Fehlerbehebung: FTD-Cluster-Asymmetrie verursacht TCP-Verbindungsfehler

Problem

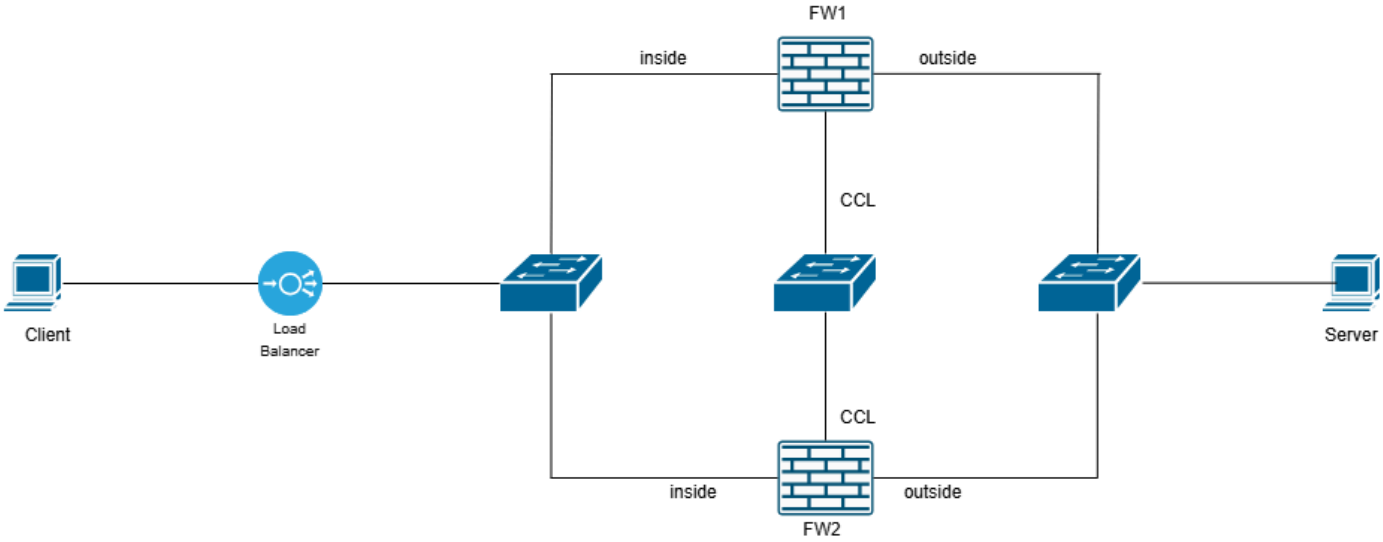
Eines oder mehrere dieser Symptome können auftreten:

- Intermittierende Verbindungsfehler bei Anwendungen, die einen FTD-Cluster durchlaufen.
- TCP-Drei-Wege-Handshake schlägt bei Verbindungsversuchen fehl.
- Der Client sendet ein SYN-Paket, empfängt aber nicht die erwartete SYN-ACK-Antwort.
- Der Client sendet ein RST-Paket nach der anfänglichen SYN.

Umwelt

- Zuerst in Secure Firewall Threat Defense 7.4 gesehen — andere Versionen können ebenfalls betroffen sein
- Cluster-Konfiguration
- Load Balancer im Netzwerkpfad - optional

Topologie



inline_image_0,png

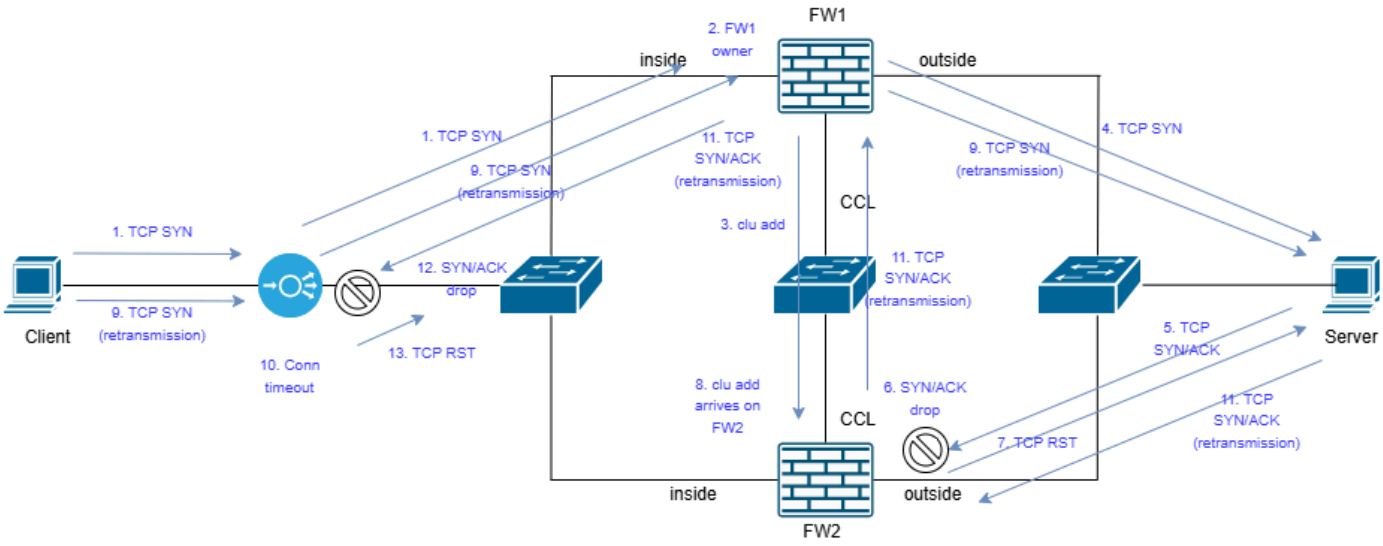
Auflösung

Um das Problem zu beheben, müssen Sie an folgenden Punkten gleichzeitig aufzeichnen:

- FW1 inside interface (with reject-hide)
- FW1 Außenschnittstelle (mit reject-hide)
- FW1 Cluster-Schnittstelle (CCL)
- FW2 inside interface (with reject-hide)
- FW2-Außenschnittstelle (mit reject-hide)
- FW2 Cluster Interface (CCL)
- Client (oder möglichst nahe am Client)
- Server (oder möglichst nah am Server)

Weitere Informationen zum Konfigurieren der Erfassungen finden Sie unter: [So aktivieren Sie die Clustererfassung.]

Die auf beiden Firewalls zusammen mit Client und Server aufgenommenen Aufzeichnungen zeigen diese Topologie:



inline_image_0,png

1. Der Client sendet TCP SYN. Das Paket erreicht den Load Balancer (LB) und wird an FW1 gesendet.

2. FW1 empfängt das TCP-SYN-Paket und wird zum Flow-Eigentümer.

3. FW1 informiert den Director (FW2) über den Flow Owner durch Senden einer speziellen (clu add) Cluster-Nachricht.

4. FW1 leitet das TCP-SYN an den Zielserver weiter.

Hinweis: Die Schritte 3 und 4 erfolgen in keiner bestimmten Reihenfolge.

5. Der Server antwortet mit SYN/ACK. In diesem Fall ergibt sich ein asymmetrischer Fluss, da SYN/ACK aufgrund des Algorithmus zum Port-Channel-Lastenausgleich an FW2 gesendet wird.

6. SYN/ACK kommt in FW2 vor der CLU-Add-Meldung an. Dies ist eine Race-Condition und stellt eine reine Umgebungsbedingung dar (z. B. Latenz in CCL). Da FW2 nicht weiß, wer der Flow-Eigentümer ist, wird SYN/ACK verworfen.

7. Eine TCP-RST wird an den Server gesendet.

8. Die CLU-Add-Meldung erreicht FW2.

9. Der Client sendet das TCP SYN-Paket erneut. Das TCP SYN-Paket wird an den Zielserver weitergeleitet.

10. Auf dem LB wird die TCP-Verbindung für den spezifischen Fluss deaktiviert.

11. Der Server antwortet mit SYN/ACK (TCP-Neuübertragung). Das SYN/ACK-Paket kommt auf FW2 an. Diesmal weiß FW2 über den Flow-Eigentümer Bescheid, da er die CLU-Add-Meldung erhalten hat, und das SYN/ACK wird über die CCL an den Flow-Eigentümer weitergeleitet. Das SYN/ACK wird an den Client gesendet.

12. Der LB kennt diesen Fluss nicht und verwirft die SYN/ACK. Daher kommt die SYN/ACK nie auf dem Client an.

13. Der LB sendet ein oder mehrere TCP-RST-Pakete.

Firewall-Erfassung mit Trace-Analyse

Bei diesen Ausgaben wurden Erfassungen von der Firewall auf CCL- und serverseitigen Schnittstellen erfasst.

- Bei CCL erfolgt die Erfassung über den UDP 4193-Port.

- An den Datenschnittstellen wird der TCP-Datenverkehr zwischen den Endpunkten mit der Option reject-hide abgeglichen. Der Grund hierfür ist, dass wir sehen möchten, wo die Pakete tatsächlich ankommen.

- IP-Adresse 192.0.2.65 = Client

- IP-Adresse 192.0.2.6 = Server

Schritt 1: Verwenden Sie diesen Befehl auf dem Firewall-Gerät, das die SYN/ACK erhält, um zu sehen, wann die clu add-Nachricht eingetroffen ist. In der CLI-Ausgabe wird die Nachricht als Add-Fluss angezeigt.

```
firepower# show capture CCL-Dekodierung

3 erfasste Pakete

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

        Cluster-ASP-Nachricht: Absender: 1, Empfänger: 0
```

```
        Fluss hinzufügen: Eigentümer 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
```

Schritt 2: Verfolgen Sie das SYN/ACK-Paket, und konzentrieren Sie sich auf den Zeitstempel und das Ablaufverfolgungsergebnis:

```
firepower# show capture CAPI-Paketnummer 1 trace

13 Pakete erfasst

   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>

Phase: 1

Typ: CAPTURE

Untertyp:

Ergebnis: ZULÄSSIG

Verstrichene Zeit: 1708 ns

Konfiguration:

Zusätzliche Informationen:

MAC-Zugriffsliste



Phase: 2

Typ: ACCESS-LIST
```

Untertyp:

Ergebnis: ZULÄSSIG

Verstrichene Zeit: 1708 ns

Konfiguration:

Implizite Regel

Zusätzliche Informationen:

MAC-Zugriffsliste

Phase 3:

Typ: INPUT-ROUTE-LOOKUP

Untertyp: Ausgangsschnittstelle auflösen

Ergebnis: ZULÄSSIG

Verstrichene Zeit: 13664 ns

Konfiguration:

Zusätzliche Informationen:

next-hop 192.168.200.140 using egress ifc INSIDE(vrfid:0);

Phase: 4

Typ: CLUSTER-EVENT

Untertyp:

Ergebnis: ZULÄSSIG

Verstrichene Zeit: 16104 ns

Konfiguration:

Zusätzliche Informationen:

Eingangsschnittstelle: 'INSIDE'

Flow-Typ: NO FLOW

Ich (0) werde Eigentümer

Phase: 5

Typ: OBJECT_GROUP_SEARCH

Untertyp:

Ergebnis: ZULÄSSIG

Verstrichene Zeit: 19520 ns

Konfiguration:

Zusätzliche Informationen:

 Anzahl der Übereinstimmungen der Quellobjektgruppe: 0

 Anzahl der Quell-NSG-Treffer: 0

 Anzahl der Ziel-NSG-Treffer: 0

 Tabellennachschlageanzahl klassifizieren: 1

 Gesamtanzahl der Suchvorgänge: 1

 Anzahl doppelter Schlüsselpaare: 0

Anzahl der Klassifizierungstabellen: 4

Phase: 6

Typ: ACCESS-LIST

Untertyp:

Ergebnis: ZULÄSSIG

Verstrichene Zeit: 366 ns

Konfiguration:

Zugriffsgruppe CSM_FW_ACL_ global

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

access-list CSM_FW_ACL_ remark rule-id 268436480: ZUGRIFFSRICHTLINIE: mzafeiro_empty - Standard

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

Zusätzliche Informationen:

Dieses Paket wird zur weiteren Verarbeitung an snort gesendet, wo ein Urteil erreicht wird

Phase: 7

Typ: CONN-SETTINGS

Untertyp:

Ergebnis: ZULÄSSIG

Verstrichene Zeit: 366 ns

Konfiguration:

Class-Map-TCP

 Abgleich Zugriffslisten-TCP

Richtlinienzuordnung global_policy

 Class TCP

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

service-policy global

Zusätzliche Informationen:

Phase: 8

Typ: NAT

Untertyp: pro Sitzung

Ergebnis: ZULÄSSIG

Verstrichene Zeit: 366 ns

Konfiguration:

Zusätzliche Informationen:

Phase: 9

Typ: IP-OPTIONEN

Untertyp:

Ergebnis: ZULÄSSIG

Verstrichene Zeit: 366 ns

Konfiguration:

Zusätzliche Informationen:

Ergebnis:

input-interface: INSIDE(vrfid:0)

Eingabestatus: nach oben

Eingabeleitungsstatus: aktiv

Ausgabeschnittstelle: INSIDE(vrfid:0)

Ausgabestatus: aktiv

Ausgabeleitungsstatus: aktiv

Aktion: Drop

Benötigte Zeit: 54168 ns

Verwerfungsgrund: (tcp-not-syn) Erstes TCP-Paket nicht SYN, Verwerfungsort: Frame snp_sp:7459 flow (NA)/NA

Wichtigste Punkte

- Die Add-Flow-Nachricht erreichte 08:14:20.630521, während SYN/ACK ~2 ms zuvor bei 08:14:20.628690 lag. Dies ist die Rennbedingung.

- Das SYN/ACK-Paket wird von der Firewall mit tcp-not-syn-ASP-Grund verworfen. Beachten Sie, dass die Firewall in Phase 4 versucht hat zu identifizieren, ob ein bekannter Flow-Besitzer vorhanden war, aber keinen Flow-Besitzer gefunden hat. Daher hat sie versucht, ein Flow-Besitzer zu werden.

Diese Ausgabe zeigt eine Ablaufverfolgung des SYN/ACK-Werts an, wenn die Firewall über den Fluss informiert ist:

```
firepower# show capture CAPI-Paketnummer 3 trace

13 Pakete erfasst

   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>

Phase: 1

Typ: CAPTURE

Untertyp:

Ergebnis: ZULÄSSIG

Verstrichene Zeit: 1708 ns

Konfiguration:

Zusätzliche Informationen:

MAC-Zugriffsliste

Phase: 2

Typ: ACCESS-LIST
```

Untertyp:

Ergebnis: ZULÄSSIG

Verstrichene Zeit: 1708 ns

Konfiguration:

Implizite Regel

Zusätzliche Informationen:

MAC-Zugriffsliste

Phase 3:

Typ: CLUSTER-EVENT

Untertyp:

Ergebnis: ZULÄSSIG

Verstrichene Zeit: 3416 ns

Konfiguration:

Zusätzliche Informationen:

Eingangsschnittstelle: 'INSIDE'

Flow-Typ: STUB

I (0) haben Fluss, gültiger Eigentümer (1).

Phase: 4

Typ: CAPTURE

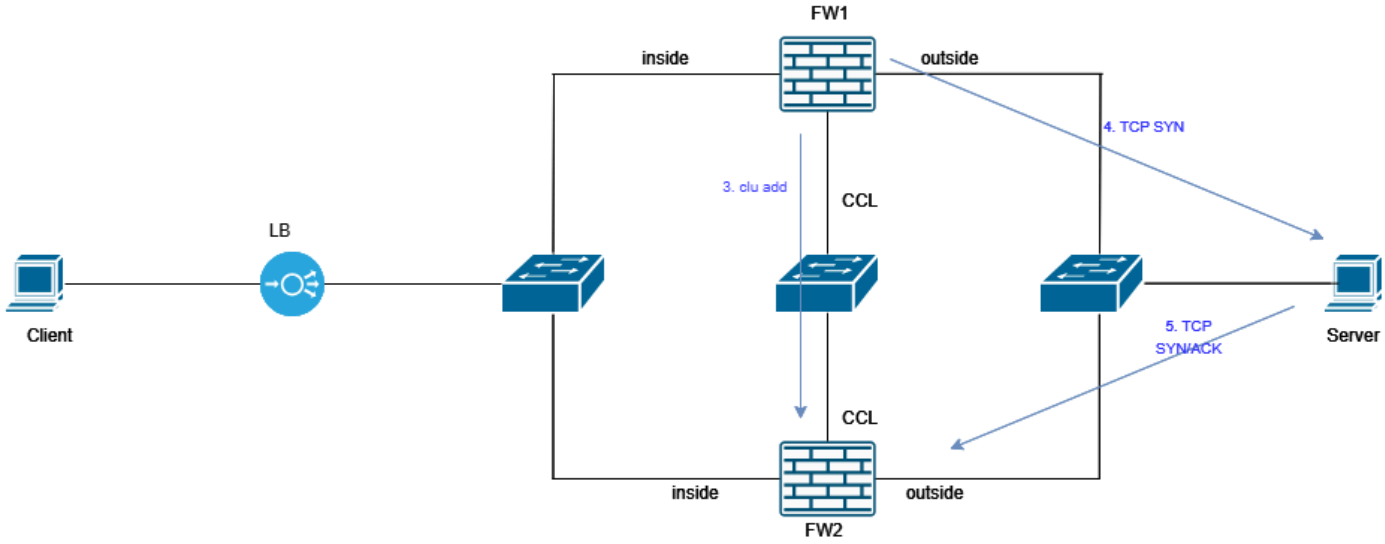
```
Untertyp:

Ergebnis: ZULÄSSIG

Verstrichene Zeit: 7808 ns

Konfiguration:

Zusätzliche Informationen:

MAC-Zugriffsliste

Ergebnis:

input-interface: INSIDE(vrfid:0)

Eingabestatus: nach oben

Eingabeleitungsstatus: aktiv

Aktion: Zulassen

Benötigte Zeit: 14640 ns



1 Paket abgebildet

Feuerkraft#
```

Der Schlüsselpunkt liegt in Phase 3. Die Firewall weiß, dass die Cluster-Einheit 1 der Datenflusseigentümer ist. Mit dem Befehl Cluster-Info anzeigen können Sie sehen, welches Gerät Einheit 0 und welches 1 ist.

Häufig gestellte Fragen

F. Warum sehen wir zeitweilige TCP-Verbindungsprobleme?

A. Da es sich um eine Rennbedingung handelt, geschieht dies zufällig. Die Rennbedingung kann entsprechend visualisiert werden:

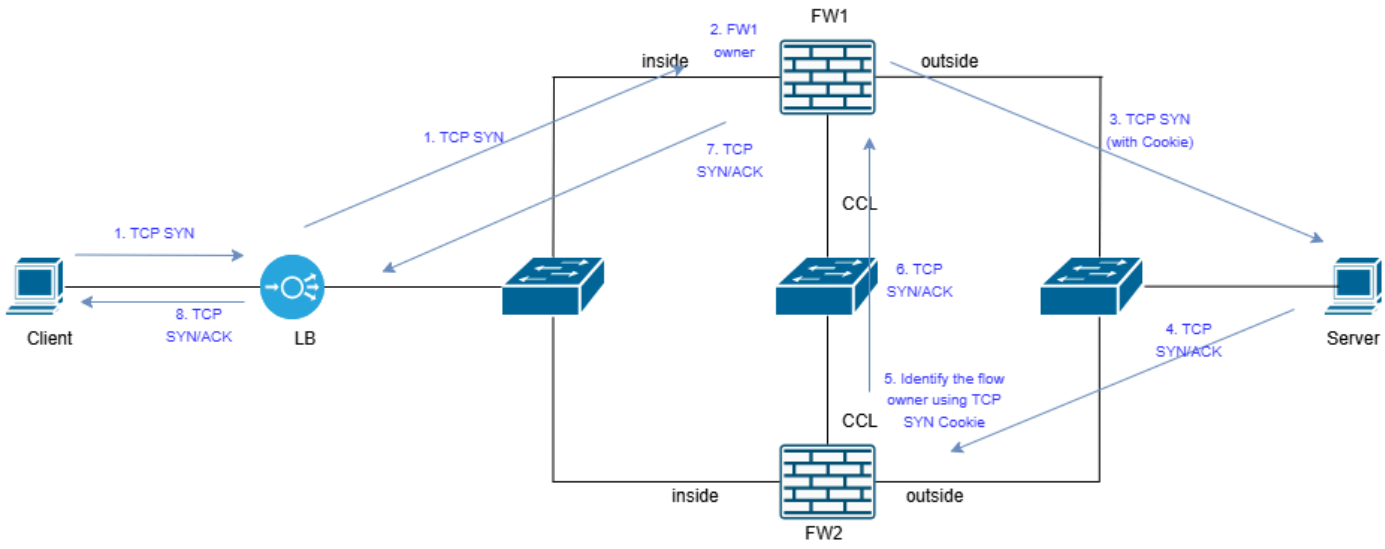


inline_image_0,png

F. Was sind mögliche Lösungen, um die Rennbedingung zu vermeiden?

Antwort:

Lösung 1: Aktivieren Sie die Randomisierung der TCP-Sequenznummer, um den TCP-SYN-Cookie-Mechanismus zu nutzen. In diesem Fall ist die Kommunikation entsprechend strukturiert:



inline_image_1.png

Lösung 2: Beseitigen Sie die Asymmetrie im Netzwerk. Zuerst müssen Sie den Grund für die

Asymmetrie identifizieren. Dies kann eine Anpassung des Port-Channel-Lastausgleichsalgorithmus erfordern, unter anderem eine Neuverkabelung der Port-Channel-Kabel in unterschiedlicher Reihenfolge.

Ursache

Die Hauptursache ist ein Race Condition, der durch eine Cluster-Asymmetrie in der FTD Cluster-Bereitstellung verursacht wird. Die SYN-ACK Pakete vom Server werden von einem anderen FTD Cluster Node verarbeitet als dem, der das anfängliche SYN Paket behandelt hat, wodurch eine ordnungsgemäße TCP Session Einrichtung verhindert wird.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.