TCP接続障害を引き起こすFTDクラスタの非対称のトラブルシューティング

内容

お問い合わせ内容

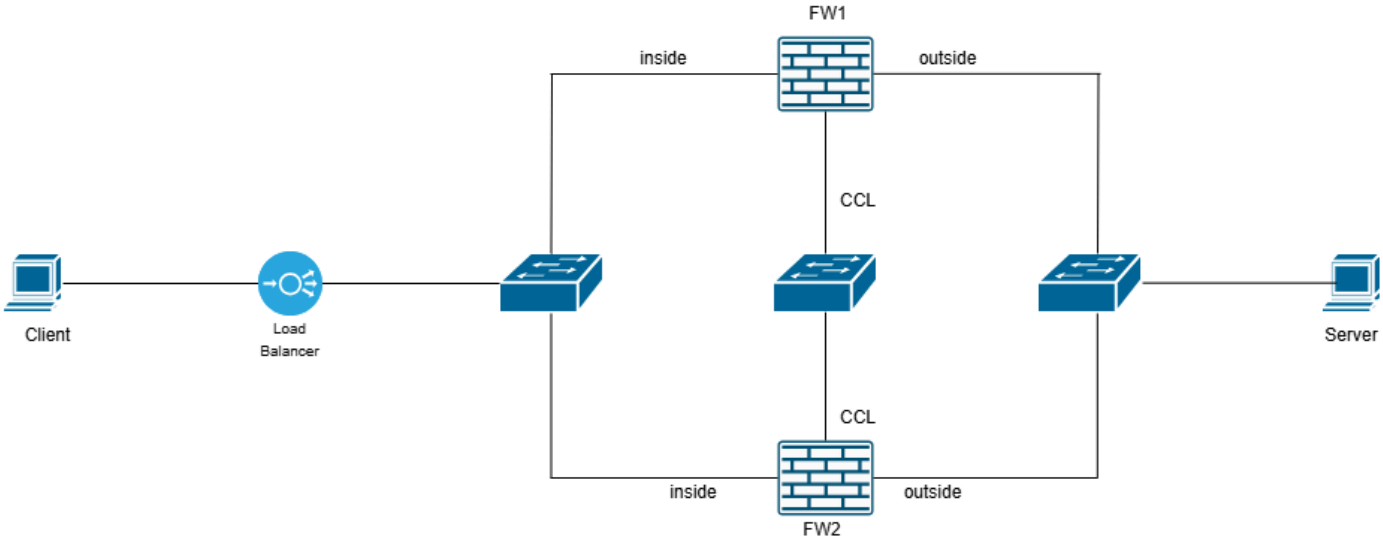
次の1つ以上の症状が現れる可能性があります。

- FTDクラスタを通過するアプリケーションの断続的な接続障害
- 接続試行中にTCP 3ウェイハンドシェイクが失敗する。
- クライアントはSYNパケットを送信しますが、予期されるSYN-ACK応答を受信しません。
- クライアントは最初のSYNの後にRSTパケットを送信します。

環境

- 最初にSecure Firewall Threat Defense(SFTD)7.4で確認されました。他のバージョンも該当する可能性があります
- クラスタの設定
- ネットワークパスのロードバランサ：これはオプションです

トポロジ



inline_image_0.png (インラインイメージ_0.png)

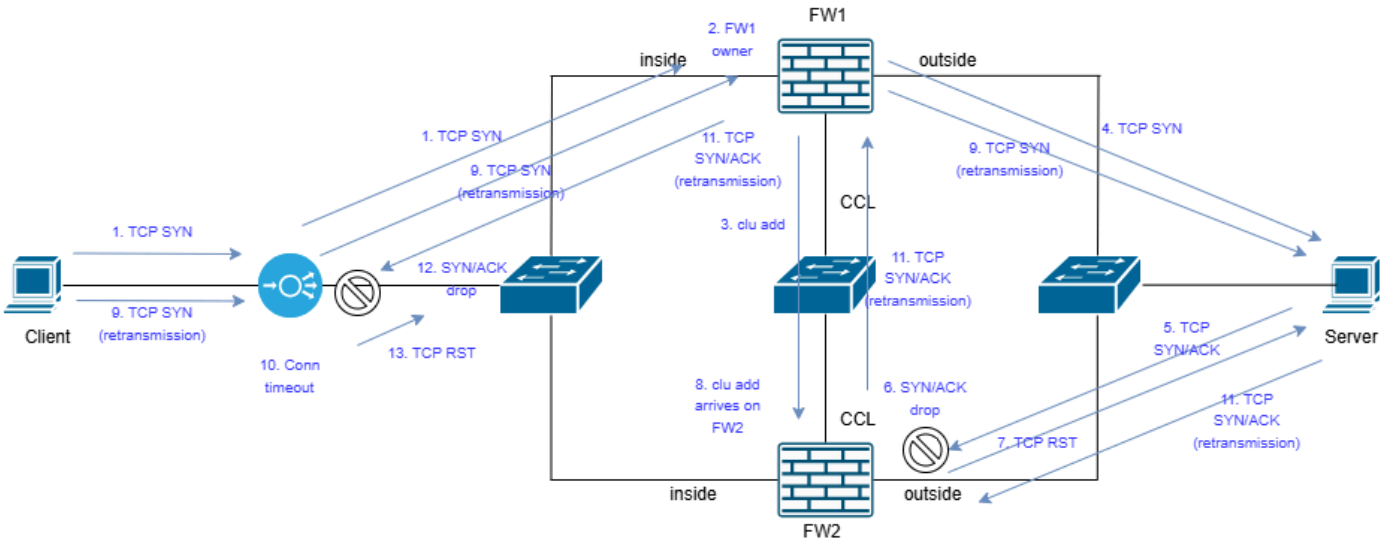
解決策

問題の根本原因を特定するには、次の時点で同時キャプチャを取得する必要があります。

- FW1内部インターフェイス (reinject-hideあり)
- FW1外部インターフェイス (reinject-hideあり)
- FW1クラスタインターフェイス(CCL)
- FW2内部インターフェイス (reinject-hideあり)
- FW2外部インターフェイス (reinject-hideあり)
- FW2クラスタインターフェイス(CCL)
- クライアント (または可能な限りクライアントの近く)
- サーバ (または可能な限りサーバの近く)

キャプチャの設定方法の詳細については、「クラスタキャプチャを有効にする方法」を参照してください。

クライアントおよびサーバとともに両方のファイアウォールで取得されたキャプチャから、次のトポロジが明らかになります。



inline_image_0.png (インラインイメージ_0.png)

1. クライアントがTCP SYNを送信します。 パケットはロードバランサ(LB)に到着し、FW1に送信されます。

2. FW1はTCP SYNパケットを受信し、フローオーナーになります。

3. FW1は、特別な(clu add)クラスタメッセージを送信して、フロー所有者についてディレクタ(FW2)に通知します。

4. FW1は宛先サーバにTCP SYNを転送します。

注：ステップ3と4の順序は特にありません。

---

5. サーバはSYN/ACKで応答します。 この場合、ポートチャネルのロードバランシングアルゴリズムにより、SYN/ACKがFW2に向けて送信されるため、非対称フローが存在します。

6. clu addメッセージの前に、FW2にSYN/ACKが到着します。 これは競合状態であり、純粋に環境です（CCLでの遅延など）。 FW2はフローの所有者が誰かを知らないため、SYN/ACKはドロップされます。

7. TCP RSTがサーバに送信されます。

8. clu addメッセージがFW2に到着します。

9. クライアントはTCP SYNパケットを再送信します。 TCP SYNパケットが宛先サーバに転送さ

れます。

10. LBで、特定のフローのTCP接続がタイムアウトします。

11. サーバはSYN/ACK（TCP再送信）で応答します。 SYN/ACKパケットがFW2に到着します。 今回は、FW2はclu addメッセージを受け取ってCCL経由でSYN/ACKがフロー所有者に転送されるため、フロー所有者を認識しています。 SYN/ACKがクライアントに送信されます。

12. LBはこのフローを認識せず、SYN/ACKをドロップします。 そのため、SYN/ACKがクライアントに到達することはありません。

13. LB 1つ以上のTCP RSTパケット。

トレース分析によるファイアウォールキャプチャ

次の出力では、キャプチャはCCLおよびサーバ側インターフェイスのファイアウォールから収集されています。

・ CCLでは、キャプチャはUDP 4193ポートで行われます。

・ データインターフェイスで、reinject-hideオプションを使用して、キャプチャがエンドポイント間のTCPトラフィックを照合します。 これは、パケットが実際に到着した場所を確認するためです。

・ IPアドレス192.0.2.65 =クライアント

・ IPアドレス192.0.2.6 =サーバ

ステップ1:SYN/ACKを取得するファイアウォールデバイスでこのコマンドを使用して、clu addメッセージがいつ着信したかを確認します。 CLI出力では、メッセージは「Add flow」と表示されます。

<#root>

```
firepower#
```

show capture CCL decode

```
3 packets captured
   1: 08:14:20.630521       127.2.1.1.51475 > 127.2.2.1.4193:  udp 820
        Cluster ASP message: sender: 1, receiver: 0
        Add flow: owner 1, director 0, backup 0,
                  ifc_in INSIDE(7020a7), ifc_out INSIDE(7020a7)
                  TCP src 192.0.2.65/37468, dest 192.0.2.6/80
```

ステップ2:SYN/ACKパケットをトレースし、タイムスタンプとトレース結果に注目します。

<#root>

```
firepower#

 show capture CAPI packet-number 1 trace


13 packets captured
   1: 08:14:20.628690       802.1Q vlan#200 P0 192.0.2.6.80 > 192.0.2.65.37468: S 2524735158:2524735158
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 1708 ns
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 1708 ns
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: INPUT-ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Elapsed time: 13664 ns
Config:
Additional Information:
Found next-hop 192.168.200.140 using egress ifc  INSIDE(vrfid:0)

Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Elapsed time: 16104 ns
Config:
Additional Information:
Input interface: 'INSIDE'
```

Flow type: NO FLOW

I (0) am becoming owner

```
Phase: 5
Type: OBJECT_GROUP_SEARCH
Subtype:
Result: ALLOW
Elapsed time: 19520 ns
Config:
Additional Information:
 Source object-group match count:          0
 Source NSG match count:                   0
 Destination NSG match count:              0
 Classify table lookup count:              1
 Total lookup count:                       1
 Duplicate key pair count:                 0
 Classify table match count:               4

Phase: 6
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 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
Additional Information:
 This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 7
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Elapsed time: 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
Additional Information:

Phase: 8
Type: NAT
Subtype: per-session
Result: ALLOW
Elapsed time: 366 ns
Config:
Additional Information:

Phase: 9
Type: IP-OPTIONS
Subtype:
```

```
Result: ALLOW
Elapsed time: 366 ns
Config:
Additional Information:

Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
output-interface: INSIDE(vrfid:0)
output-status: up
output-line-status: up

Action: drop


Time Taken: 54168 ns

Drop-reason: (tcp-not-syn) First TCP packet not SYN, Drop-location: frame snp_sp:7459 flow (NA)/NA
```

キー ポイント

・ Add flowメッセージは08:14:20.630521に到達しましたが、SYN/ACKは約2ミリ秒早い08:14:20.628690でした。 これがレースコンディションです。

・ SYN/ACKパケットがファイアウォールによって「tcp-not-syn」ASP理由でドロップされます。 フェーズ4では、ファイアウォールが既知のフロー所有者の存在を特定しようとしたが、見つからなかったことに注目してください。 それでフローのオーナーになろうとした。

次の出力は、ファイアウォールがフローを認識している場合のSYN/ACKのトレースを示しています。

<#root>

```
firepower#

show capture CAPI packet-number 3 trace


13 packets captured

   3: 08:14:21.629560       802.1Q vlan#200 P0 192.0.2.6.80 > 192.0.2.65.37468: S 2540375172:2540375172
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
```

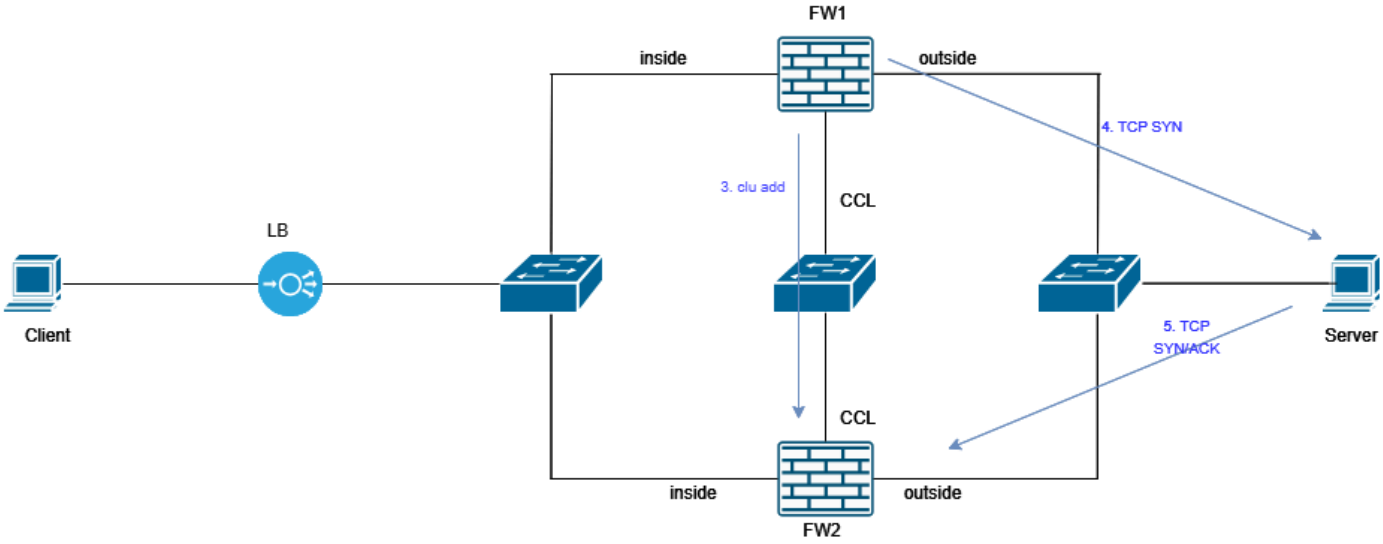
```
Elapsed time: 1708 ns
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 1708 ns
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Elapsed time: 3416 ns
Config:
Additional Information:
Input interface: 'INSIDE'
Flow type: STUB

I (0) have flow, valid owner (1).



Phase: 4
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 7808 ns
Config:
Additional Information:
MAC Access list

Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
Action: allow
Time Taken: 14640 ns

1 packet shown
firepower#
```

重要な点はフェーズ3にあります。 ファイアウォールは、クラスタユニット1がフロー所有者であることを認識します。 show cluster infoコマンドを使用して、ユニット0とユニット1のデバイスを確認できます。

FAQ

Q.断続的なTCP接続の問題が発生するのはなぜですか。

A.これは競合状態であるため、ランダムに発生します。 状況に応じて競合状態を視覚化できます。

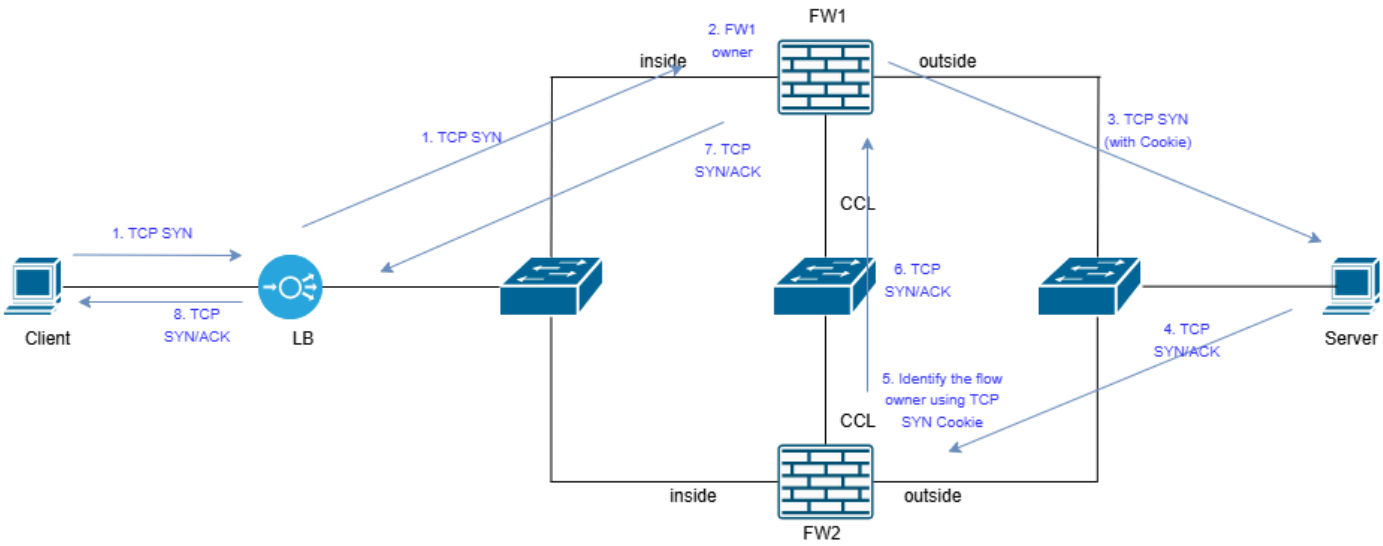


inline_image_0.png (インラインイメージ_0.png)

Q.この競合状態を回避するために可能なソリューションは何ですか。

A.

解決策1:TCP SYN Cookieメカニズムを利用するために、TCPシーケンス番号のランダム化を有効にします。 この場合、通信は次のように構成されます。



inline_image_1.pngファイル

解決策2：ネットワーク内の非対称を排除します。 まず、非対称性の理由を特定する必要があり

ます。 これには、特に、ポートチャネルのロードバランシングアルゴリズムの調整、ポートチャネルケーブルの別の順序での再配線が必要になる場合があります。

原因

根本原因は、FTDクラスタ導入内のクラスタの非対称が原因で発生する競合状態です。 サーバからのSYN-ACKパケットは、最初のSYNパケットを処理したノードとは異なるFTDクラスタノードで処理されているため、適切なTCPセッションの確立ができません。

関連コンテンツ

- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。