Solucionar problemas de asimetría de clústeres de FTD que provocan errores de conexión TCP

Problema

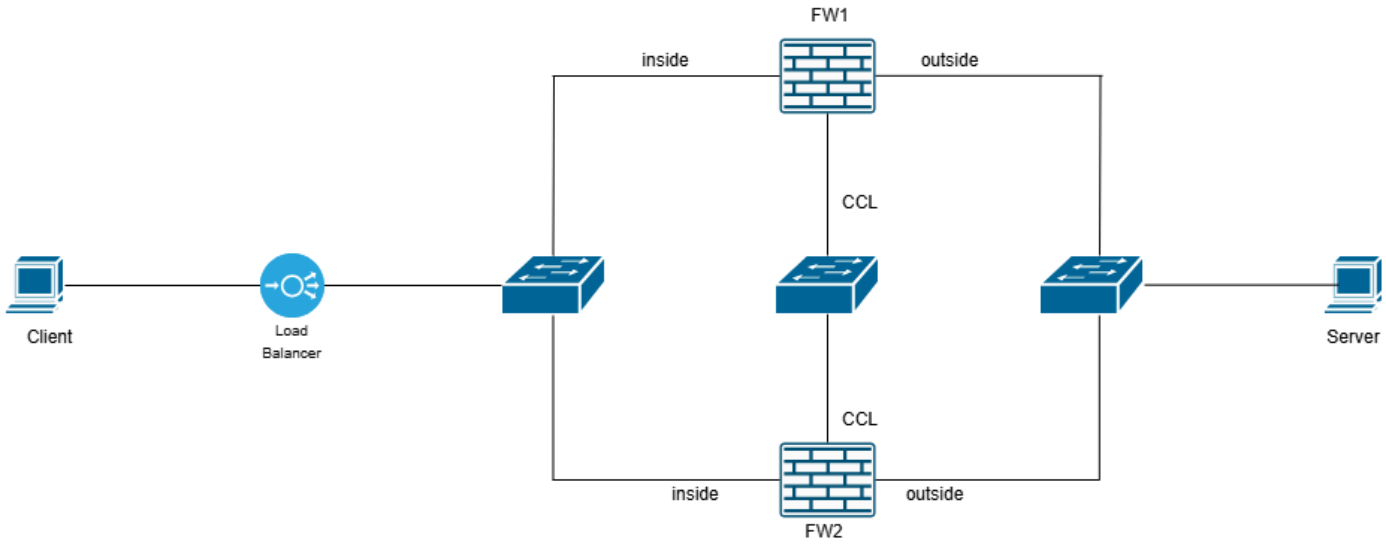
Pueden aparecer uno o más de estos síntomas:

- Fallos de conectividad intermitentes para aplicaciones que atraviesan un clúster FTD.
- El protocolo de enlace de tres vías TCP falla durante los intentos de conexión.
- El cliente envía un paquete SYN, pero no recibe la respuesta SYN-ACK esperada.
- El cliente envía un paquete RST después del SYN inicial.

Entorno

- Visto por primera vez en Secure Firewall Threat Defence 7.4, otras versiones también pueden verse afectadas
- Configuración de agrupamiento
- Equilibrador de carga en la ruta de red: es opcional

Topología



inline_image_0.png

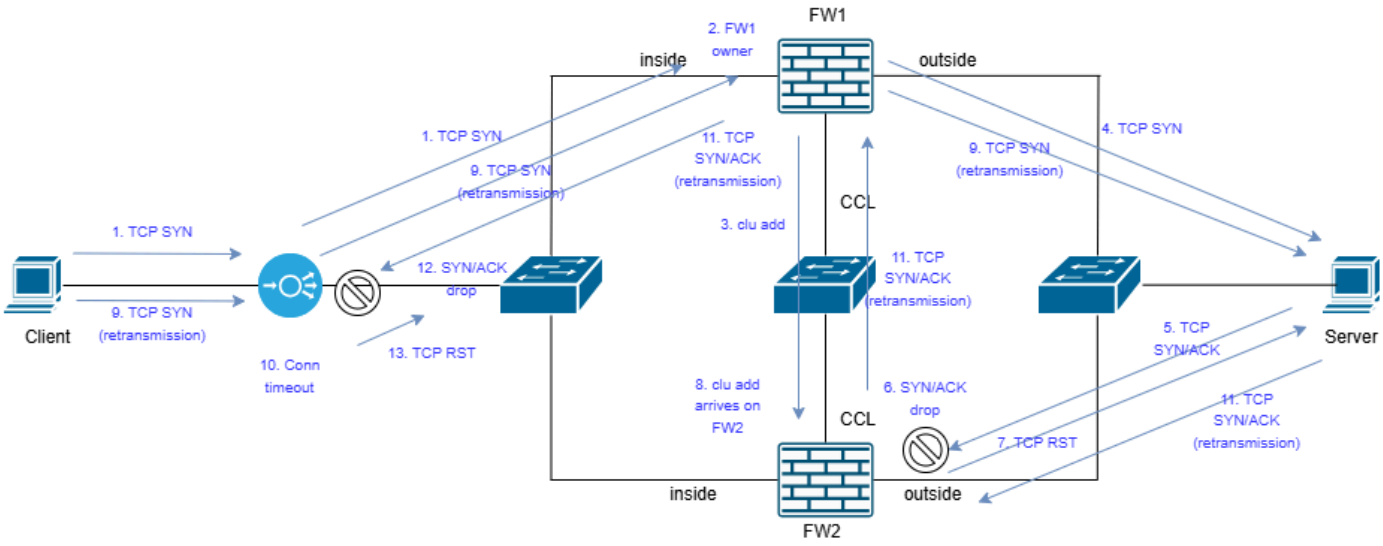
Resolución

Para provocar el problema, debe realizar capturas simultáneas en estos puntos:

- Interfaz interna FW1 (con reinyección y ocultación)
- Interfaz exterior FW1 (con reinyección y ocultación)
- Interfaz de clúster FW1 (CCL)
- Interfaz interior FW2 (con reinyección y ocultación)
- Interfaz exterior FW2 (con reinyección y ocultación)
- Interfaz de clúster FW2 (CCL)
- Cliente (o lo más cerca posible del cliente)
- Servidor (o lo más cerca posible del servidor)

Para obtener detalles sobre cómo configurar la verificación de capturas: Cómo Habilitar las Capturas de Clúster.

Las capturas realizadas en ambos firewalls, junto con el cliente y el servidor, revelan esta topología:



inline_image_0.png

1. El cliente envía TCP SYN. El paquete llega al balanceador de carga (LB) y se envía a FW1.

2. FW1 recibe el paquete TCP SYN y se convierte en el propietario del flujo.

3. FW1 informa al director (FW2) sobre el propietario del flujo mediante el envío de un mensaje de clúster especial (club add).

4. FW1 reenvía el TCP SYN al servidor de destino.

Nota: los pasos 3 y 4 se realizan en un orden no específico.

5. El servidor responde con SYN/ACK. En este caso, tenemos un flujo asimétrico ya que SYN/ACK se envía hacia FW2 debido al algoritmo de balanceo de carga de canal de puerto.

6. SYN/ACK llega a FW2 antes del mensaje de adición de club. Esta es una condición de carrera y es puramente ambiental (como la latencia en CCL). Dado que FW2 no sabe quién es el propietario del flujo, se descarta SYN/ACK.

7. Se envía un TCP RST al servidor.

8. El mensaje de adición de club llega al FW2.

9. El cliente retransmite el paquete TCP SYN. El paquete TCP SYN se reenvía al servidor de destino.

10. En el LB, la conexión TCP para el flujo específico agota el tiempo de espera.

11. El servidor responde con SYN/ACK (retransmisión TCP). El paquete SYN/ACK llega a FW2. Esta vez, FW2 conoce al propietario del flujo, ya que recibió el mensaje club add y el SYN/ACK se reenvía al propietario del flujo a través de CCL. El SYN/ACK se envía al cliente.

12. El LB no conoce este flujo y descarta el SYN/ACK. Por lo tanto, el SYN/ACK nunca llega al cliente.

13. El LB tiene uno o más paquetes TCP RST.

Captura de firewall con análisis de seguimiento

En estos resultados, las capturas se recopilaron del firewall en las interfaces CCL y de cara al servidor.

· En CCL, la captura se realiza en el puerto UDP 4193.

· En las interfaces de datos, la captura coincide con el tráfico TCP entre los terminales usando la opción reinject-hide. La razón es que queremos ver a dónde llegan realmente los paquetes.

· Dirección IP 192.0.2.65 = cliente

· Dirección IP 192.0.2.6 = servidor

Paso 1: Utilice este comando en el dispositivo de firewall que obtiene el SYN/ACK para ver cuándo llegó el mensaje trace add. En la salida de CLI se muestra el mensaje como Add flow.

```
firepower# show capture CCL decode

3 paquetes capturados

   1: 08:14:20.630521 127.2.1.1.51475 > 127.2.2.1.4193: udp 820

        Mensaje ASP de clúster: remitente: 1, receptor: 0

        Agregar flujo: propietario 1, director 0, copia de seguridad 0,

                  ifc_in_INSIDE(7020a7), ifc_out_INSIDE(7020a7)
```

```
                TCP src 192.0.2.65/37468, dest 192.0.2.6/80
```

Paso 2: Rastree el paquete SYN/ACK y céntrese en la marca de tiempo y el resultado de seguimiento:

```
firepower# show capture CAPI packet-number 1 trace

13 paquetes capturados

   1: 08:14:20.628690 802.1Q vlan#200 P0 192.0.2.6.80 > 192.0.2.65.37468: S
2524735158:2524735158(0) ack 2881263901 win 65160 <mss 1460,sackOK,timestamp 611712900
970937593,nop,wscale 7>

Fase: 1

Tipo: CAPTURA

Subtipo:

Resultado: PERMITIR

Tiempo transcurrido: 1708 ns

Config:

Información adicional:

Lista de acceso MAC




Fase: 2

Tipo: ACCESS-LIST

Subtipo:

Resultado: PERMITIR
```

Tiempo transcurrido: 1708 ns

Config:

Regla implícita

Información adicional:

Lista de acceso MAC

Fase: 3

Tipo: INPUT-ROUTE-LOOKUP

Subtipo: Resolver interfaz de salida

Resultado: PERMITIR

Tiempo transcurrido: 13664 ns

Config:

Información adicional:

Next-hop encontrado 192.168.200.140 usando egress ifc INSIDE(vrfid:0)

Fase: 4

Tipo: CLUSTER-EVENT

Subtipo:

Resultado: PERMITIR

Tiempo transcurrido: 16104 ns

Config:

Información adicional:

Interfaz de entrada: 'INSIDE'

Tipo de flujo: SIN FLUJO

Me (0) estoy convirtiendo en propietario

Fase: 5

Tipo: OBJECT_GROUP_SEARCH

Subtipo:

Resultado: PERMITIR

Tiempo transcurrido: 19520 ns

Config:

Información adicional:

 Recuento de coincidencias de grupo de objetos de origen: 0

 Recuento de coincidencias NSG de origen: 0

 Recuento de coincidencias NSG de destino: 0

 Clasificar conteo de búsqueda de tabla: 1

 Recuento total de búsquedas: 1

 Número de pares de claves duplicados: 0

 Clasificar recuento de coincidencias de tabla: 4

Fase: 6

Tipo: ACCESS-LIST

Subtipo:

Resultado: PERMITIR

Tiempo transcurrido: 366 ns

Config:

access-group CSM_FW_ACL_global

access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268436480

access-list CSM_FW_ACL_ remark rule-id 268436480: ACCESS POLICY: mzafeiro_empty - Default

access-list CSM_FW_ACL_ remark rule-id 268436480: L4 RULE: DEFAULT ACTION RULE

Información adicional:

Este paquete se enviará a snort para procesamiento adicional donde se alcanzará un veredicto

Fase: 7

Tipo: CONN-SETTINGS

Subtipo:

Resultado: PERMITIR

Tiempo transcurrido: 366 ns

Config:

class-map tcp

```
 match access-list tcp

policy-map global_policy

 class tcp

  set connection conn-max 0 embryonic-conn-max 0 random-sequence-number disable syn-cookie-mss
1380

service-policy global_policy global
```

Información adicional:

Fase: 8

Tipo: NAT

Subtipo: por sesión

Resultado: PERMITIR

Tiempo transcurrido: 366 ns

Config:

Información adicional:

Fase: 9

Tipo: IP-OPTIONS

Subtipo:

```
Resultado: PERMITIR

Tiempo transcurrido: 366 ns

Config:

Información adicional:



Resultado:

interfaz de entrada: INSIDE(vrfid:0)

input-status: up

input-line-status: up

interfaz de salida: INSIDE(vrfid:0)

output-status: up

output-line-status: up

Acción: descartar

Tiempo empleado: 54168 ns

Razón de la caída: (tcp-not-syn) Primer paquete TCP que no es SYN, Ubicación de la caída: frame
snp_sp:7459 flow (NA)/NA
```

Puntos clave

· El mensaje Add flow llegó a las 08:14:20.630521 mientras que el SYN/ACK ~2 ms antes a las 08:14:20.628690. Esta es la condición de carrera.

· El firewall descarta el paquete SYN/ACK con el motivo tcp-not-syn ASP. Observe que en la fase

4 el firewall intentó identificar si había un propietario de flujo conocido pero no encontró ninguno. Por lo tanto, intentó convertirse en un propietario de flujo.

Este resultado muestra un seguimiento del SYN/ACK cuando el firewall conoce el flujo:

```
firepower# show capture CAPI packet-number 3 trace

13 paquetes capturados

   3: 08:14:21.629560 802.1Q vlan#200 P0 192.0.2.6.80 > 192.0.2.65.37468: S
2540375172:2540375172(0) ack 2881263901 win 65160 <mss 1460,sackOK,timestamp 611713901
970938595,nop,wscale 7>

Fase: 1

Tipo: CAPTURA

Subtipo:

Resultado: PERMITIR

Tiempo transcurrido: 1708 ns

Config:

Información adicional:

Lista de acceso MAC

Fase: 2

Tipo: ACCESS-LIST

Subtipo:

Resultado: PERMITIR

Tiempo transcurrido: 1708 ns
```

Config:

Regla implícita

Información adicional:

Lista de acceso MAC

Fase: 3

Tipo: CLUSTER-EVENT

Subtipo:

Resultado: PERMITIR

Tiempo transcurrido: 3416 ns

Config:

Información adicional:

Interfaz de entrada: 'INSIDE'

Tipo de flujo: STUB

I (0) tiene flujo, propietario válido (1).

Fase: 4

Tipo: CAPTURA

Subtipo:

Resultado: PERMITIR

Tiempo transcurrido: 7808 ns

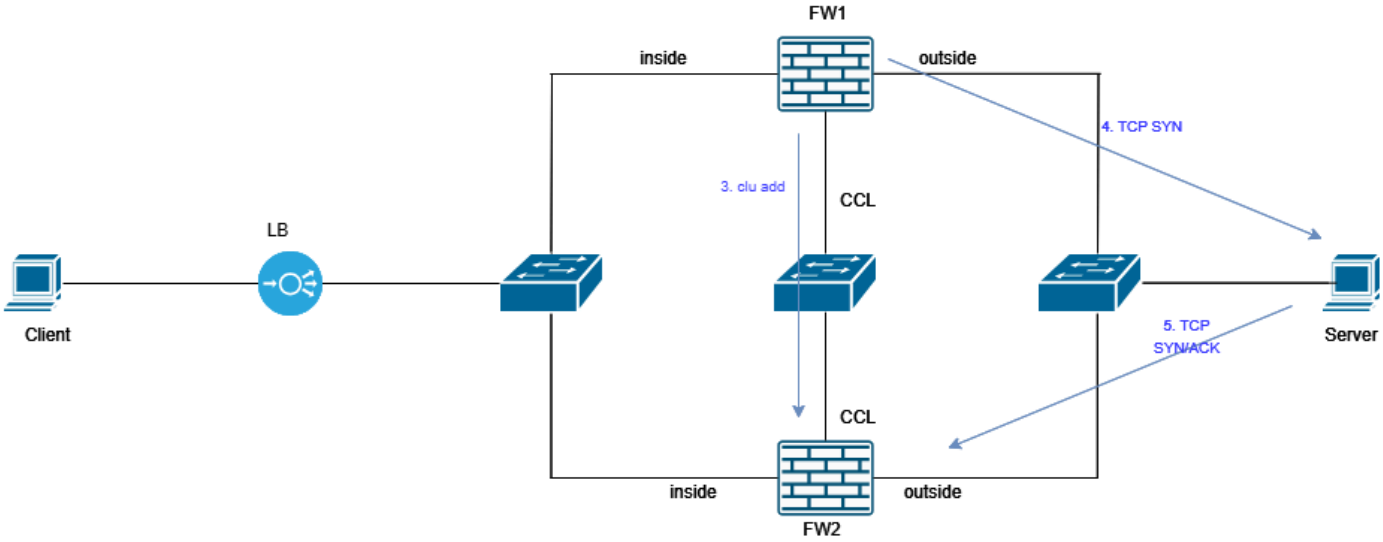
```
Config:

Información adicional:

Lista de acceso MAC

Resultado:

interfaz de entrada: INSIDE(vrfid:0)

input-status: up

input-line-status: up

Acción: permitir

Tiempo empleado: 14640 ns




Se muestra 1 paquete

firepower#
```

El punto clave está en la Fase 3. El firewall sabe que la unidad de clúster 1 es el propietario del flujo. Puede utilizar el comando show cluster info para ver qué dispositivo es la unidad 0 y cuál es 1.

Preguntas Frecuentes

P. ¿Por qué vemos problemas de conectividad TCP intermitentes?

R. Dado que se trata de una condición de carrera, se produce al azar. La condición de carrera se puede visualizar en consecuencia:

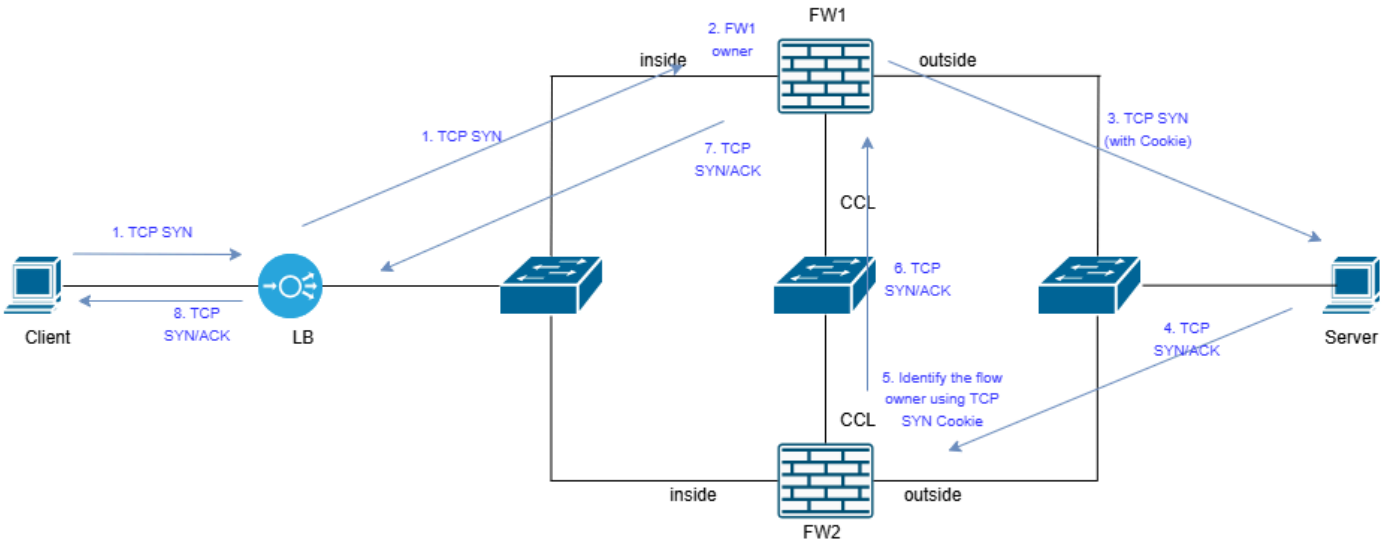


inline_image_0.png

P. ¿Cuáles son las posibles soluciones para evitar la condición de carrera?

A.

Solución 1: habilite la aleatorización de números de secuencia TCP para aprovechar el mecanismo de la cookie SYN TCP. En ese caso, la comunicación se estructura en consecuencia:



inline_image_1.png

Solución 2: Elimine la asimetría de la red. En primer lugar, debe identificar el motivo de la asimetría. Esto puede requerir el ajuste del algoritmo de equilibrio de carga del canal de puerto, el nuevo cableado de los cables del canal de puerto en orden diferente, entre otras cosas.

Causa

La causa raíz es una condición de anticipación causada por la asimetría del clúster dentro de la implementación del clúster de FTD. Los paquetes SYN-ACK del servidor están siendo procesados por un nodo de clúster de FTD diferente al que manejó el paquete SYN inicial, lo que impide el establecimiento correcto de la sesión TCP.

Contenido relacionado

- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).