 1 als router 2 hoort niet bij dezelfde Internet Service Provider (ISP). Op de buiteninterface is een dynamisch routingprotocol vereist om te verzekeren dat het verkeer naar

het juiste apparaat doorgaat.

Voorbeeld 1: Router 1 Configuration Snippet (Hostname ZBFW1)

```
parameter-map type inspect global
redundancy
log dropped-packets enable
!
redundancy
application redundancy
group 1
name ZBFW_HA
preempt
priority 200
control Ethernet0/2 protocol 1
data Ethernet0/2
!
class-map type inspect match-any PROTOCOLS
match protocol tcp
match protocol udp
match protocol icmp
class-map type inspect match-all INSIDE_TO_OUTSIDE_CMAP
match class-map PROTOCOLS
match access-group name INSIDE_TO_OUTSIDE_ACL
!
policy-map type inspect INSIDE_TO_OUTSIDE_PMAP
class type inspect INSIDE_TO_OUTSIDE_CMAP
inspect
class class-default
drop
!
ip access-list extended INSIDE_TO_OUTSIDE_ACL
permit ip any any
!
zone security INSIDE
zone security OUTSIDE
zone-pair security INSIDE_TO_OUTSIDE source INSIDE destination OUTSIDE
service-policy type inspect INSIDE_TO_OUTSIDE_PMAP
!
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip nat inside
ip virtual-reassembly in
zone-member security INSIDE
redundancy rii 100
redundancy group 1 ip 10.1.1.3 exclusive
!
interface Ethernet0/1
ip address 203.0.113.1 255.255.255.0
ip nat outside
ip virtual-reassembly in
zone-member security OUTSIDE
redundancy rii 200
```

Voorbeeld 2: Router 2 Configuration Snippet (Hostname ZBFW2)

```
parameter-map type inspect global
redundancy
```

```
log dropped-packets enable
!
redundancy
application redundancy
group 1
name ZBFW_HA
preempt
priority 200
control Ethernet0/2 protocol 1
data Ethernet0/2
!
class-map type inspect match-any PROTOCOLS
match protocol tcp
match protocol udp
match protocol icmp
class-map type inspect match-all INSIDE_TO_OUTSIDE_CMAP
match class-map PROTOCOLS
match access-group name INSIDE_TO_OUTSIDE_ACL
!
policy-map type inspect INSIDE_TO_OUTSIDE_PMAP
class type inspect INSIDE_TO_OUTSIDE_CMAP
inspect
class class-default
drop
!
ip access-list extended INSIDE_TO_OUTSIDE_ACL
permit ip any any
!
zone security INSIDE
zone security OUTSIDE
zone-pair security INSIDE_TO_OUTSIDE source INSIDE destination OUTSIDE
service-policy type inspect INSIDE_TO_OUTSIDE_PMAP
!
interface Ethernet0/0
ip address 10.1.1.2 255.255.255.0
ip nat inside
ip virtual-reassembly in
zone-member security INSIDE
redundancy rii 100
redundancy group 1 ip 10.1.1.3 exclusive
!
interface Ethernet0/1
ip address 203.0.113.2 255.255.255.0
ip nat outside
ip virtual-reassembly in
zone-member security OUTSIDE
redundancy rii 200
```

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Bevestig dat apparaten met elkaar kunnen communiceren

Om te bevestigen dat de apparaten elkaar kunnen zien, moet u verifiëren dat de operationele status van de redundantie toepassingsgroep omhoog is. Zorg er vervolgens voor dat elk apparaat de juiste rol heeft genomen en zijn peer in zijn juiste rollen kan zien. In voorbeeld 3 is ZBFW1 actief en detecteert deze peer als standby. Dit wordt teruggedraaid op ZBFW2. Wanneer beide

apparaten ook tonen dat de operationele staat omhoog is, en hun peer aanwezigheid wordt gedetecteerd, kunnen de twee routers met succes over de controlelink communiceren.

Voorbeeld 3: Peer Presence-detectie

```
ZBFW1# show redundancy application group 1
Group ID:1
Group Name:ZBFW_HA

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: STANDBY
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes

RF Domain: btob-one
RF state: ACTIVE
Peer RF state: STANDBY COLD-BULK
!
ZBFW2# show redundancy application group 1
Group ID:1
Group Name:ZBFW_HA

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: STANDBY
Peer Role: ACTIVE
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes

RF Domain: btob-one
RF state: STANDBY COLD-BULK
Peer RF state: ACTIVE
```

De uitvoer in Voorbeeld 4 toont meer korreluitvoer over de controle interface van de twee routers. De output bevestigt de fysieke interface die voor controleverkeer wordt gebruikt, en het bevestigt ook het IP adres van de peer.

Voorbeeld 4: granulaat

```
ZBFW1#  show redundancy application control-interface group 1
The control interface for rg[1] is Ethernet0/2
Interface is Control interface associated with the following protocols: 1
BFD Enabled
Interface Neighbors:
Peer: 10.60.1.2 Standby RGs: 1 BFD handle: 0

ZBFW1# show redundancy application data-interface group 1
The data interface for rg[1] is Ethernet0/2
!
ZBFW2# show redundancy application control-interface group 1
The control interface for rg[1] is Ethernet0/2
Interface is Control interface associated with the following protocols: 1
BFD Enabled
```

```
Interface Neighbors:
Peer: 10.60.1.1 Active RGs: 1 BFD handle: 0

ZBFW2# show redundancy application data-interface group 1
The data interface for rg[1] is Ethernet0/2
```

Wanneer de communicatie gevestigd is, helpt de opdracht in Voorbeeld 5 u begrijpen waarom elk apparaat in zijn specifieke rol is. ZBFW1 is actief omdat het een hogere prioriteit heeft dan zijn peer. ZBFW1 heeft een prioriteit van **200**, terwijl ZBFW2 een prioriteit van **150** heeft. Deze output wordt vet gemarkeerd.

Voorbeeld 5: Rol en prioriteit

```
ZBFW1#  show redundancy application protocol group 1

RG Protocol RG 1
Role: Active
Negotiation: Enabled
Priority: 200
Protocol state: Active
Ctrl Intf(s) state: Up
Active Peer: Local
Standby Peer: address 10.60.1.2, priority 150, intf Et0/2
Log counters:
role change to active: 1
role change to standby: 0
disable events: rg down state 0, rg shut 0
ctrl intf events: up 1, down 0, admin_down 0
reload events: local request 0, peer request 0

RG Media Context for RG 1
--------------------------
Ctx State: Active
Protocol ID: 1
Media type: Default
Control Interface: Ethernet0/2
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 249, Bytes 15438, HA Seq 0, Seq Number 249, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 0
Standby Peer: Present. Hold Timer: 10000
Pkts 237, Bytes 8058, HA Seq 0, Seq Number 252, Pkt Loss 0

!
ZBFW2# show redundancy application protocol group 1

RG Protocol RG 1
------------------
Role: Standby
Negotiation: Enabled
Priority: 150
Protocol state: Standby-cold
Ctrl Intf(s) state: Up
Active Peer: address 10.60.1.1, priority 200, intf Et0/2
Standby Peer: Local
```

```
Log counters:
role change to active: 0
role change to standby: 1
disable events: rg down state 0, rg shut 0
ctrl intf events: up 1, down 0, admin_down 0
reload events: local request 0, peer request 0

RG Media Context for RG 1
--------------------------
Ctx State: Standby
Protocol ID: 1
Media type: Default
Control Interface: Ethernet0/2
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 232, Bytes 14384, HA Seq 0, Seq Number 232, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 0
Active Peer: Present. Hold Timer: 10000
Pkts 220, Bytes 7480, HA Seq 0, Seq Number 229, Pkt Loss 0
```

De laatste bevestiging is ervoor te zorgen dat de RII groep ID aan elke interface wordt toegewezen. Als u deze opdracht op beide routers invoert, controleren ze dubbel om te verzekeren dat de interfaceparen op hetzelfde net tussen apparaten dezelfde RII ID worden toegewezen. Als zij niet met dezelfde unieke RII ID zijn geconfigureerd, worden de verbindingen niet tussen de twee apparaten herhaald. Zie voorbeeld 6.

Voorbeeld 6: Bevestig dat aan RII-groep-id is toegewezen

```
ZBFW1# show redundancy rii
No. of RIIs in database: 2
Interface RII Id decrement
Ethernet0/1 : 200           0
Ethernet0/0 : 100           0
!
ZBFW2# show redundancy rii
No. of RIIs in database: 2
Interface RII Id decrement
Ethernet0/1 : 200           0
Ethernet0/0 : 100           0
```

Controleer dat verbindingen worden herhaald met de peer router

In voorbeeld 7 gaat ZBFW1 actief het verkeer voor een verbinding over. De verbinding wordt met succes gerepliceerd naar het standby apparaat ZBFW2. Om de verbindingen te bekijken die door de zone firewall zijn verwerkt, gebruikt u de opdracht **showbeleid-firewallsessie**.

Voorbeeld 7: Verwerkte verbindingen

```
ZBFW1#show policy-firewall session
Session B2704178 (10.1.1.100:52980)=>(203.0.113.100:23) tcp
```

```
SIS_OPEN/TCP_ESTAB
Created 00:00:31, Last heard 00:00:30
Bytes sent (initiator:responder) [37:79]
HA State: ACTIVE, RG ID: 1
Established Sessions = 1

ZBFW2#show policy-firewall session
Session B2601288 (10.1.1.100:52980)=>(203.0.113.100:23) tcp
SIS_OPEN/TCP_ESTAB
Created 00:00:51, Last heard never
Bytes sent (initiator:responder) [0:0]
HA State: STANDBY, RG ID: 1
Established Sessions = 1
```

Merk op dat de verbinding zich herhaalt, maar de overgedragen bytes worden niet bijgewerkt. De verbindingsstaat (TCP-informatie) wordt regelmatig bijgewerkt via de gegevensinterface om er zeker van te zijn dat verkeer niet wordt beïnvloed als er een failover-gebeurtenis optreedt.

Voor meer korreluitvoer, voer het **showbeleid-firewall sessie zone-paar *<ZP>*ha** opdracht in. Het verstrekt gelijkaardige output zoals Voorbeeld 7, maar het staat de gebruiker toe om de uitvoer tot slechts het zone-paar te beperken dat gespecificeerd wordt.

Gather Debug-uitvoer

In deze sectie worden de debug-opdrachten weergegeven die relevant worden uitgevoerd voor het oplossen van problemen met deze functie.

Inschakelen van apparaten kan zeer zwaar zijn op een drukke router. Daarom moet je de impact begrijpen voordat je ze in staat stelt.

- **debug van redundantie groepsgebeurtenis**

  Deze opdracht wordt gebruikt om ervoor te zorgen dat de aansluitingen overeenkomen met de juiste RII-groep die correct wordt herhaald. Wanneer het verkeer op ZBFW aankomt, worden de bron en de doelinterfaces gecontroleerd voor een RII groep-ID. Deze informatie wordt vervolgens verspreid via de datalink naar de peer. Wanneer de RII-groep van de stand-by peer zich uitleent op de actieve eenheden, dan wordt de syslog in Voorbeeld 8 gegenereerd en bevestigt de RII groep ID's die worden gebruikt om de verbinding te repliceren:

  Voorbeeld 8: Syslog

  ```
  debug redundancy application group rii event
  debug redundancy application group rii error
  !
  *Feb 1 21:13:01.378: [RG-RII-EVENT]: get idb: rii:100
  *Feb 1 21:13:01.378: [RG-RII-EVENT]: get idb: rii:200
  ```

- **defect redundantie en alle toepassingsprotocollen**

  Deze opdracht wordt gebruikt om te bevestigen dat de twee peers elkaar kunnen zien. Het

peer IP-adres wordt in de debugs bevestigd. Zoals in Voorbeeld 9 wordt gezien, ziet ZBFW1 zijn peer in de standby staat met IP adres **10.60.1.2**. Het omgekeerde is waar voor ZBFW2.

Voorbeeld 9: IP-peer in debugs bevestigen

```
debug redundancy application group protocol all
!
ZBFW1#
*Feb 1 21:35:58.213: RG-PRTCL-MEDIA: RG Media event, rg_id=1, role=Standby,
addr=10.60.1.2, present=exist, reload=0, intf=Et0/2, priority=150.
*Feb 1 21:35:58.213: RG-PRTCL-MEDIA: [RG 1] [Active/Active] set peer_status 0.
*Feb 1 21:35:58.213: RG-PRTCL-MEDIA: [RG 1] [Active/Active] priority_event
'media: low priority from standby', role_event 'no event'.
*Feb 1 21:35:58.213: RG-PRTCL-EVENT: [RG 1] [Active/Active] select fsm event,
priority_event=media: low priority from standby, role_event=no event.
*Feb 1 21:35:58.213: RG-PRTCL-EVENT: [RG 1] [Active/Active] process FSM event
'media: low priority from standby'.
*Feb 1 21:35:58.213: RG-PRTCL-EVENT: [RG 1] [Active/Active] no FSM transition

ZBFW2#
*Feb 1 21:36:02.283: RG-PRTCL-MEDIA: RG Media event, rg_id=1, role=Active,
addr=10.60.1.1, present=exist, reload=0, intf=Et0/2, priority=200.
*Feb 1 21:36:02.283: RG-PRTCL-MEDIA: [RG 1] [Standby/Standby-hot]
set peer_status 0.
*Feb 1 21:36:02.283: RG-PRTCL-MEDIA: [RG 1] [Standby/Standby-hot] priority_event
'media: high priority from active', role_event 'no event'.
*Feb 1 21:36:02.283: RG-PRTCL-EVENT: [RG 1] [Standby/Standby-hot] select
fsm event, priority_event=media: high priority from active, role_event=no event.
*Feb 1 21:36:02.283: RG-PRTCL-EVENT: [RG 1] [Standby/Standby-hot] process
FSM event 'media: high priority from active'.
*Feb 1 21:36:02.283: RG-PRTCL-EVENT: [RG 1] [Standby/Standby-hot] no FSM
transition
```

Veelvoorkomende problemen

In dit gedeelte worden enkele vaak voorkomende problemen beschreven.

Selectie van controle- en gegevensinterfaces

Hier zijn een aantal tips voor de controle en gegevensVLAN's:

- Neem de controle en gegevensinterfaces niet in de ZBFW-configuratie op. zij worden uitsluitend gebruikt om met elkaar te communiceren; derhalve is het niet nodig deze interfaces te beveiligen .
- De controle en gegevensinterfaces kunnen op dezelfde interface of VLAN zijn. Dit behoudt poorten op de router.

Zonder RII-groep

De RII groep moet worden toegepast op zowel de LAN als WAN-interfaces. De LAN interfaces moeten op hetzelfde net zijn gericht, maar de WAN interfaces kunnen op afzonderlijke subnetten

zijn. Als er een RII groep afwezig op een interface is, komt deze syslog voor in de uitvoer van **debug redundantie toepassingsgroep rii gebeurtenis** en **debug redundantie toepassingsgroep rii fout**:

```
000515: Dec 20 14:35:07.753 EST: FIREWALL*: RG not found for ID 0
```

Automatisch failover

Om automatische failover te configureren moet de ZBFW HA worden geconfigureerd om een SLA-object (Service Level Agreement) te volgen en de prioriteit dynamisch te verlagen op basis van deze SLA-gebeurtenis. In voorbeeld 10, volgt ZBFW HA de verbindingsstatus van de **Gigabit Ethernet0** interface. Als deze interface daalt, wordt de prioriteit verminderd zodat het peer apparaat meer favoriet is.

Voorbeeld 10: ZBFW HA-automatische failover-configuratie

```
redundancy
application redundancy
group 1
name ZBFW_HA
preempt
priority 230
control Vlan801 protocol 1
data Vlan801
track 1 decrement 200
!
track 1 interface GigabitEthernet0 line-protocol

redundancy
application redundancy
group 1
name ZBFW_HA
preempt
priority 180
control Vlan801 protocol 1
data Vlan801
```

Soms is de ZBFW HA niet automatisch failliet, zelfs al is er een lagere prioriteit gebeurtenis. Dit komt doordat het **voorproefsleutelwoord** niet bij beide apparaten is ingesteld. Het preempt sleutelwoord heeft andere functionaliteit dan in Hot Standby Router Protocol (HSRP) of Adaptieve Security Appliance (ASA) failover. In ZBFW HA, staat het **voorproefsleutelwoord** toe om een overvalgebeurtenis te voorkomen als de prioriteit van het apparaat verandert. Dit wordt gedocumenteerd in de Security Configuration Guide: Zone-Based Policy Firewall, Cisco IOS release 15.2M&T. Hier is een extract van het Zone-Based Policy Firewall High Availability-hoofdstuk:

"Een overgang naar het standby apparaat kan onder andere omstandigheden plaatsvinden. Een andere factor die een omschakeling kan veroorzaken is een prioriteitsinstelling die op elk apparaat kan worden gevormd. Het apparaat met de hoogste prioriteitswaarde is het actieve apparaat. Als er een fout optreedt op het actieve of het stand-by apparaat, wordt de prioriteit van het apparaat bepaald door een configureerbare hoeveelheid, bekend als het gewicht. Als de prioriteit van het actieve apparaat onder de prioriteit van het standby apparaat valt, treedt een omschakeling op en wordt het standby apparaat het actieve apparaat. Dit standaardgedrag kan worden gecorrigeerd door de voorkoopeigenschap voor de redundantiegroep in te schakelen. U kunt ook elke interface configureren om de prioriteit te verminderen wanneer Layer 1 status van de interface wordt

verlaagd. De prioriteit die wordt ingesteld heeft voorrang op de standaardprioriteit van een redundantiegroep."

Deze uitgangen geven de juiste toestand aan:

```
ZBFW01#show redundancy application group 1
Group ID:1
Group Name:ZBFW_HA

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: STANDBY
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes

RF Domain: btob-one
RF state: ACTIVE
Peer RF state: STANDBY HOT

ZBFW01#show redundancy application faults group 1
Faults states Group 1 info:
Runtime priority: [230]
RG Faults RG State: Up.
Total # of switchovers due to faults: 0
Total # of down/up state changes due to faults: 0
```

Deze logbestanden worden op de ZBFW gegenereerd zonder dat de debugs zijn ingeschakeld. Dit logbestand toont aan wanneer het apparaat actief wordt:

```
*Feb  1 21:47:00.579: %RG_PROTOCOL-5-ROLECHANGE: RG id 1 role change from
Init to Standby
*Feb 1 21:47:09.309: %RG_PROTOCOL-5-ROLECHANGE: RG id 1 role change from Standby
to Active
*Feb 1 21:47:19.451: %RG_VP-6-BULK_SYNC_DONE: RG group 1 BULK SYNC to standby
complete.
*Feb 1 21:47:19.456: %RG_VP-6-STANDBY_READY: RG group 1 Standby router is in
SSO state
```

Dit logbestand toont aan wanneer het apparaat in de stand-by modus staat:

```
*Feb  1 21:47:07.696: %RG_VP-6-BULK_SYNC_DONE: RG group 1 BULK SYNC to standby
complete.
*Feb 1 21:47:07.701: %RG_VP-6-STANDBY_READY: RG group 1 Standby router is in
SSO state
*Feb 1 21:47:09.310: %RG_PROTOCOL-5-ROLECHANGE: RG id 1 role change from Active
to Init
*Feb 1 21:47:19.313: %RG_PROTOCOL-5-ROLECHANGE: RG id 1 role change from
Init to Standby
```

Asymmetric routing

Asymmetric routingondersteuning wordt gedefinieerd in de Asymmetric Routing Support-handleiding.

Om asymmetrische routing te configureren voegt u de functies toe aan zowel de redundantie applicatiegroep en de subconfiguratie van de interface. Het is belangrijk om op te merken dat

asymmetrische routing en een RG niet op dezelfde interface kunnen worden ingeschakeld, omdat deze niet wordt ondersteund. Dit is toe te schrijven aan hoe asymmetrische routing werkt. Wanneer een interface is aangewezen voor asymmetrische routing, kan het op dat punt geen deel uitmaken van HA-connectie-replicatie, omdat het routing niet consistent is. Het configureren van een RG verwart de router, omdat een RG aangeeft dat een interface deel uitmaakt van de HA-verbinding replicatie.

Voorbeeld 11: Asymmetrische routingconfiguratie

```
redundancy
application redundancy
group 1
asymmetric-routing interface Ethernet0/3

interface Ethernet0/1
redundancy asymmetric-routing enable
```

Deze configuratie moet worden toegepast op beide routers in het HA-paar.

De eerder genoemde **Ethernet0/3** interface is een nieuwe toegewijde link tussen de twee routers. Deze link wordt uitsluitend gebruikt om asymmetrisch routed-verkeer tussen de twee routers door te geven. Dit is waarom het een toegewijde link zou moeten zijn die gelijkwaardig is aan de extern gerichte interface.

Gerelateerde informatie

- Security configuratiegids: Zone-Based Policy Firewall, Cisco IOS release 15.2M&T
- Firewallconfiguratie met hoge beschikbaarheid van zone-gebaseerde beleidsfirewall
- Cisco IOS-softwarerelease 15.2M&T
- Cisco IOS Firewall
- Security-productmeldingen
- Technische ondersteuning en documentatie – Cisco Systems