Impatto dell'ispezione di layer 7 sul traffico multilivello: Revisione dell'implementazione di Snort3

Sommario

Problema

Dopo aver abilitato le regole DNS Sinkhole in un Access Control Policy (ACP), il traffico VXLAN incapsulato ha iniziato a essere scartato in modo imprevisto sui dispositivi Firepower Threat Defense (FTD) con le versioni del motore Snort 3.

· Il traffico incapsulato dalla VXLAN diminuisce dopo l'abilitazione dei criteri DNS Sinkhole.

· Eventi di connessione che mostrano gli indirizzi IP interni (ad esempio, 100.70.x.x) anziché le intestazioni VXLAN esterne.

· Comportamento imprevisto rilevato con l'implementazione di Snort 3 durante i test di laboratorio.

Ambiente

•Piattaforma: Coppia FTD ad alta disponibilità (HA)

· Versione interessata: 7.6.2.1 (Snort 3)

· Versione fissa: 7.6.4+ (Snort 3)

Risoluzione

Soluzione al punto 7.6.2.1:

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

Passaggio 1:

Criterio di prefiltro (scelta consigliata)

Creare una regola di prefiltro per ignorare l'ispezione snort per il traffico VXLAN:

· Criterio di prefiltro

•Azione: Fastpath (Regola Tunnel)

· Fonte: <IP_origine_VXLAN_esterna>

•Destinazione: <IP_destinazione_VXLAN_esterna>

•Protocollo: UDP

•Port: 4789

Passaggio 2:

Cancella connessioni esistenti

· clear conn address <ip_1> address <ip_router_2>

Modifica l'ordinamento delle regole se non si utilizza il criterio di prefiltro

Posiziona le regole L7 (DNS Sinkhole, App-ID) prima delle regole di autorizzazione IP interne in ACP.

Soluzione a lungo termine:

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

1. Aggiornamento a FTD 7.6.4 o versione successiva

· Risoluzione di CSCwo54753 (DIFETTO PSIRT)

· Funzionamento coerente dell'ispezione multilivello.

2. Configurare sia le regole interne che quelle esterne per il sinkhole DNS:

· Quando si utilizza il sinkhole DNS o altre funzionalità di intelligence di sicurezza con traffico incapsulato.

3. Per le funzionalità non SI di layer 7 (filtro URL, controllo app):

· In ACP sono richieste solo regole di intestazione interna.

· Le regole di intestazione esterna non sono necessarie.

Ulteriori dettagli sulla funzione di ispezione VXLAN multilivello

##

FTD include una funzionalità di ispezione multilivello per le funzionalità di Security Intelligence (SI) e Layer 7. Questa funzione determina se Snort controlla le intestazioni di incapsulamento esterno o le intestazioni di payload interno in base ai criteri di livello 7 configurati.

Le Caratteristiche Del Layer 7 Includono:

· Sinkhole DNS

· Controllo applicazione (App-ID)

· Filtro URL

· Geolocalizzazione

· Prevenzione delle intrusioni

Comportamento chiave:

##########

Quando si abilita una funzionalità di layer 7 nel provider di servizi di audioconferenza, Snort passa all'ispezione delle intestazioni più interne dei pacchetti incapsulati (ad esempio, VXLAN, GRE, IP-in-IP).

Analisi tecnica:
##########
Snort 3 (7.6.2.1) - Comportamento difettoso

Senza regole di livello 7:

· Snort si basa sui metadati di connessione di Lina (ASA datapath engine).

· Il traffico è consentito/rifiutato solo in base alle regole dell'intestazione esterna.

· L'ispezione dell'intestazione interna non viene eseguita.

Con regole di livello 7:

· Snort esegue i controlli ACP e applica l'ispezione multilivello.

· Questioni relative all'ordine (difetto nello Snort 3).

· Se la regola IP interna viene visualizzata prima della regola L7 → caduta del traffico Vxlan —> Comportamento difettoso

Uscita LAB
LAB FTD — 7.6.2.1 — snort3 — Regola ACP IP interna seguita da regola L7 — Drop

Dettagli di Lab Packet Tracer:

17:46:48,773778 10.142.133,15:36066 > 10.126.133,15:4789 udp 80

Interno (vrfid:0)

CERCA_GRUPPO_OGGETTI

MODALITÀ NGIPS

| modalità ngips

ACCESS-LIST

NGIPS-ROUTE-INTERFACE-LOOKUP

| Interfaccia di risoluzione in uscita

CREAZIONE DEL FLUSSO

ISPEZIONE ESTERNA

SNORT

Tipo:

SNORT

Risultato:

DROP

Config:

Tempo trascorso:

814472 ns

Ulteriori informazioni

Risultato: drop

Interfaccia di ingresso:

Interno (vrfid:0)

Stato input:

attivo

Stato linea di input:

attivo

Interfaccia di output:

Esterno (vrfid:0)

Stato output:

attivo

Stato linea di output:

attivo

Azione:

drop

Tempo impiegato:

928908 ns

Motivo eliminazione:

(firewall) Bloccato dal preprocessore del firewall <— MOTIVO DELLA PERDITA

Elimina dettaglio:

Rilascio: frame inspect_dp_snort_snp_drop_frame_wcaller:flusso 58 (NA)/NA

Esterno (vrfid:0)

· Se la regola L7 viene visualizzata prima della regola IP interna → traffico Vxlan consentito

Comportamento specifico del sinkhole DNS (snort 3):

· Il sinkhole DNS attiva l'ispezione multilivello anche quando l'ordinamento delle regole consentirebbe altrimenti il traffico.

Snort 3 (7.6.4+) - Comportamento fisso

Post-correzione (CSCwo54753):

· L'ispezione multilivello è attivata in modo coerente quando sono presenti funzionalità L7.

· L'ordine delle regole non influisce sul comportamento.

· L'ispezione del traffico si basa sulle intestazioni più interne, indipendentemente dalla posizione della regola.

· Sia le intestazioni interne che quelle esterne devono essere consentite in ACP per gli scenari DNS Sinkhole.

Matrice di confronto dei test case

Scenario di test	FTD 7.6.2.1 (Snort 3)	FTD 7.6.4+ (Snort 3)	Comportamento previsto
Regola L7 seguita da Regola IP interna	ALLOWED	ALLOWED	Traffico consentito
Regola IP interna seguita da regola L7	Eliminato (difetto)	ALLOWED	Traffico consentito
Solo regola IP interna (No L7)	Bloccato	Bloccato	Bloccato (nessun permesso interno)

Solo regola IP esterno (No L7)	ALLOWED	Bloccato	Snort 3 ispeziona l'intestazione interna
Solo sinkhole IP esterno + DNS	Bloccato	Bloccato	La regola L7 applica l'ispezione interna
Solo sinkhole IP + DNS interno	Bloccato	Bloccato	La regola L7 applica l'ispezione interna

Causa

Questo comportamento è causato dalla capacità di ispezione multilivello di Snort 3 per le funzioni di Security Intelligence. Quando il sinkhole DNS (parte di Security Intelligence) è abilitato, l'SQL Server 3 esegue un'ispezione approfondita dei pacchetti che rileva e valuta gli indirizzi IP più interni all'interno dei pacchetti incapsulati, indipendentemente dal livello di trasporto.

Il problema è documentato nell'ID bug Cisco CSCwt12564, che afferma: "Se si utilizza la condizione L7 (filtro URL, app-id, geolocalizzazione e così via) nella regola o una funzionalità di intelligence di sicurezza nel provider di servizi di audioconferenza, è necessaria una regola del provider di servizi di audioconferenza con intestazione interna per la corrispondenza delle regole. Con il sinkhole DNS, che fa parte dei criteri DNS in SI, in un provider di servizi di audioconferenza sono necessarie sia l'intestazione interna che quella esterna per consentire la corrispondenza delle regole."

Questo comportamento è diverso dal normale funzionamento, in cui solo le intestazioni esterne vengono valutate per il traffico VXLAN in transito quando non sono configurate funzionalità di layer 7 o Security Intelligence.

Contenuto correlato

- Guida alla configurazione dello Snort 3
- Supporto tecnico Cisco e download
- ID bug Cisco CSCwt12564
- ID bug Cisco CSCwt07320

- ID bug Cisco CSCwu75396
- ID bug Cisco CSCwt58320

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).