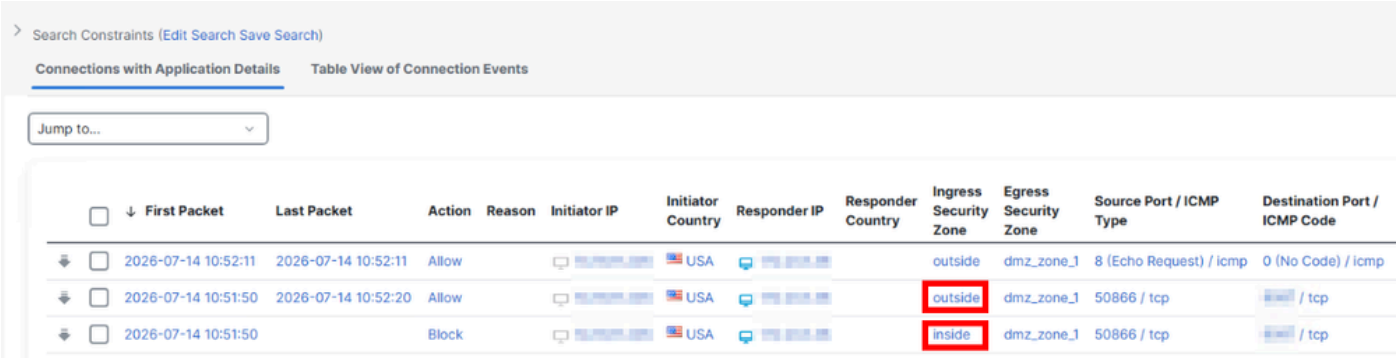
TCPドロップおよびデュアルゾーン接続ログを引き起こすFTD非対称ルーティングのトラブルシューティング

内容

問題

Cisco Secure Firewall Threat Defense(FTD)HAペアの背後にあるDMZでホストされたアプリケーションへの着信接続で、同じ接続試行のトラフィックソースとして2つのセキュリティゾーンが断続的に示されます。FMC接続イベントでは、outsideゾーンから予想される許可された接続が表示され、その後にinsideゾーンに関連付けられた拒否されたトラフィックが表示されます。これにより、TCP接続の失敗が発生します。



- FTDルートとパケットトレーサは、送信元と宛先間の適切なルーティング、NAT、およびルールを確認します。
- ただし、FTDのシステムサポートトレースでは、送信元からの着信パケットだけが表示され、宛先からのリターントラフィックは表示されません。

<#root>

```
> system support trace
.....

10.x.x.200 40812 -> 172.x.x.36 9997 6 AS=0 ID=6 GR=1-1 New firewall session
10.x.x.200 40812 -> 172.x.x.36 9997 6 AS=0 ID=6 GR=1-1 using HW or preset rule order 23, 'intended
10.x.x.200 40812 -> 172.x.x.36 9997 6 AS=0 ID=6 GR=1-1 allow action
```

```
10.x.x.200 40812 -> 172.x.x.36 9997 6 AS=0 ID=6 GR=1-1 app event changes: created
10.x.x.200 40812 -> 172.x.x.36 9997 6 AS=0 ID=9 GR=1-1 Got start of flow event from hardware with
10.x.x.200 40812 -> 172.x.x.36 9997 6 AS=0 ID=9 GR=1-1 Generating an SOF event with rule_id = 2684
10.x.x.200 39194 -> 172.x.x.36 9997 6 AS=0 ID=7 GR=1-1 Got end of flow event from hardware with fl
10.x.x.200 39194 -> 172.x.x.36 9997 6 AS=0 ID=7 GR=1-1 Rule Match Data: rule_id 0, rule_action 0 r
10.x.x.200 39194 -> 172.x.x.36 9997 6 AS=0 ID=7 GR=1-1 Generating an EOF event with rule_id = 2684

10.x.x.200 39194 -> 172.x.x.36 9997 6 AS=0 ID=7 GR=1-1 Received EOF, deleting the snort session
10.x.x.200 39194 -> 172.x.x.36 9997 6 AS=0 ID=7 GR=1-1 Deleting Firewall session flags=0x20190040,
```

- ホストから、接続は最終的にタイムアウトします。
- FTDの「outside」インターフェイスのキャプチャは、10.x.x.200が外部宛先IP 10.x.x.220にSYNおよびエコー要求を送信することを確認します。

<#root>

```
firepower# show capture outside_intf

 1: 13:59:03.051388       10.x.x.200.39194 > 10.x.x.220.9997: S 320277106:320277106(0) win 65535



   2: 13:59:04.063458       10.x.x.200.39194 > 10.x.x.220.9997: S 320277106:320277106(0) win 65535
   3: 13:59:06.073009       10.x.x.200.39194 > 10.x.x.220.9997: S 320277106:320277106(0) win 65535
   4: 13:59:10.081477       10.x.x.200.39194 > 10.x.x.220.9997: S 320277106:320277106(0) win 65535
   5: 13:59:18.090876       10.x.x.200.40812 > 10.x.x.220.9997: S 320277106:320277106(0) win 65535

  6: 13:59:24.127984       10.x.x.200 > 10.x.x.220 icmp: echo request
```

- FTDは、これを内部宛先IPアドレス172.x.x.36にNAT変換します。

<#root>

```
firepower# show capture 1 packet-number 1 trace detail
.....
Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Elapsed time: 3186 ns
Config:

nat (dmz_zone_1,outside_primary) source static dmz1-172.x.x.36 outside-10.x.x.220
Additional Information:
NAT divert to egress interface dmz_zone_1(vrfid:0)
Untranslate 10.x.x.220/0 to 172.x.x.36/0
```

- FTDは、適切な許可ルールを使用して、意図したとおりにトラフィックを許可します。

```
<#root>

Phase: 5
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 0 ns
Config:

access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit object-group ping-echo ifc outside_primary any ifc dmz_zon
access-list CSM_FW_ACL_ remark rule-id 268434459: ACCESS POLICY: nf-policy - Mandatory



access-list CSM_FW_ACL_ remark rule-id 268434459: L7 RULE: intended_allow_rule


object-group service ping-echo
 service-object icmp echo
Additional Information:
 This packet will be sent to snort for additional processing where a verdict will be reached
 Forward Flow based lookup yields rule:
 in  id=0x146e745dbd00, priority=12, domain=permit, deny=false
        hits=3532, user_data=0x0000000000000000, cs_id=0x0, use_real_addr, flags=0x0, protocol=1
        src ip/id=0.0.0.0, mask=0.0.0.0, icmp-type=8, tag=any, ifc=outside_primary(vrfid:0)
        dst ip/id=172.x.x.36, mask=255.255.255.255, icmp-code=0, tag=any, ifc object-group id 4590
```

- その後、同じトラフィックがDMZの宛先172.x.x.36への「dmz_zone_1」インターフェイスで正常に終了します。

```
<#root>

Result:

input-interface: outside_primary(vrfid:0)


input-status: up
input-line-status: up

output-interface: dmz_zone_1(vrfid:0)


output-status: up
output-line-status: up

Action: allow


Time Taken: 106476 ns
```

- FTD dmz_zone_1 インターフェイスのキャプチャは、10.x.x.200が内部宛先IP 10.x.x.220に

SYNおよびエコー要求を送信することを確認します。

<#root>

```
firepower# show capture dmz_intf

 1: 13:59:03.051709       802.1Q vlan#600 P0 10.x.x.200.39194 > 172.x.x.36.9997: S 1245309079:1245

   2: 13:59:04.063610       802.1Q vlan#600 P0 10.x.x.200.39194 > 172.x.x.36.9997: S 1245309079:12
   3: 13:59:06.073146       802.1Q vlan#600 P0 10.x.x.200.39194 > 172.x.x.36.9997: S 1245309079:12
   4: 13:59:10.081630       802.1Q vlan#600 P0 10.x.x.200.39194 > 172.x.x.36.9997: S 1245309079:12
   5: 13:59:18.091166       802.1Q vlan#600 P0 10.x.x.200.40812 > 172.x.x.36.9997: S 1210202278:12

 6: 13:59:24.128197       802.1Q vlan#600 P0 10.x.x.200 > 172.x.x.36 icmp: echo request
```

- ただし、FTD dmz_zone_1インターフェイスでは、内部宛先IP 172.x.x.36からのリターントラフィックは表示されません。
- キャプチャは、宛先172.x.x.36 SYN、ACK、およびエコー応答が代わりにFTDの内部インターフェイスで受信されることを確認します。

<#root>

```
firepower# show capture inside_intf

 1: 13:59:03.051861       802.1Q vlan#667 P0 172.x.x.36.9997 > 10.x.x.200.39194: S 3938871380:3938

   2: 13:59:03.051938       802.1Q vlan#667 P0 10.x.x.200.39194 > 172.x.x.36.9997: R 1245309080:12
   3: 13:59:03.051968       802.1Q vlan#667 P0 10.x.x.200.39194 > 172.x.x.36.9997: R 1245309080:12
   4: 13:59:04.063839       802.1Q vlan#667 P0 172.x.x.36.9997 > 10.x.x.200.39194: S 3938871380:39

   5: 13:59:04.063915       802.1Q vlan#667 P0 10.x.x.200.39194 > 172.x.x.36.9997: R 1245309080:12
   6: 13:59:04.064068       802.1Q vlan#667 P0 10.x.x.200.39194 > 172.x.x.36.9997: R 1245309080:12
  .....
  23: 13:59:24.128411       802.1Q vlan#667 P0 172.x.x.36 > 10.x.x.200 icmp: echo reply
```

- 宛先SYN、ACKが誤ったインターフェイスで返されると、FTDはSYNではない最初のパケ

ットであると識別されるため、トラフィックをドロップします。

注：その他のTCPドロップは非対称ルーティングが原因で発生する可能性があり、FTDのshow asp dropの出力で確認できます。

<#root>

```
Result:

input-interface: inside(vrfid:0)


input-status: up
input-line-status: up
output-interface: outside_primary(vrfid:0)
output-status: up
output-line-status: up
Action: drop
Time Taken: 15572 ns

Drop-reason: (tcp-not-syn) First TCP packet not SYN, Drop-location: frame snp_sp:7337 flow (NA)/NA


.....
firepower# show asp drop
Frame drop:
  SVC Module does not have a channel for reinjection (mp-svc-no-channel)
  SVC Module unable to fragment packet (mp-svc-no-fragment)                  25
  Flow is being freed (flow-being-freed)                                     78
  No valid adjacency (no-adjacency)                                         707
  Flow is denied by configured rule (acl-drop)                             1738


First TCP packet not SYN (tcp-not-syn)                                     760



 TCP failed 3 way handshake (tcp-3whs-failed)                               34
  TCP RST/FIN out of order (tcp-rstfin-ooo)                                1785
  TCP SEQ in SYN/SYNACK invalid (tcp-seq-syn-diff)                            5
  TCP SYNACK on established conn (tcp-synack-ooo)                             1
  TCP packet SEQ past window (tcp-seq-past-win)                              87
  TCP invalid ACK (tcp-invalid-ack)                                           1
  TCP RST/SYN in window (tcp-rst-syn-in-win)                                  1


  DNS Inspect id not matched (inspect-dns-id-not-matched)                    12
  FP L2 rule drop (l2_acl)                                                   34
  Dropped pending packets in a closed socket (np-socket-closed)             145
  NAT failed (nat-xlate-failed)                                               1
  Connection to PAT address without pre-existing xlate (nat-no-xlate-to-pat-pool)
  TCP Proxy retransmited packet drop (tcp-proxy-retransmit-drop)             90
  TCP Proxy probe reset injected (tcp-proxy-probe-rst-injected)             223
  TCP Proxy probe receive drop (tcp-proxy-probe-tcp-probe-drop)             129
  Blocked or blacklisted by the firewall preprocessor (firewall)              2
  Blocked or blacklisted by the stream preprocessor (stream)                301
  Packet is blacklisted by snort (snort-blacklist)                           81
  Packet is blocked as requested by snort (snort-block)                      26
```

環境

- Cisco Secure Firewall Threat Defenseのすべてのモデルとバージョン
- Cisco Secure Firewall Management Centerのすべてのモデルとバージョン
- 同じトラフィックに影響を与える外部ルーティングデバイスまたはプロキシがFTDに隣接して設定されている。

解決方法

1. 誤ったFTDインターフェイスにリターントラフィックを送信しているデバイスで、非対称ルーティングの動作を解決します。

2. それ以外の場合は、非対称ルーティングの解決を試みるようにTCP状態バイパスを設定します。

- これにより、ファイアウォールは、異なるインターフェイスに着信する着信パケットと発信パケットを持つTCPセッションを処理できます。
- バイパスは、非対称ルーティングシナリオでドロップを引き起こす特定のステートフルチェックを無効にしますが、セキュリティのトレードオフを理由に慎重かつ選択的に使用する必要があります。
- これはFTDの外部で発生する非対称ルーティングを回避するための試みであり、その要因を主な手順として解決するのが最善です。

非対称ルーティングのTCP状態チェックのバイパス（TCP状態バイパス）:https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/760/management-center-device-config-76/advanced-access-service-policies.html#ID-2068-00000337

[ビデオ]非対称ルーティングのTCP状態チェックのバイパス（TCP状態バイパス）:https://www.youtube.com/watch?v=v6vJUpPqdYk

原因

この問題は、FTDファイアウォール外部の非対称ルーティングが原因で発生しました。着信パケットはoutside_primaryインターフェイスを介してファイアウォールに入り、dmz_zone_1上の宛先に正しく転送されましたが、172.x.x.36からの戻りパケットは予期されたdmz_zone_1インターフェイスではなくFTD insideインターフェイスに到着しました。

リターントラフィックが元のフローとは異なるインターフェイスに到達したため、FTDステートフルインスペクションエンジンがパケットを無効として扱い、ドロップ理由「tcp-not-syn First TCP packet not SYN」でそれらをドロップしました。 この動作は、複数のインターフェイスで非対称ルーティングが発生している場合のステートフルTCPインスペクションで想定されます。

関連コンテンツ

- 非対称ルーティングのためのTCP状態チェックのバイパス（TCP状態バイパス）
- FTD:FlexConfigポリシーを使用してTCP状態バイパス設定を有効にする方法
- 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。