Configuración de alta disponibilidad ZBFW y Nota Técnica del troubleshooting

Contenido

Introducción

Esta guía proporciona la configuración básica para la Alta disponibilidad del Firewall de la zona (HA) por una configuración activa/espera, así como los comandos de Troubleshooting, y problemas frecuentes considerados con la característica.

El ® del Cisco IOS Zona-basó los soportes HA del Firewall (ZBFW) para poder configurar dos Routers del Cisco IOS en una configuración activa/espera o activa/activa. Esto permite que la Redundancia para prevenir un solo punto de falla.

Prerrequisitos

Requisitos

Usted debe tener una versión más adelante que el Cisco IOS Software Release15.2(3)T.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

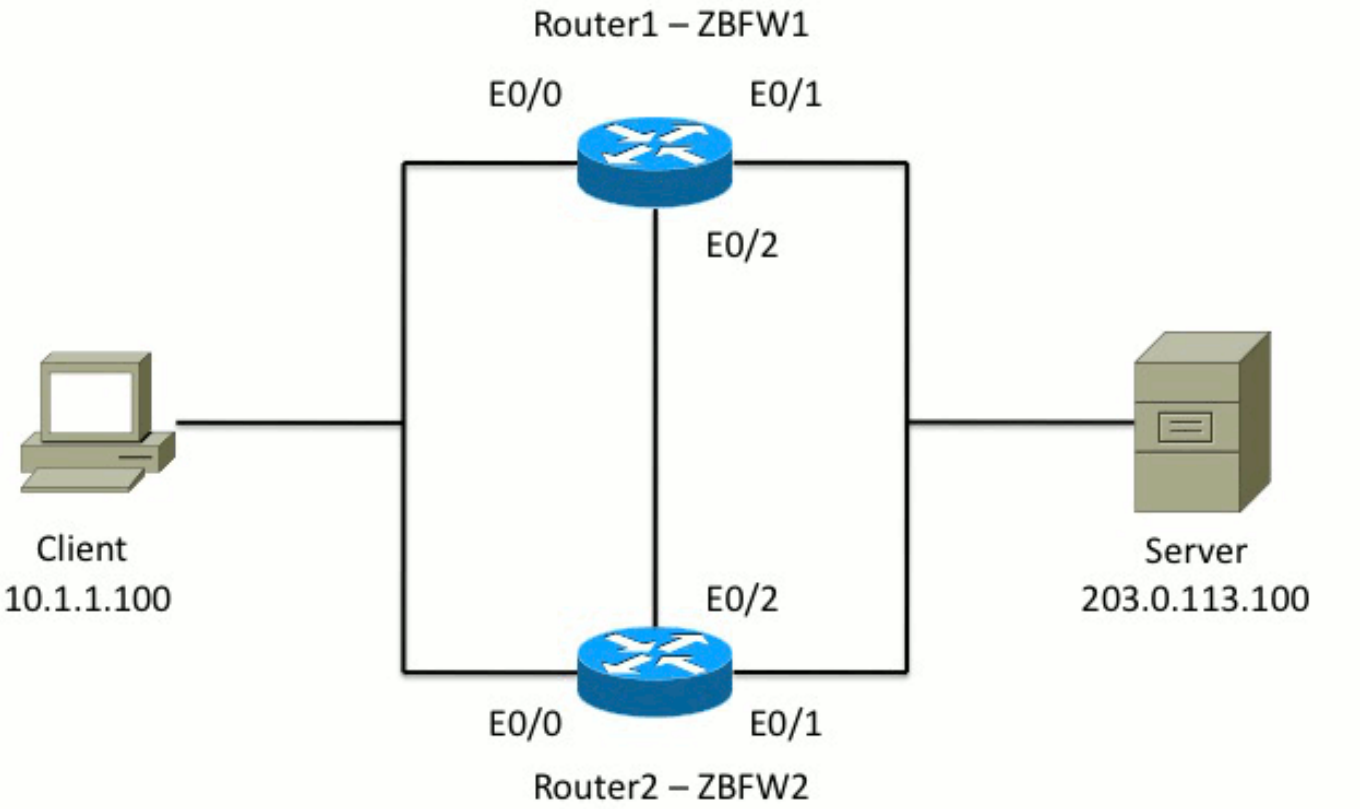
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Configurar

Este diagrama muestra la topología usada en los ejemplos de configuración.



En la configuración mostrada en el ejemplo 1, ZBFW se configura para examinar el TCP, el UDP, y el tráfico del Internet Control Message Protocol (ICMP) desde adentro al exterior. La configuración mostrada en intrépido configura la característica HA. En el Routers del Cisco IOS, el HA se configura vía el comando del subconfig de la **Redundancia**. Para configurar la Redundancia, el primer paso es habilitar la Redundancia en la correspondencia global del parámetro de inspección.

Después de que usted habilite la Redundancia, ingrese el subconfig de la **Redundancia de la aplicación**, y seleccione las interfaces que se utilizan para el **control** y los **datos**. La interfaz de control se utiliza para intercambiar la información sobre el estado de cada router. La Interfaz de datos se utiliza para intercambiar la información sobre las conexiones que deben ser replicadas.

En el ejemplo 2, fijan al **comando priority** también de hacer router1 la unidad activa en los pares si el router1 y el router2 son operativos. El comando de la **apropiación** (también discutido más lejos en este documento) se utiliza para asegurarse de que ocurre el error una vez los cambios de la prioridad.

El último paso es asignar el **identificador de la interfaz redundante (RII)** y el **grupo de redundancia (RG) a** cada interfaz. El número de grupo **RII** tiene que ser único para cada interfaz, pero debe hacer juego a través de los dispositivos para las interfaces en la misma subred. El RII se utiliza solamente para el bulto sincroniza el proceso cuando el dos Routers sincroniza la configuración. Éste es cómo el dos Routers sincroniza las interfaces redundantes. **El RG** se utiliza para indicar que las conexiones a través de esa interfaz están replicadas en la tabla de conexiones HA.

En el ejemplo 2, utilizan al **comando 1 del grupo de redundancia** para crear el direccionamiento a IP virtual (VIP) en la interfaz interior. Esto asegura el HA, porque todos los usuarios internos comunican solamente con el VIP, para el cual los procesos de unidad activa.

La interfaz exterior no tiene ninguna configuración RG porque ésta es la interfaz de WAN. La interfaz exterior de ambo router1 y el router2 no pertenecen al mismo Proveedor de servicios de

Internet (ISP). En la interfaz exterior, un Dynamic Routing Protocol se requiere para asegurarse de que el tráfico pase al dispositivo correcto.

Ejemplo 1: Fragmentos de la configuración del router1 (nombre de host 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
```

Ejemplo 2: Fragmentos de la configuración del router2 (nombre de host 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
```

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

Confirme que los dispositivos pueden comunicar con uno a

Para confirmar que los dispositivos pueden considerarse, usted debe verificar que el estado operacional del grupo de aplicaciones de la Redundancia esté para arriba. Entonces, asegúrese de que cada dispositivo haya tomado el papel correcto, y puede ver a su par en sus papeles correctos. En el ejemplo 3, ZBFW1 es activo y detecta a su par como recurso seguro. Esto se

invierte en ZBFW2. Cuando ambos dispositivos también muestran que el estado operacional está para arriba, y se detecta su presencia del par, el dos Routers puede comunicar con éxito a través del link de control.

Ejemplo 3: Detección de la presencia del par

```
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
```

La salida en una salida más granular de las demostraciones del ejemplo 4 sobre la interfaz de control del dos Routers. La salida confirma la interfaz física usada para el tráfico de control, y también confirma la dirección IP del par.

Ejemplo 4: Salida granular

```
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
```

Cuando se establece la comunicación, el comando en el ejemplo 5 le ayuda a entender porqué cada dispositivo está en su rol específico. ZBFW1 es activo porque tiene una prioridad más alta que su par. ZBFW1 tiene una prioridad de **200**, mientras que ZBFW2 tiene una prioridad de **150**. Esta salida se resalta en intrépido.

Ejemplo 5: Estatus y prioridad del papel

```
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
```

La confirmación más reciente es asegurarse de que el ID de grupo RII está asignado a cada interfaz. Si usted ingresa este comando en ambo Routers, comprueban con minuciosidad para asegurarse de que los pares de la interfaz en la misma subred entre los dispositivos están asignados el mismo RII ID. Si no se configuran con el mismo RII único ID, las conexiones no replican entre los dos dispositivos. Vea el ejemplo 6.

Ejemplo 6: Confirme el ID de grupo RII se asigna

```
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
```

Verifique que réplica de las conexiones al router del par

En el ejemplo 7, ZBFW1 pasa activamente el tráfico para una conexión. La conexión se replica con éxito al dispositivo en espera ZBFW2. Para ver las conexiones procesadas por el Firewall de la zona, utilice el **comando session del directiva-Firewall de la demostración**.

Ejemplo 7: Conexiones procesadas

```
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
```

Note que las réplicas de la conexión, sino los bytes transferidos no son actualizados. Ponen al día al estado de la conexión (información TCP) regularmente a través de la Interfaz de datos para asegurarse de que el tráfico no es afectado si ocurre un evento de falla.

Para una salida más granular, ingrese el comando de los zona-**pares *<ZP>* ha de la sesión del directiva-Firewall de la demostración**. Proporciona la salida similar como ejemplo 7, pero permite que el usuario restrinja la salida solamente a los zona-pares especificados.

Salida de los debugs del frunce

Esta sección muestra los comandos debug que producen la salida relevante para resolver problemas esta característica.

La habilitación de los debugs puede ser muy vigorosa en un router ocupado. Por lo tanto, usted debe entender el impacto antes de que usted los habilite.

- **evento del rii del grupo de aplicaciones de la Redundancia del debug**

  Este comando se utiliza para aseegurarse coincidencia de las conexiones al grupo correcto RII que se replicará correctamente. Cuando el tráfico llega en el ZBFW, la fuente y las interfaces de destino se marcan para saber si hay un ID de grupo RII. Esta información entonces se comunica a través del link de datos al par. Cuando el grupo RII del par espera alinea con las unidades activas, después el Syslog en el ejemplo 8 se genera, y confirma los ID de grupos RII que se utilizan para replicar la conexión:

  Ejemplo 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
  ```

- **protocolo todo del grupo de aplicaciones de la Redundancia del debug**

  Este comando se utiliza para confirmar que los dos pares pueden verse. El IP Address de Peer se confirma en los debugs. Como se ve en el ejemplo 9, ZBFW1 ve a su par en el estado espera con la dirección IP 10.60.1.2. El revés es verdad para ZBFW2.

  Ejemplo 9: Confirme al par IP en los debugs

  ```
  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
```

Problemas comunes

Esta sección detalla algunos problemas frecuentes se encuentren que.

Control y selección de la Interfaz de datos

Aquí están algunas extremidades para el control y los VLAN de datos:

- No incluya el control y las Interfaces de datos en la configuración ZBFW. Los utilizan solamente para comunicar con uno a; por lo tanto, no hay necesidad de asegurar estas interfaces.
- El control y las Interfaces de datos pueden estar en la misma interfaz o VLA N. Esto preserva los puertos en el router.

Grupo ausente RII

El grupo RII debe ser aplicado en el LAN y las interfaces de WAN. Las interfaces LAN deben estar en la misma subred, pero las interfaces de WAN pueden estar en las subredes distintas. Si hay un grupo RII ausente en una interfaz, este Syslog ocurre en la salida del **error del rii del evento del rii del grupo de aplicaciones de la Redundancia del debug** y del **grupo de aplicaciones de la Redundancia del debug**:

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

Falla automática

Para configurar a la falla automática, el ZBFW HA se debe configurar para seguir un objeto del Acuerdo de nivel de servicio (SLA), y disminuye dinámicamente la prioridad basada en este

evento de SLA. En el ejemplo 10, ZBFW HA sigue el estado de link de la interfaz **GigabitEthernet0**. Si va esta interfaz abajo, se reduce la prioridad de modo que el dispositivo de peer sea favorecido.

Ejemplo 10: Configuración de la falla automática ZBFW HA

```
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
```

El ZBFW HA no hace a veces automáticamente Conmutación por falla aunque hay un evento disminuido de la prioridad. Esto es porque la palabra clave de la **apropiación** no se configura bajo ambos dispositivos. La palabra clave de la **apropiación** tiene diversas funciones que en el Hot Standby Router Protocol (HSRP) o la Conmutación por falla adaptante del dispositivo de seguridad (ASA). En ZBFW HA, la palabra clave de la **apropiación** permite que un evento de falla ocurra si la prioridad del dispositivo cambia. Esto se documenta en la guía de configuración de seguridad: Firewall Zona-basado de la directiva, Cisco IOS Release 15.2M&T. Aquí está un extracto del capítulo de gran disponibilidad Zona-basado del Firewall de la directiva:

“Un intercambio al dispositivo en espera puede ocurrir bajo otras circunstancias. Otro factor que puede causar un intercambio es una Configuración de prioridad que se puede configurar en cada dispositivo. El dispositivo con el valor más prioritario sea el dispositivo activo. Si un incidente ocurre en el active o el dispositivo en espera, la prioridad del dispositivo decremented por una cantidad configurable, conocida como la ponderación. Si la prioridad del dispositivo activo baja debajo de la prioridad del dispositivo en espera, un intercambio ocurre y el dispositivo en espera se convierte en el dispositivo activo. Este comportamiento predeterminado puede ser reemplazado inhabilitando el atributo del derecho preferente de compra para el grupo de redundancia. Usted puede también configurar cada interfaz para disminuir la prioridad cuando va el estado del Layer 1 de la interfaz abajo. La prioridad se configura que reemplaza la prioridad predeterminada de un grupo de redundancia.”

Estas salidas indican el estado apropiado:

```
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
```

Estos registros se generan en el ZBFW sin ningunos debugs habilitados. Este registro muestra cuando el dispositivo llega a ser activo:

```
*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
```

Este registro muestra cuando el dispositivo va en el recurso seguro:

```
*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
```

Ruteo Asimétrico

El soporte del Asymmetric Routing outined en la guía del soporte del Asymmetric Routing.

Para configurar el Asymmetric Routing, agregue las características a la configuración global del grupo de aplicaciones de la Redundancia y a la sub-configuración de la interfaz. Es importante observar ese Asymmetric Routing y un RG no se puede habilitar en la misma interfaz, porque no se soporta. Esto es debido a cómo el Asymmetric Routing trabaja. Cuando una interfaz se señala para el Asymmetric Routing, no puede ser replicación de la conexión de la parte de HA en ese momento, porque la encaminamiento es contraria. Configurar un RG confunde al router, porque un RG especifica que una interfaz es replicación de la conexión de la parte de HA.

Ejemplo 11: Configuración del Asymmetric Routing

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

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

Esta configuración se debe aplicar en ambo Routers en los pares HA.

La interfaz **Ethernet0/3** enumerada previamente es un nuevo link dedicado entre el dos Routers. Este link se utiliza exclusivamente para pasar el tráfico asimétrico-ruteado entre el dos Routers. Esta es la razón por la cual debe ser un link dedicado equivalente a la interfaz del externo-revestimiento.

Información Relacionada

- Guía de configuración de seguridad: Firewall Zona-basado de la directiva, Cisco IOS Release 15.2M&T
- De la directiva de la guía de configuración de seguridad del Firewall Alta disponibilidad Zona-basada
- Cisco IOS 15.2M&T
- Cisco IOS Firewall
- Field Notice de seguridad del producto
- Soporte Técnico y Documentación - Cisco Systems