Impact van Layer 7-inspectie op meerlagig verkeer: beoordeling van de implementatie van Snort3

Inhoud

uitgifte

Nadat DNS Sinkhole-regels waren ingeschakeld in een Access Control Policy (ACP), begon het ingekapselde VXLAN-verkeer onverwacht te dalen op Firepower Threat Defense (FTD)-apparaten met Snort 3-motorversies.

· VXLAN ingekapseld verkeer daalt na het inschakelen van DNS Sinkhole beleid.

· Verbindingsevenementen met binnenste IP-adressen (bijvoorbeeld 100.70.x.x) in plaats van buitenste VXLAN-headers.

· Onverwacht gedrag gevonden bij implementatie van Snort 3 tijdens Lab Testing.

milieu

· Platform: FTD High Availability (HA) Pair

· Betrokken versie: 7.6.2.1 (Snort 3)

· Vaste versie: 7.6.4+ (Snort 3)

resolutie

Oplossing voor 7.6.2.1:

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

Stap 1:

Voorfilterbeleid (aanbevolen)

Maak een voorfilterregel om de Snort-inspectie voor VXLAN-verkeer te omzeilen:

· Voorfilterbeleid

· Actie: FastPath (tunnelregel)

· Bron: <Outer_VXLAN_Source_IPs>

· Bestemming: <Outer_VXLAN_Destination_IPs>

· Protocol: UDP

· Poort: 4789

Stap 2:

Bestaande verbindingen wissen

· Clear CONN adres <outer_ip_1> adres <outer_ip_2>

Regelvolgorde aanpassen als geen voorfilterbeleid wordt gebruikt

Plaats L7-regels (DNS Sinkhole, App-ID) vóór de regels voor interne IP-vergunningen in ACP.

Lange termijn oplossing:

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

1. Upgrade naar FTD 7.6.4 of hoger

· Lost CSCwo54753 (PSIRT DEFECT) op

· Biedt consistent meerlaags inspectiegedrag.

2. Configureer zowel de binnen- als de buitenregels voor DNS Sinkhole:

· Bij gebruik van DNS Sinkhole of andere Security Intelligence-functies met ingekapseld verkeer.

3. Voor niet-SI Layer 7-functies (URL-filtering, App Control):

· Alleen regels voor de binnenste koptekst zijn vereist in ACP.

· Regels voor de buitenste koptekst zijn niet nodig.

Meer informatie over de meerlaagse VXLAN-inspectiefunctie

##########

FTD bevat een meerlaagse inspectiemogelijkheid voor Security Intelligence (SI) en Layer 7-functies. Deze functie bepaalt of Snort de kop van de buitenste inkapseling of de kop van de binnenste lading inspecteert op basis van het geconfigureerde Layer 7-beleid.

Layer 7-functies zijn onder meer:

· DNS Sinkhole

· Toepassingscontrole (App-ID)

•URL-filtering

· Geolocatie

· Intrusion Prevention

Sleutelgedrag:

##########

Wanneer een Layer 7-functie is ingeschakeld in de ACP, schakelt Snort over op het inspecteren van de binnenste headers van ingekapselde pakketten (bijvoorbeeld VXLAN, GRE, IP-in-IP).

Technische analyse:
##################
SNORT 3 (7.6.2.1) - Defect gedrag

Zonder Layer 7-regels:

· Snort vertrouwt op verbindingsmetadata van Lina (ASA datapath engine).

· Verkeer is alleen toegestaan/geweigerd op basis van de regels voor de buitenste koptekst.

· Inner header inspectie wordt niet uitgevoerd.

Met Layer 7-regels:

· Snort voert ACS-controles uit en handhaaft meerlagige inspectie.

· Regel orde zaken (defect in Snort 3).

· Als Inner IP-regel verschijnt vóór L7-regel → VXLAN-verkeersval --> Defect gedrag

LAB-uitvoer:
LAB FTD -- 7.6.2.1 -- snort3 -- Inner IP ACP rule gevolgd door L7 rule -- Drop

Details Lab Packet Tracer:

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

Binnenkant (vrfid: 0)

OBJECT_GROUP_SEARCH

NGIPS-MODUS

| NGIPS-modus

TOEGANGSLIJST

NGIPS-EGRESS-INTERFACE-LOOKUP

| Egress-interface oplossen

STROOMVORMING

EXTERN INSPECTEREN

SNORT

Type:

SNORT

Resultaat:

AFWIJZING

Config:

Verlopen tijd:

814472 NS

Aanvullende informatie

Resultaat: drop

Invoerinterface:

Binnenkant (vrfid: 0)

Invoerstatus:

omhoog

Status invoerlijn:

omhoog

Uitvoerinterface:

Buiten (vrfid: 0)

Uitvoerstatus:

omhoog

Status van uitvoerlijn:

omhoog

Actie:

afwijzing

Tijd genomen:

928908 NS

Reden voor neerzetten:

(firewall) Geblokkeerd door de firewall preprocessor <--- DROP REASON

Details neerzetten:

Vestigingsplaats: frame inspect_dp_snort_snp_drop_frame_wcaller:58 flow (NA)/NA

Buiten (vrfid: 0)

· Als de L7-regel wordt weergegeven vóór de Inner IP-regel → VXLAN-verkeer toegestaan

Specifiek gedrag DNS-sinkhole (Snort 3):

· DNS Sinkhole activeert meerlaagse inspectie, zelfs wanneer regelbestelling anders verkeer zou toestaan.

Snurt 3 (7.6.4+) - Vast gedrag

Post-fix (CSCwo54753):

· Meerlaagse inspectie wordt consistent ingeschakeld wanneer L7-functies aanwezig zijn.

· Regelvolgorde heeft geen invloed op gedrag.

· Verkeersinspectie is gebaseerd op binnenste headers, ongeacht de regelpositie.

· Zowel binnen- als buitenheaders moeten in ACP zijn toegestaan voor DNS Sinkhole-scenario's.

vergelijkingsmatrix voor testcasussen

testscenario	FTD 7.6.2.1 (Snort 3)	FTD 7.6.4+ (Snort 3)	verwacht gedrag
L7-regel gevolgd door innerlijke IP-regel	TOEGESTAAN	TOEGESTAAN	Verkeer toegestaan
Inner IP Rule volgt L7 Rule	Gevallen (defect)	TOEGESTAAN	Verkeer toegestaan
Alleen interne IP-regel (geen L7)	geblokkeerd	geblokkeerd	Geblokkeerd (geen interne vergunning)
Alleen buitenste IP-regel (nr. L7)	TOEGESTAAN	geblokkeerd	Snort 3 inspecteert binnenste header
Alleen buitenste IP + DNS-sinkhole	geblokkeerd	geblokkeerd	L7-regel dwingt interne inspectie af
Alleen binnenste IP + DNS-sinkhole	geblokkeerd	geblokkeerd	L7-regel dwingt interne inspectie af

Oorzaak

Dit gedrag wordt veroorzaakt door de meerlagige inspectiemogelijkheid van Snort 3 voor beveiligingsintelligentie-functies. Wanneer DNS Sinkhole (onderdeel van Security Intelligence) is ingeschakeld, voert Snort 3 een diepe pakketinspectie uit die de binnenste IP-adressen in ingekapselde pakketten detecteert en evalueert, ongeacht de transportlaag.

Het probleem is gedocumenteerd in Cisco bug ID CSCwt12564, waarin staat: "Als u de L7-voorwaarde (URL-filtering, app-id, geolocatie enzovoort) in de regel of een beveiligingsinlichtingenfunctie in de ACP gebruikt, hebt u een ACP-regel met binnenkoptekst nodig om regels te laten overeenkomen. Met dns sinkhole, dat deel uitmaakt van het DNS-beleid in SI, zijn zowel de binnen- als de buitenste header vereist in een ACP voor regels die overeenkomen."

Dit gedrag verschilt van de normale werking waarbij alleen de buitenste headers worden geëvalueerd voor transit VXLAN-verkeer wanneer er geen Layer 7- of Security Intelligence-functies zijn geconfigureerd.

Gerelateerde inhoud

- Configuratiegids voor Snoort 3
- Cisco Technical Support en downloads
- Cisco bug ID CSCwt12564
- Cisco bug ID CSCwt07320
- Cisco bug ID CSCwu75396
- Cisco bug ID CSCwt58320

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.