Solucionar problemas de assimetria de cluster FTD que causam falhas de conexão TCP

Problema

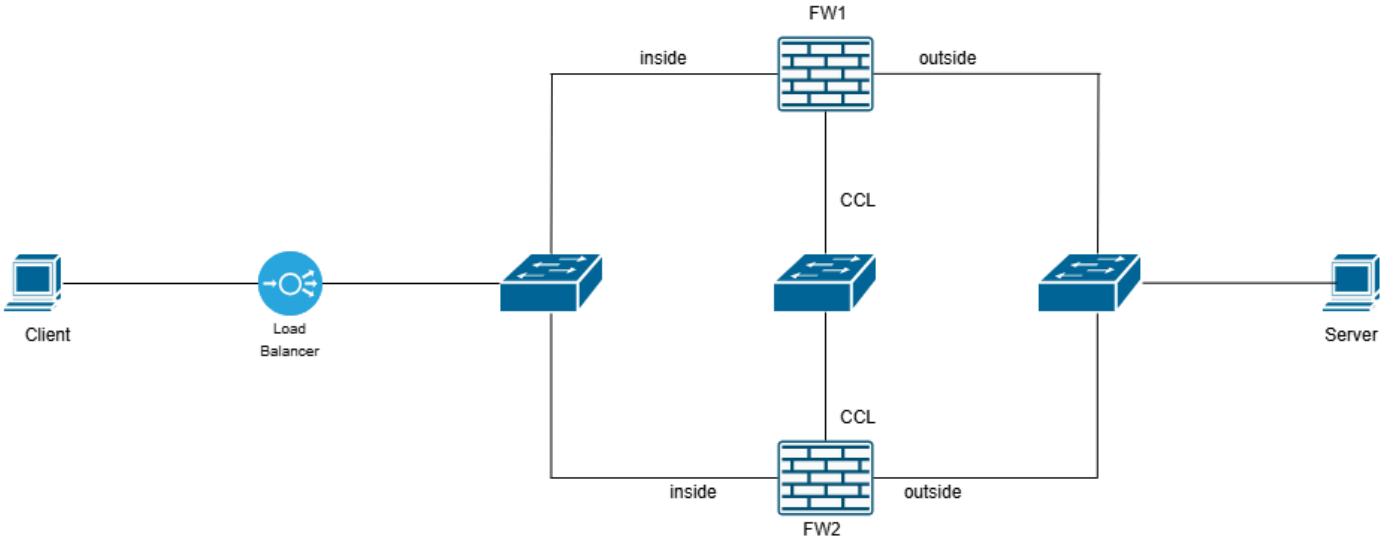
Um ou mais destes sintomas podem aparecer:

- Falhas intermitentes de conectividade para aplicativos que passam por um cluster FTD.
- O handshake triplo TCP falha durante as tentativas de conexão.
- O cliente envia um pacote SYN, mas não recebe a resposta SYN-ACK esperada.
- O cliente envia um pacote RST após o SYN inicial.

Ambiente

- Visto pela primeira vez no Secure Firewall Threat Defense 7.4 — outras versões também podem ser afetadas
- Configuração de cluster
- Balanceador de carga no caminho de rede — opcional

Topologia



inline_image_0.png

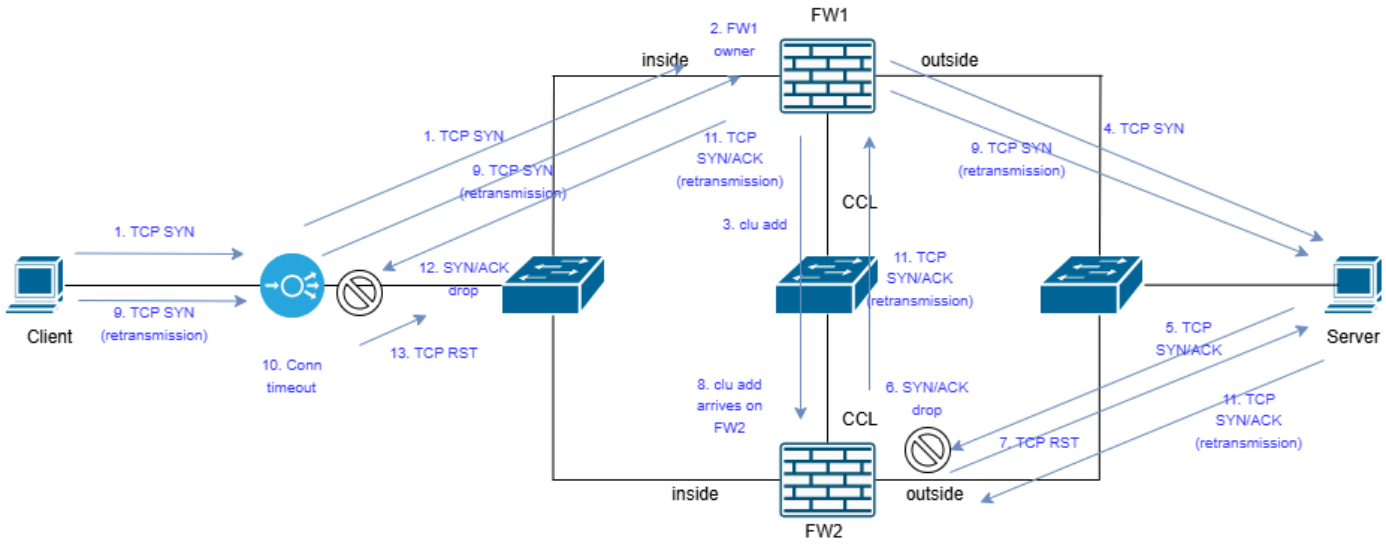
Resolução

Para fazer a raiz do problema, você precisa fazer capturas simultâneas nestes pontos:

- Interface interna FW1 (com reinserção-ocultação)
- Interface externa FW1 (com reinserção-ocultação)
- Interface de cluster FW1 (CCL)
- Interface interna FW2 (com reinserção/ocultação)
- Interface externa FW2 (com reinserção-ocultação)
- Interface de cluster FW2 (CCL)
- Cliente (ou o mais próximo possível do cliente)
- Servidor (ou o mais próximo possível do servidor)

Para obter detalhes sobre como configurar as capturas, verifique: Como ativar as capturas de cluster.

As capturas feitas nos firewalls junto com o cliente e o servidor revelam esta topologia:



inline_image_0.png

1. O cliente envia TCP SYN. O pacote chega ao LB (balanceador de carga) e é enviado para FW1.

2. FW1 recebe o pacote TCP SYN e torna-se o proprietário do fluxo.

3. O FW1 informa o direcionador (FW2) sobre o proprietário do fluxo enviando uma mensagem de cluster especial (clu add).

4. FW1 encaminha o TCP SYN ao servidor de destino.

Observação: as etapas 3 e 4 acontecem em uma ordem não específica.

5. O servidor responde com SYN/ACK. Nesse caso, temos um fluxo assimétrico, pois o SYN/ACK é enviado para o FW2 devido ao algoritmo de balanceamento de carga do canal da porta.

6. SYN/ACK chega ao FW2 antes da mensagem de adição de clu. Essa é uma condição de corrida e é puramente ambiental (como a latência no CCL). Como o FW2 não sabe quem é o proprietário do fluxo, o SYN/ACK é descartado.

7. Um TCP RST é enviado ao servidor.

8. A mensagem de adição de clu chega ao FW2.

9. O Cliente retransmite o pacote TCP SYN. O pacote TCP SYN é encaminhado ao servidor de destino.

10. No LB, a conexão TCP para o fluxo específico expira.

11. O servidor responde com SYN/ACK (retransmissão TCP). O pacote SYN/ACK chega ao FW2. Desta vez, o FW2 sabe sobre o proprietário do fluxo desde que recebeu a mensagem clu add e o SYN/ACK é encaminhado ao proprietário do fluxo pelo CCL. O SYN/ACK é enviado ao cliente.

12. O LB não sabe sobre esse fluxo e descarta o SYN/ACK. Assim, o SYN/ACK nunca chega ao cliente.

13. O LB contém um ou mais pacotes TCP RST.

Captura de firewall com análise de rastreamento

Nessas saídas, foram coletadas capturas do firewall nas interfaces CCL e de servidor.

· No CCL, a captura é na porta UDP 4193.

· Nas interfaces de dados, a captura corresponde ao tráfego TCP entre os pontos finais usando a opção reinject-hide. O motivo é que queremos ver onde os pacotes realmente chegam.

· Endereço IP 192.0.2.65 = cliente

· Endereço IP 192.0.2.6 = servidor

Etapa 1: Use este comando no dispositivo de firewall que obtém o SYN/ACK para ver quando a mensagem clu add chegou. Na saída da CLI, a mensagem é mostrada como Add flow.

```
firepower#show capture CCL decode

3 pacotes capturados

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

        Mensagem ASP do cluster: remetente: 1, destinatário: 0

        Adicionar fluxo: proprietário 1, diretor 0, backup 0,

                  ifc_in INSIDE(7020a7), ifc_out INSIDE(7020a7)
```

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

Etapa 2: Rastreie o pacote SYN/ACK e concentre-se no carimbo de data/hora e no resultado do rastreamento:

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

13 pacotes 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: CAPTURE

Subtipo:

Resultado: ALLOW

Tempo decorrido: 1708 ns

Config:

Informações adicionais:

Lista de Acesso MAC




Fase: 2

Tipo: ACCESS-LIST

Subtipo:

Resultado: ALLOW
```

Tempo decorrido: 1708 ns

Config:

Regra Implícita

Informações adicionais:

Lista de Acesso MAC

Fase: 3

Tipo: INPUT-ROUTE-LOOKUP

Subtipo: Resolver interface de saída

Resultado: ALLOW

Tempo decorrido: 13664 ns

Config:

Informações adicionais:

Encontrado próximo salto 192.168.200.140 usando ifc de saída INSIDE(vrfid:0)

Fase: 4

Tipo: CLUSTER-EVENT

Subtipo:

Resultado: ALLOW

Tempo decorrido: 16104 ns

Config:

Informações adicionais:

Interface de entrada: 'INSIDE'

Tipo de fluxo: NO FLOW

Eu (0) estou me tornando proprietário

Fase: 5

Tipo: OBJECT_GROUP_SEARCH

Subtipo:

Resultado: ALLOW

Tempo decorrido: 19520 ns

Config:

Informações adicionais:

 Contagem de correspondência do grupo de objetos de origem: 0

 Contagem de correspondência do NSG de origem: 0

 Contagem de correspondência de NSG de destino: 0

 Classificar contagem de pesquisa da tabela: 1

 Contagem total de pesquisas: 1

 Contagem de pares de chaves duplicados: 0

 Classificar contagem de correspondência de tabela: 4

Fase: 6

Tipo: ACCESS-LIST

Subtipo:

Resultado: ALLOW

Tempo decorrido: 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

Informações adicionais:

Este pacote será enviado ao snort para processamento adicional onde um veredito será alcançado

Fase: 7

Tipo: CONN-SETTINGS

Subtipo:

Resultado: ALLOW

Tempo decorrido: 366 ns

Config:

class-map tcp

```
 match access-list tcp

policy-map global_policy

 class tcp

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

service-policy global_policy global

Informações adicionais:




Fase: 8

Tipo: NAT

Subtipo: por sessão

Resultado: ALLOW

Tempo decorrido: 366 ns

Config:

Informações adicionais:




Fase: 9

Tipo: IP-OPTIONS

Subtipo:
```

```
Resultado: ALLOW

Tempo decorrido: 366 ns

Config:

Informações adicionais:



Resultado:

interface de entrada: INSIDE(vrfid:0)

input-status: ativado

input-line-status: ativado

interface de saída: INSIDE(vrfid:0)

output-status: up

output-line-status: ativado

Ação: descartar

Tempo Decorrido: 54168 ns

Motivo da queda: (tcp-not-syn) Primeiro pacote TCP não SYN, Local da queda: frame snp_sp:7459
flow (NA)/NA
```

Pontos principais

A mensagem Add flow chegou às 08:14:20.630521 enquanto o SYN/ACK ~2 ms antes às 08:14:20.628690. Essa é a condição de corrida.

· O pacote SYN/ACK é descartado pelo firewall com a razão ASP tcp-not-syn. Observe que na

Fase 4 o firewall tentou identificar se havia um proprietário de fluxo conhecido, mas não encontrou nenhum. Portanto, ele tentou se tornar um proprietário de fluxo.

Esta saída mostra um rastreamento do SYN/ACK quando o firewall sabe sobre o fluxo:

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

13 pacotes 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: CAPTURE

Subtipo:

Resultado: ALLOW

Tempo decorrido: 1708 ns

Config:

Informações adicionais:

Lista de Acesso MAC

Fase: 2

Tipo: ACCESS-LIST

Subtipo:

Resultado: ALLOW

Tempo decorrido: 1708 ns
```

Config:

Regra Implícita

Informações adicionais:

Lista de Acesso MAC

Fase: 3

Tipo: CLUSTER-EVENT

Subtipo:

Resultado: ALLOW

Tempo decorrido: 3416 ns

Config:

Informações adicionais:

Interface de entrada: 'INSIDE'

Tipo de fluxo: STUB

I (0) tem fluxo, proprietário válido (1).

Fase: 4

Tipo: CAPTURE

Subtipo:

Resultado: ALLOW

Tempo decorrido: 7808 ns

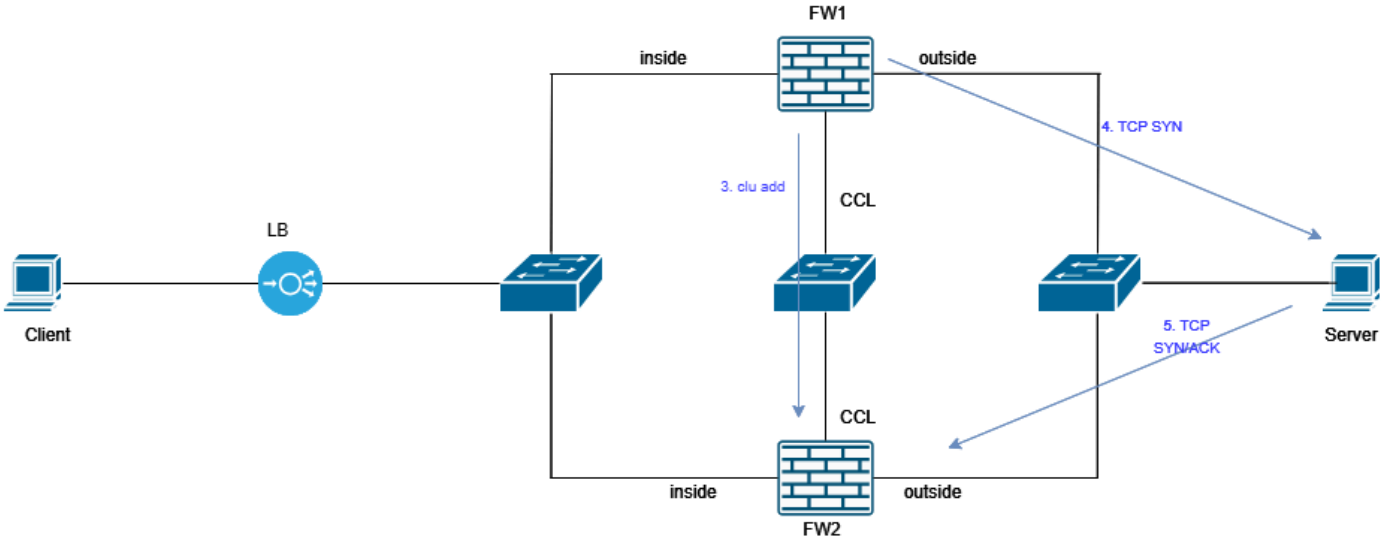
```
Config:

Informações adicionais:

Lista de Acesso MAC

Resultado:

interface de entrada: INSIDE(vrfid:0)

input-status: ativado

input-line-status: ativado

Ação: permitir

Tempo Decorrido: 14640 ns



1 pacote mostrado

firepower#
```

O ponto-chave está na Fase 3. O firewall sabe que a unidade de cluster 1 é o proprietário do fluxo. Você pode usar o comando show cluster info para ver qual dispositivo é a unidade 0 e qual é a 1.

Perguntas mais freqüentes

P. Por que vemos problemas intermitentes de conectividade TCP?

R. Como esta é uma condição de corrida, ela acontece aleatoriamente. A condição de corrida pode ser visualizada de acordo:

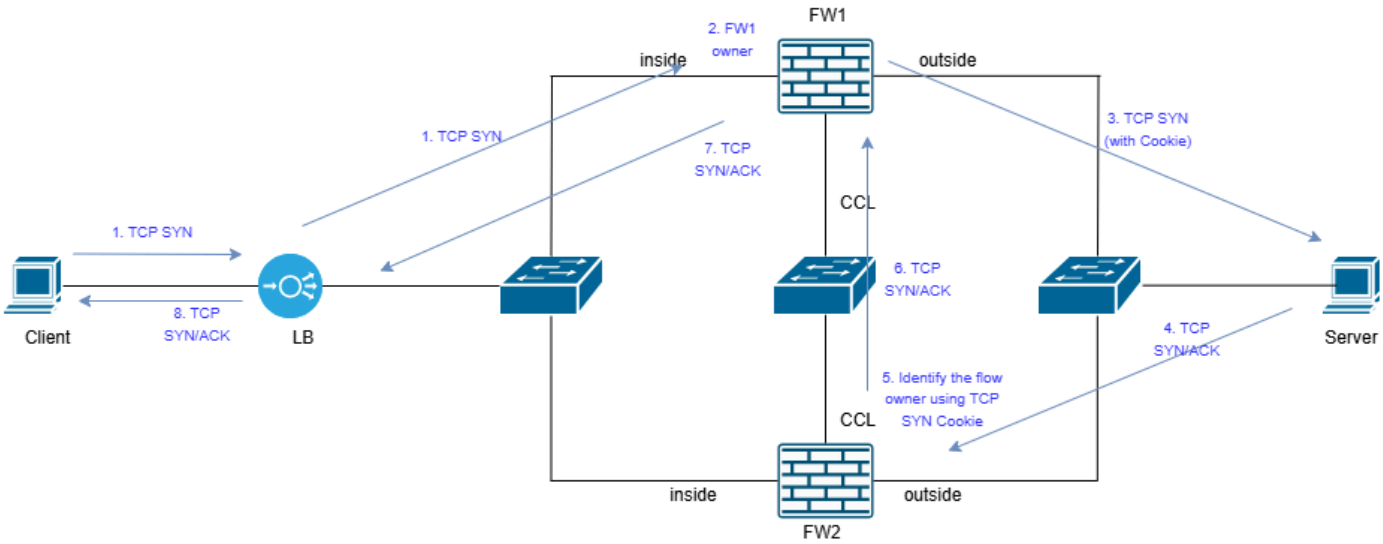


inline_image_0.png

P. Quais são as soluções possíveis para evitar a condição de corrida?

A.

Solução 1: Ative a aleatorização do número de sequência TCP para aproveitar o mecanismo TCP SYN Cookie. Nesse caso, a comunicação é estruturada de acordo:



inline_image_1.png

Solução 2: Elimine a assimetria na rede. Primeiro, você precisa identificar o motivo da assimetria. Isso pode exigir o ajuste do algoritmo de balanceamento de carga do canal de porta, reconectar os cabos do canal de porta em ordem diferente, entre outras coisas.

Causa

A causa raiz é uma condição de corrida causada devido à assimetria do cluster na implantação do cluster de FTD. Os pacotes SYN-ACK do servidor estão sendo processados por um nó de cluster de FTD diferente daquele que tratou do pacote SYN inicial, impedindo o estabelecimento adequado da sessão TCP.

Conteúdo relacionado

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.