第7层检测对多层流量的影响：Snort3实施回顾

目录

问题

在访问控制策略(ACP)中启用DNS Sinkhole规则后，封装的VXLAN流量开始在运行Snort 3引擎版本的Firepower威胁防御(FTD)设备上意外丢弃。

·启用DNS Sinkhole策略后VXLAN封装流量丢弃。

·显示内部IP地址（例如，100.70.x.x）而不是外部VXLAN报头的连接事件。

·在实验室测试期间发现Snort 3实施存在意外行为。

环境

•平台：FTD高可用性(HA)对

·受影响的版本：7.6.2.1(Snort 3)

·固定版本：7.6.4+(Snort 3)

分辨率

7.6.2.1上的解决方案：

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

步骤 1：

预过滤器策略（推荐）

创建预过滤器规则以绕过VXLAN流量的Snort检查：

·预过滤器策略

•操作:快速路径（隧道规则）

·来源：<Outer_VXLAN_Source_IPs>

•目的地：<Outer_VXLAN_Destination_IPs>

•协议：UDP

·端口：4789

步骤 2：

清除现有连接

· clear conn address <outer_ip_1> address <outer_ip_2>

如果未使用预过滤器策略，则调整规则排序

在ACP中，将L7规则(DNS Sinkhole、App-ID)置于内部IP允许规则之前。

长期解决方案：

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

1.升级到FTD 7.6.4或更高版本

·解决CSCwo54753（PSIRT缺陷）

·提供一致的多层检测行为。

2.为DNS Sinkhole配置内部和外部规则：

·将DNS Sinkhole或其他安全情报功能与封装流量配合使用时。

3.对于非SI第7层功能（URL过滤、应用控制）：

·在ACP中只需要内部报头规则。

·不需要外部报头规则。

有关多层VXLAN检测功能的详细信息

##

FTD包括针对安全情报(SI)和第7层功能的多层检测功能。此功能确定Snort是基于配置的第7层策略检查外部封装报头还是内部负载报头。

第7层功能包括：

· DNS Sinkhole

·应用控制（应用ID）

•URL 过滤

·地理定位

•入侵防御

关键行为：

##########

在ACP中启用任何第7层功能时，Snort将转向检查封装数据包（例如，VXLAN、GRE、IP-in-IP）的最内部报头。

技术分析：

###############
Snort 3(7.6.2.1) — 有缺陷的行为

没有第7层规则：

· Snort依赖来自Lina（ASA数据路径引擎）的连接元数据。

·仅根据外部报头规则允许/拒绝流量。

·不执行内部报头检查。

使用第7层规则：

· Snort执行ACP检查和实施多层检查。

·规则顺序问题（Snort 3中的缺陷）。

·如果内部IP规则出现在L7规则之前→Vxlan流量丢弃 — > Defective Behavior

实验输出：
LAB FTD — 7.6.2.1 — snort3 — 内部IP ACP规则后跟L7规则 — 丢弃

实验Packet Tracer详细信息：

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

内部(vrfid:0)

OBJECT_GROUP_SEARCH

NGIPS模式

| ngips-mode

访问列表

NGIPS-EGRESS-INTERFACE-LOOKUP

|解析出口接口

流创建

EXTERNAL-INSPECT

SNORT

type：

SNORT

结果：

丢弃

Config :

运行时间:

814472 ns

Additional Information

结果：丢弃

输入界面:

内部(vrfid:0)

输入状态：

up

输入行状态：

up

输出接口:

外部(vrfid:0)

输出状态：

up

输出行状态：

up

操作：

丢弃

所用时间：

928908 ns

删除原因：

（防火墙）被防火墙预处理器阻止< — 丢弃原因

删除详细信息：

放置位置：frame inspect_dp_snort_snp_drop_frame_wcaller:58 flow(NA)/NA

外部(vrfid:0)

·如果L7规则出现在Inner IP rule → Vxlan traffic allowed之前

DNS Sinkhole特定行为(Snort 3):

· DNS Sinkhole会触发多层检查，即使规则排序在其它情况下会允许流量。

Snort 3(7.6.4+) — 固定行为

修复后(CSCwo54753):

·当存在L7功能时，将一致启用多层检查。

·规则顺序不影响行为。

·流量检测基于最内部的报头，而不考虑规则位置。

·对于DNS Sinkhole方案，必须在ACP中同时允许内部报头和外部报头。

测试用例比较表

测试场景	FTD 7.6.2.1(Snort 3)	FTD 7.6.4+(Snort 3)	预期行为
L7规则后跟内部IP规则	允许	允许	允许的流量
内部IP规则遵循L7规则	已丢弃（缺陷）	允许	允许的流量
仅内部IP规则（无L7）	已阻止	已阻止	已阻止（无内部允许）
仅外部IP规则（无L7）	允许	已阻止	Snort 3检查最内部信头
仅外部IP + DNS Sinkhole	已阻止	已阻止	L7规则实施内部检查
仅内部IP + DNS Sinkhole	已阻止	已阻止	L7规则实施内部检查

原因

此行为是由Snort 3对安全情报功能的多层检测功能引起的。启用DNS Sinkhole（安全情报的一部分）后，Snort 3会执行深度数据包检测，无论传输层如何，该检测都会检测并评估封装数据包内最内部的IP地址。

Cisco Bug ID CSCwt12564（仅限注册用户）中记录了此问题，其中指出：“如果在规则或ACP的安全情报功能中使用L7条件（URL过滤、应用ID、地理定位等），则需要具有内部报头的ACP规则来

匹配规则。使用SI中DNS策略的DNS sinkhole时，ACP需要内部报头和外部报头才能匹配规则。”

此行为与正常操作不同，在正常操作中，如果未配置第7层或安全情报功能，则仅针对中转VXLAN流量评估外部报头。

相关内容

- Snort 3配置指南
- 思科技术支持和下载
- Cisco Bug ID CSCwt12564
- Cisco Bug ID CSCwt07320
- Cisco Bug ID CSCwu75396
- Cisco Bug ID CSCwt58320

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。