レイヤ7インスペクションのマルチレイヤトラフィックへの影響：Snort3の実装のレビュー

内容

問題

アクセスコントロールポリシー(ACP)でDNSシンクホールルールを有効にした後、Snort 3エンジンバージョンを実行するFirepower Threat Defense(FTD)デバイスで、カプセル化されたVXLANトラフィックが予期せずドロップされ始めました。

・ DNSシンクホールポリシーを有効にすると、VXLANカプセル化トラフィックがドロップします。

・ 外部VXLANヘッダーではなく、内部IPアドレス（100.70.x.xなど）を示す接続イベント。

・ ラボテスト中にSnort 3の実装で予期しない動作が見つかりました。

環境

・ プラットフォーム：FTDハイアベイラビリティ(HA)ペア

・ 該当バージョン：7.6.2.1(Snort 3)

・ 修正済みバージョン：7.6.4+(Snort 3)

解決方法

7.6.2.1での解決策：

##############

手順 1：

プレフィルタポリシー（推奨）

VXLANトラフィックのSnortインスペクションをバイパスするプレフィルタルールを作成します。

・ プレフィルタポリシー

・ アクション： Fastpath （トンネル規則）

・ 送信元： <Outer_VXLAN_Source_IPs>

・ 宛先： <Outer_VXLAN_Destination_IPs>

・ プロトコル：UDP

・ ポート： 4789

ステップ 2：

既存の接続のクリア

・ clear conn address <outer_ip_1> address <outer_ip_2>

プレフィルタポリシーを使用しない場合はルールの順序を調整する

ACPの内部IP許可ルールの前にL7ルール（DNSシンクホール、アプリケーションID）を配置します。

長期的なソリューション：

##############

1. FTD 7.6.4以降へのアップグレード

・ CSCwo54753の解決(PSIRT不具合)

・ 一貫したマルチレイヤインスペクション動作を提供

2. DNSシンクホールの内部ルールと外部ルールの両方を設定します。

・ カプセル化されたトラフィックでDNSシンクホールまたは他のセキュリティインテリジェンス機能を使用する場合。

3. SI以外のレイヤ7機能（URLフィルタリング、アプリケーション制御）の場合：

・ ACPでは、内側のヘッダー・ルールのみが必要です。

・ 外側ヘッダー規則は必要ありません。

マルチレイヤVXLANインスペクション機能の詳細

##

FTDには、セキュリティインテリジェンス(SI)およびレイヤ7機能に対するマルチレイヤインスペクション機能が含まれています。この機能は、Snortが、設定されたレイヤ7ポリシーに基づいて、外部カプセル化ヘッダーと内部ペイロードヘッダーのどちらを検査するかを決定します。

レイヤ7には次の機能があります。

・ DNSシンクホール

・ アプリケーション制御(App-ID)

•URL フィルタリング

•位置情報

・ 侵入防御

主な動作：

##########

ACPでレイヤ7機能が有効になっている場合、Snortは、カプセル化されたパケット（VXLAN、GRE、IP-in-IPなど）の最も内側のヘッダーの検査に移行します。

技術分析：
###############
Snort 3(7.6.2.1)：不具合のある動作

レイヤ7ルールなし：

・ Snortは、Linaからの接続メタデータ（ASAデータパスエンジン）に依存します。

・ トラフィックは、外部ヘッダー規則のみに基づいて許可/拒否されます。

・ 内部ヘッダ検査は行わない。

レイヤ7ルールを使用する場合：

・ SnortはACPチェックを実行し、マルチレイヤインスペクションを適用します。

・ ルールの順序が重要（Snort 3の不具合）

・ Inner IP ruleがL7 rule → Vxlan traffic dropの前に表示される場合 – > Defective Behavior

ラボの出力：
ラボFTD:7.6.2.1:snort3：内部IP ACPルール、L7ルールの順：ドロップ

実習Packet Tracerの詳細：

17:46:48.773778 10.142.133.15:36066 > 10.126.133.15:4789 udp 80

内部(vrfid:0)

オブジェクト_グループ_検索

NGIPS-MODE

| ngipsモード

ACCESS-LIST

NGIPS-EGRESS-INTERFACE-LOOKUP（オプション）

|出力インターフェイスの解決

フロー作成

外部検査

SNORT

Type:

SNORT

Result:

DROP

Config:

Elapsed Time:

814472 ns

追加情報

結果：ドロップ

入力インターフェイス：

内部(vrfid:0)

入力ステータス：

up

入力回線ステータス：

up

出力インターフェイス：

外部(vrfid:0)

出力ステータス：

up

出力回線のステータス：

up

Action:

drop

所要時間：

928908 ns

ドロップの理由：

(firewall)Blocked by the firewall preprocessor <— DROP REASON

ドロップ詳細：

ドロップの場所：frame inspect_dp_snort_snp_drop_frame_wcaller:58フロー(NA)/NA

外部(vrfid:0)

・ L7ルールが内部IPルールより先に出現する場合→Vxlanトラフィックが許可される

DNSシンクホール固有の動作(Snort 3):

・ DNSシンクホールは、ルールの順序付けでトラフィックが許可される場合でも、マルチレイヤインスペクションをトリガーします。

Snort 3(7.6.4+)：修正済み動作

事後修正(CSCwo54753):

・ L7機能が存在する場合、マルチレイヤインスペクションは一貫して有効になります。

・ ルールの順序は動作に影響しません。

・ トラフィック検査は、ルールの位置に関係なく、最も内側のヘッダーに基づいています。

・ DNSシンクホールシナリオでは、ACPで内部ヘッダーと外部ヘッダーの両方が許可されている必要があります。

テストケースの比較マトリックス

テスト シナリオ	FTD 7.6.2.1(Snort 3)	FTD 7.6.4+(Snort 3)	予想される動作
L7ルールに続けて内部IPルール	許可	許可	許可されたトラフィック
内部IPルールがL7ルールに従う	ドロップ(不具合)	許可	許可されたトラフィック
内部IPルールのみ（L7なし）	Blocked	Blocked	ブロック（内部許可なし）
外部IPルールのみ（L7なし）	許可	Blocked	Snort 3は最も内側のヘッダーを検査
外部IP + DNSシンクホールのみ	Blocked	Blocked	L7ルールによる内部検査の実施

内側のIP + DNSシンクホールのみ	Blocked	Blocked	L7ルールによる内部検査の実施

原因

この動作は、Snort 3のセキュリティインテリジェンス機能用のマルチレイヤインスペクション機能が原因で発生します。DNSシンクホール（セキュリティインテリジェンスの一部）が有効になっている場合、Snort 3は、トランスポート層に関係なく、カプセル化されたパケット内の最も内側のIPアドレスを検出および評価するディープパケットインスペクションを実行します。

この問題は、Cisco Bug ID CSCwt12564に次のように記載されています。「ルールでL7条件（URLフィルタリング、アプリケーションID、位置情報など）を使用している場合、またはACPのセキュリティインテリジェンス機能を使用している場合は、一致するルールの内側のヘッダーを持つACPルールが必要です。SIのDNSポリシーの一部であるDNSシンクホールでは、ルールが一致するためにACPの内部ヘッダーと外部ヘッダーの両方が必要です。」

この動作は、レイヤ7またはセキュリティインテリジェンス機能が設定されていない場合に、中継VXLANトラフィックに対して外側のヘッダーのみが評価される通常の動作とは異なります。

関連コンテンツ

- Snort 3コンフィギュレーションガイド
- シスコのテクニカルサポートとダウンロード
- Cisco Bug ID CSCwt12564
- Cisco Bug ID CSCwt07320
- Cisco Bug ID CSCwu75396
- Cisco Bug ID CSCwt58320

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。