

セキュアファイアウォールFTD – 電話機の音声ブロックリストのズーム(): 古いVDBが原因

内容

問題

コールが接続されても音声失われるZoom Phoneコールで、ユーザに音声の問題が発生します。FTDはZoom IP範囲からUDPメディアパケットをドロップし、パケットキャプチャおよびASPドロップカウンタでSnortによりブロックリストとして示されます。

具体的な症状は次のとおりです。

- ファイアウォールでCisco Vulnerability Database(VDB)バージョン427以前が実行されている。
- ファイアウォールには、Firepowerデータベースによって提供されるデフォルトのZoom/RTPアプリケーションIDに基づいてZoomトラフィックを許可する必要があるアクセスルールが含まれています。appid.cisco.comによると、このルールはZoom AppIDを介してすべてのポートを許可する必要があります。
 - UserZoom (6243): 80,443/tcp
 - ズームダウンロード(4628):80,443/tcp
 - ズームアップロード(4627):80,443/tcp
 - 会議のズーム(4629):80/tcp
 - RTP音声(2475):5004/udp
 - SIP(426):5060/udp
- ただし、パケットトレーサの出力には、ブロックリストの理由「ファイアウォールプリプロセッサによってブロックまたはブラックリストに登録されている」によってトラフィックがドロップされたことが示されます。

<#root>

Phase: 17

Type: SNORT
Subtype: firewall

Result: DROP

Elapsed time: 345716 ns

Config:

Network 0, Inspection 0, Detection 4, Rule ID 268434438

Additional Information:

Starting rule matching, zone 3 -> 3, geo 840 -> 840, vlan 0, src sgt: 0, src sgt type: unknown, ds

Matched rule ids 268434438 - Block

Result:

input-interface: Outside(vrfid:0)

input-status: up

input-line-status: up

output-interface: Outside(vrfid:0)

output-status: up

output-line-status: up

Action: drop

Time Taken: 640578 ns

Drop-reason: (firewall) Blocked or blacklisted by the firewall preprocessor, Drop-location: frame

- パケットキャプチャは、「snort-blacklist」という理由でドロップを示します。

<#root>

40: 22:52:36.383692 206.247.118.57.60030 > 10.X.X.1.9178: udp 103

Drop-reason: (snort-blacklist) Packet is blacklisted by snort

, Drop-location: frame inspect_dp_snort_snp_drop_frame_wcaller:61 flow (NA)/NA

141: 22:52:36.383723 206.247.118.57.60030 > 10.X.X.1.9178: udp 103

Drop-reason: (snort-blacklist) Packet is blacklisted by snort

, Drop-location: frame inspect_dp_snort_snp_drop_frame_wcaller:61 flow (NA)/NA

142: 22:52:36.385188 206.247.118.57.60030 > 10.X.X.1.9178: udp 44

Drop-reason: (snort-blacklist) Packet is blacklisted by snort

, Drop-location: frame inspect_dp_snort_snp_drop_frame_wcaller:61 flow (NA)/NA

- system support trace出力では、保留中のアプリケーションIDのために、ルール照合中にトラフィックが遅延されます。ただし、トラフィックは誤識別され、ブロックリストに登録されます。IPアドレスは、Zoomの記事「[ネットワークファイアウォールまたはプロキシサーバの設定をズーム](#)」に従ってアクセスを必要とするZoomのパブリックIPです。

<#root>

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1

pending rule order 12, 'allow-outbound', AppID

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1

Deferring trust until a rule is matched

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1

match rule order 28, 'Default Block', action Block

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1 MidRecovery data sent for rule id: 26843

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1 Matched a rule, stop deferring trust

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1 Generating an SOF event with rule_id = 2

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1

deny action

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1 Deleting Firewall session flags=0x20, 1c

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Packet 17168248: UDP, 04/14-14:44:53.110

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Firewall: starting rule matching, zone 1

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1

Firewall: block rule, 'Default Block', force_block

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1

AppID: service: (-1), client: (0), payload: (0), misc: (0)

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Stream: pending block, drop

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Policies: Network 0, Inspection 0, Detect

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1

Verdict: blacklist

- システムサポートトレースは、Zoom IPが応答を試みたときに、「RTP client candidate returned error-invalid (-11)」メッセージと「サードパーティが不明(0)」メッセージを返したことを示しています。

<#root>

206.247.118.55 54808 -> 10.X.X.1 9824 17 AS=0 ID=2 GR=1-1 New AppId session

206.247.118.55 54808 -> 10.X.X.1 9824 17 AS=0 ID=2 GR=1-1

3rd party returned unknown (0)

206.247.118.55 54808 -> 10.X.X.1 9824 17 AS=0 ID=2 GR=1-1

RTP client candidate returned error-invalid (-11)

10.X.X.1 9824 -> 206.247.118.55 54808 17 AS=0 ID=2 GR=1-1 app event changes: created

- FTD show asp dropコマンドでは、ブロックリストの廃棄が迅速に増加していることが示されています。

<#root>

Frame drop:

-----ABBREVIATED-----

Blocked or blacklisted by the firewall preprocessor (firewall)	11224
Blocked or blacklisted by the stream preprocessor (stream)	2354
Fragment reassembly failed (fragment-reassembly-failed)	3
Packet is blacklisted by snort (snort-blacklist)	27173
Packet is blocked as requested by snort (snort-block)	42

環境

- FMCによって管理されるCisco Firepower FTDバージョン7.7.11
- 脆弱性データベース(VDB)バージョン427以前
- Snortバージョン3.3.5.1100-66
- 主にZoom IPサブネット170.114.0.0/16および206.247.0.0/16に影響を与えるが、他のZoom IPを含むことができるトラフィック

解決方法

Cisco Bug ID CSCwu22106 – 回避策 – プレフィルタールの実装

1: Zoomトラフィックのプレフィルタールを作成します。

Policies > Access Control > Prefilterの順に移動し、次の設定で新しいルールを作成します。

- ルール名 : Zoom-Prefilter
- 操作 : Fastpath
- ソースゾーン : 入カインターフェイス
- 宛先ゾーン : 出カインターフェイス
- 送信元アドレス : 任意
- 送信元ポート : any
- Destination Address (宛先アドレス) : IP範囲(170.114.0.0/16、206.247.0.0/16)およびその他をズームします。表示される内容は、「[ネットワークファイアウォールまたはプロキシサーバの設定をズーム](#)」で確認できます。
- 宛先ポート : UDP 10000-64000

2 : 代替アクセスコントロールルールの設定

プレフィルタリングを推奨しない場合は、Zoomアプリケーション識別子を削除し、明示的なIPとポートの照合を使用して、既存のアクセスコントロールポリシー(ACL)ルールを変更します。

- ルール名 : Zoom-Allow
- アクション : 許可
- ソースゾーン : 入カインターフェイス
- 宛先ゾーン : 出カインターフェイス
- 送信元アドレス : 任意
- 送信元ポート : any
- Destination Address (宛先アドレス) : IP範囲(170.114.0.0/16、206.247.0.0/16)およびその他をズームします。表示される内容は、「[ネットワークファイアウォールまたはプロキシサーバの設定をズーム](#)」で確認できます。
- 宛先ポート : UDP / 「Zoom-Phone-Ports」 (範囲10000 64000)
- ロギング : (オプション、許可されたトラフィックのモニタリング用)

3 : 設定変更をFTDデバイスに適用し、双方向オーディオ機能が復元されたことを確認します。

- ASPドロップカウンタを監視して、ブロックリストが停止したことを確認します。

```
device# show asp drop
```

- 正常な双方向トラフィックのパケットキャプチャを確認します。

```
device# show capture
```

4:不具合のCisco Bug ID CSCwu22106は、Cisco Vulnerability Database(VDB)バージョン428のリリースで解決されました。Firepowerデバイスは、この不具合の影響を受けないように、最新のVDBバージョンを実行する必要があります。同様に、関連する不具合のCisco Bug ID CSCwn80786は、VDBバージョン395で解決されました。

原因

Vulnerability Database(VDB)バージョン427内のCisco Secure Firewall Application Identification(CCAP)シグニチャの不具合により、Zoom Phoneのメディアトラフィックが誤って分類され、Snortインスペクションエンジンによってブロックされます。この動作は、Cisco Bug ID CSCwu22106および関連不具合のCisco Bug ID CSCwn80786で追跡されています。この文書では、アプリケーションIDが使用された場合のZoomのIPアドレスとメディアフローの不適切な処理について説明しています。

関連コンテンツ

- [ネットワークファイアウォールまたはプロキシサーバーの設定のズーム](#)
- [ファストパスプレフィルタリングのベストプラクティス](#)
- [Cisco Bug ID CSCwu22106 - VDB 427でズームIPアドレスが誤って処理される](#)
- [Cisco Bug ID CSCwn80786 - Zoom Application DetectorがZoom Phoneのネットワークを検出しない](#)

- [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。