Impact of Layer 7 Inspection on Multi-Layer Traffic: Review of Snort3 Implementation

Contents

Issue

After enabling DNS Sinkhole rules in an Access Control Policy (ACP), encapsulated VXLAN traffic began getting dropped unexpectedly on Firepower Threat Defense (FTD) devices running Snort 3 engine versions.

• VXLAN encapsulated traffic drops after enabling DNS Sinkhole policy.

• Connection events showing inner IP addresses (for example, 100.70.x.x) instead of outer VXLAN headers.

• Unexpected behavior found with Snort 3 implementation during Lab Testing.

Environment

• Platform: FTD High Availability (HA) Pair

• Affected Version: 7.6.2.1 (Snort 3)

• Fixed Version: 7.6.4+ (Snort 3)

Resolution

Solution on 7.6.2.1:

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

Step 1:

Prefilter Policy (Recommended)

Create a Prefilter rule to bypass Snort inspection for VXLAN traffic:

• Prefilter Policy

• Action: Fastpath (Tunnel Rule)

• Source: <Outer_VXLAN_Source_IPs>

• Destination: <Outer_VXLAN_Destination_IPs>

• Protocol: UDP

• Port: 4789

Step 2:

Clear Existing Connections

• clear conn address <outer_ip_1> address <outer_ip_2>

Adjust Rule Ordering if not using prefilter Policy

Place L7 rules (DNS Sinkhole, App-ID) ahead of inner IP permit rules in ACP.

Long-Term Solution:

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

1. Upgrade to FTD 7.6.4 or Later

• Resolves CSCwo54753 (PSIRT DEFECT)

• Provides consistent multi-layer inspection behavior.

2. Configure both Inner and Outer Rules for DNS Sinkhole:

• When using DNS Sinkhole or other Security Intelligence features with encapsulated traffic.

3. For Non-SI Layer 7 Features (URL Filtering, App Control):

• Only inner header rules are required in ACP.

• Outer header rules are not necessary.

More Details about Multi-Layer VXLAN Inspection Feature

##

FTD includes a multi-layer inspection capability for Security Intelligence (SI) and Layer 7 features. This feature determines whether Snort inspects outer encapsulation headers or inner payload headers based on configured Layer 7 policies.

Layer 7 Features Include:

• DNS Sinkhole

• Application Control (App-ID)

• URL Filtering

• Geolocation

• Intrusion Prevention

Key Behavior:

###########

When any Layer 7 feature is enabled in the ACP, Snort shifts to inspecting the innermost headers of encapsulated packets (for example, VXLAN, GRE, IP-in-IP).

Technical Analysis:
###############
Snort 3 (7.6.2.1) - Defective Behavior

Without Layer 7 Rules:

• Snort relies on connection metadata from Lina (ASA datapath engine).

• Traffic is allowed/denied based on outer header rules only.

• Inner header inspection is not performed.

With Layer 7 Rules:

• Snort performs ACP checks and enforces multi-layer inspection.

• Rule order matters (defect in Snort 3).

• If Inner IP rule appears ahead of L7 rule → Vxlan traffic drop --> Defective Behavior

LAB Output:
LAB FTD -- 7.6.2.1 -- snort3 -- Inner IP ACP rule followed by L7 rule -- Drop

Lab Packet Tracer Details:

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

Inside(vrfid:0)

OBJECT_GROUP_SEARCH

NGIPS-MODE

| ngips-mode

ACCESS-LIST

NGIPS-EGRESS-INTERFACE-LOOKUP

| Resolve Egress Interface

FLOW-CREATION

EXTERNAL-INSPECT

SNORT

Type:

SNORT

Result:

DROP

Config:

Elapsed Time:

814472 ns

Additional Information

Result: drop

Input Interface:

Inside(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:

928908 ns

Drop Reason:

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

Drop Detail:

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

Outside(vrfid:0)

• If L7 rule appears ahead of Inner IP rule → Vxlan traffic allowed

DNS Sinkhole Specific Behaviour (Snort 3):

• DNS Sinkhole triggers multi-layer inspection even when rule ordering would otherwise permit traffic.

Snort 3 (7.6.4+) - Fixed Behavior

Post-Fix (CSCwo54753):

• Multi-layer inspection is enabled consistently when L7 features are present.

• Rule order does not impact behavior.

• Traffic inspection is based on innermost headers regardless of rule position.

• Both inner and outer headers must be permitted in ACP for DNS Sinkhole scenarios.

Test Case Comparison Matrix

Test Scenario	FTD 7.6.2.1 (Snort 3)	FTD 7.6.4+ (Snort 3)	Expected Behavior
L7 Rule followed by Inner IP Rule	Allowed	Allowed	Traffic Allowed
Inner IP Rule followed L7 Rule	Dropped (Defect)	Allowed	Traffic Allowed
Only Inner IP Rule (No L7)	Blocked	Blocked	Blocked (No inner permit)
Only Outer IP Rule (No L7)	Allowed	Blocked	Snort 3 inspects innermost header
Only Outer IP + DNS Sinkhole	Blocked	Blocked	L7 rule enforces inner inspection
Only Inner IP + DNS Sinkhole	Blocked	Blocked	L7 rule enforces inner inspection

Cause

This behavior is caused by Snort 3's multi-layer inspection capability for Security Intelligence features. When DNS Sinkhole (part of Security Intelligence) is enabled, Snort 3 performs deep packet inspection that detects and evaluates the innermost IP addresses within encapsulated packets, regardless of the transport layer.

The issue is documented in Cisco bug ID CSCwt12564, which states: "If using L7 condition (url filtering, app-id, geolocation and so on) in the rule or a security intelligence feature in the ACP, you need an ACP rule with inner header for rules to match. With dns sinkhole, which is part of DNS policy in SI, both inner and outer header are required in an ACP for rules to match."

This behavior differs from normal operation where only outer headers are evaluated for transit VXLAN traffic when no Layer 7 or Security Intelligence features are configured.

Related Content

- Snort 3 Configuration Guide

- Cisco Technical Support & Downloads
- Cisco bug ID CSCwt12564
- Cisco bug ID CSCwt07320
- Cisco bug ID CSCwu75396
- Cisco bug ID CSCwt58320