第7層檢測對多層流量的影響：Snort3實施回顧

目錄

問題

在存取控制原則(ACP)中啟用DNS Sinkhole規則後，封裝的VXLAN流量開始在執行Snort 3引擎版本的Firepower威脅防禦(FTD)裝置上意外遭到捨棄。

·啟用DNS Sinkhole策略後，VXLAN封裝的流量丟棄。

·顯示內部IP地址（例如100.70.x.x）而不是外部VXLAN報頭的連線事件。

·在實驗室測試期間發現Snort 3實施中存在意外行為。

環境

•平台:FTD高可用性(HA)配對

·受影響的版本：7.6.2.1(Snort 3)

·固定版本：7.6.4+(Snort 3)

解析

7.6.2.1上的解決方案：

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

步驟 1:

預過濾器策略（推薦）

建立預過濾器規則以繞過VXLAN流量的Snort檢查：

·預過濾器策略

•動作:Fastpath（通道規則）

·來源：<Outer_VXLAN_Source_IP>

·目的地：<Outer_VXLAN_Destination_IPs>

•通訊協定:UDP

•連接埠:4789

步驟 2:

清除現有連線

· clear conn address <outer_ip_1> address <outer_ip_2>

如果不使用預過濾器策略，則調整規則排序

在ACP中，將L7規則(DNS Sinkhole、App-ID)置於內部IP允許規則之前。

長期解決方案：

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

1.升級到FTD 7.6.4或更高版本

·解決CSCwo54753（PSIRT缺陷）

·提供一致的多層檢查行為。

2.為DNS沈孔配置內部和外部規則：

·將DNS Sinkhole或其他安全情報功能與封裝流量一起使用時。

3.對於非SI第7層功能（URL過濾、應用控制）：

·在ACP中只需要內部報頭規則。

·不需要外部報頭規則。

有關多層VXLAN檢查功能的更多詳細資訊

##

FTD包括適用於安全情報(SI)和第7層功能的多層檢查功能。此功能可確定Snort是否根據配置的第7層策略檢查外部封裝報頭或內部負載報頭。

第7層功能包括：

· DNS Sinkhole

·應用控制（應用ID）

· URL篩選

·地理定位

·入侵防禦

關鍵行為：

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

在ACP中啟用任何第7層功能時，Snort會轉而檢查封裝封包的最內部標頭（例如VXLAN、GRE、IP-in-IP）。

技術分析：

###############
Snort 3(7.6.2.1) — 故障行為

沒有第7層規則：

· Snort依賴來自Lina的連線後設資料（ASA資料路徑引擎）。

·僅根據外部報頭規則允許/拒絕流量。

·不執行內部報頭檢查。

使用第7層規則：

· Snort執行ACP檢查並執行多層檢查。

·規則順序問題（Snort 3中的缺陷）。

·如果內部IP規則出現在L7規則之前→ Vxlan流量丟棄 — >缺陷行為

實驗輸出：
實驗FTD — 7.6.2.1 — snort3 — 內部IP ACP規則後跟L7規則 — 丟棄

實驗Packet Tracer詳細資訊：

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

內部(vrfid:0)

OBJECT_GROUP_SEARCH

NGIPS-MODE

| ngips-mode

ACCESS-LIST

NGIPS-EGRESS-INTERFACE-LOOKUP

|解析輸出介面

FLOW-CREATE

EXTERNAL-INSPECT

SNORT

Type:

SNORT

Result:

DROP

Config:

運行時間：

814472 ns

其他資訊

Result:drop

輸入介面：

內部(vrfid:0)

輸入狀態：

up

輸入行狀態：

up

輸出介面：

外部(vrfid:0)

輸出狀態：

up

輸出行狀態：

up

Action:

drop

所用時間：

928908 ns

刪除原因：

（防火牆）被防火牆前處理器阻止< — 丟棄原因

Drop Detail:

Drop-location:frame inspect_dp_snort_snp_drop_frame_wcaller:58 flow(NA)/NA

外部(vrfid:0)

·如果L7規則顯示在允許的Vxlan流量的→部IP規則之前

DNS Sinkhole特定行為(Snort 3):

· DNS Sinkhole會觸發多層檢查，即使規則排序在其它情況下會允許流量。

Snort 3(7.6.4+) — 固定行為

修復後(CSCwo54753):

·當存在L7功能時，多層檢查功能始終啟用。

·規則順序不影響行為。

·流量檢測基於最內層的報頭，而不考慮規則位置。

·對於DNS Sinkhole方案，必須在ACP中同時允許內部報頭和外部報頭。

測試用例比較矩陣

測試方案	FTD 7.6.2.1(Snort 3)	FTD 7.6.4+(Snort 3)	預期行為
L7規則後跟內部IP規則	已允許	已允許	允許的流量
內部IP規則遵循L7規則	Dropped(Defect)	已允許	允許的流量
僅內部IP規則（無L7）	已阻止	已阻止	已阻止（無內部允許）
僅外部IP規則（無L7）	已允許	已阻止	Snort 3檢查最內部報頭
僅外部IP + DNS沈孔	已阻止	已阻止	L7規則強制內部檢查
僅內部IP + DNS沈孔	已阻止	已阻止	L7規則強制內部檢查

原因

此行為是由Snort 3對安全情報功能的多層檢查功能引起的。啟用DNS Sinkhole（安全情報的一部分）後，Snort 3會執行深度資料包檢查，無論傳輸層如何，該檢查都會檢測並評估封裝資料包內最內部的IP地址。

此問題已記錄在Cisco錯誤ID CSCwt12564中，其中指出：「如果在規則或ACP的安全情報功能中使用L7條件（url過濾、app-id、地理定位等），則需要具有內部報頭的ACP規則以進行匹配。使用

SI中DNS策略的DNS sinkhole時，ACP需要內部報頭和外部報頭才能匹配規則。」

此行為與正常操作不同，正常操作在沒有配置第7層或安全情報功能時，只為傳輸VXLAN流量評估外部報頭。

相關內容

- Snort 3配置指南
- 思科技術支援與下載
- 思科錯誤ID CSCwt12564
- 思科錯誤ID CSCwt07320
- 思科錯誤ID CSCwu75396
- 思科錯誤ID CSCwt58320

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。