Impact de l'inspection de couche 7 sur le trafic multicouche : Examen de la mise en oeuvre de Snort3

Table des matières

Problème

Après l'activation des règles d'entaille DNS dans une politique de contrôle d'accès (ACP), le trafic VXLAN encapsulé a commencé à être abandonné de manière inattendue sur les périphériques Firepower Threat Defense (FTD) exécutant les versions de moteur Snort 3.

· Le trafic encapsulé VXLAN est abandonné après l'activation de la politique DNS Sinkhole.

· Événements de connexion montrant les adresses IP internes (par exemple, 100.70.x.x) au lieu des en-têtes VXLAN externes.

· Comportement inattendu détecté lors de la mise en oeuvre de Snort 3 lors des tests en laboratoire.

Environnement

· Plateforme : Paire haute disponibilité (HA) FTD

· Version concernée : 7.6.2.1 (Snort 3)

· Version fixe : 7.6.4+ (Snort 3)

Résolution

Solution du point 7.6.2.1 :

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

Étape 1:

Stratégie de préfiltrage (recommandée)

Créez une règle de préfiltre pour contourner l'inspection Snort pour le trafic VXLAN :

· Politique de préfiltrage

•Action : Fastpath (règle de tunnel)

•Source : <IPs_Source_VXLAN_Externe>

•Destination : <AdresseIP_deDestination_VXLAN_Externe>

· Protocole : UDP

· Port : 4789

Étape 2:

Effacer les connexions existantes

· clear conn address <ip_routeur_1> adresse <ip_routeur_2>

Ajuster l'ordre des règles si aucune stratégie de préfiltrage n'est utilisée

Placez les règles L7 (DNS Sinkhole, App-ID) avant les règles d'autorisation IP internes dans ACP.

Solution à long terme :

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

1. Mise à niveau vers FTD 7.6.4 ou version ultérieure

· Résout CSCwo54753 (DÉFAUT PSIRT)

· Offre un comportement d'inspection multicouche cohérent.

2. Configurez les règles internes et externes pour l'entaille DNS :

· Lors de l'utilisation de DNS Sinkhole ou d'autres fonctionnalités de sécurité adaptative avec trafic encapsulé.

3. Pour les fonctionnalités non-SI de couche 7 (filtrage des URL, contrôle des applications) :

· Seules les règles d'en-tête internes sont requises dans ACP.

· Les règles d'en-tête externes ne sont pas nécessaires.

Plus d'informations sur la fonction d'inspection VXLAN multicouche

##

FTD inclut une fonctionnalité d'inspection multicouche pour les fonctions Security Intelligence (SI) et Layer 7. Cette fonctionnalité détermine si Snort inspecte les en-têtes d'encapsulation externes ou les en-têtes de charge utile internes en fonction des politiques de couche 7 configurées.

Fonctionnalités de la couche 7 :

· Enfoncement DNS

· Contrôle des applications (App-ID)

· Filtrage des URL

· Géolocalisation

· Prévention des intrusions

Comportement clé :

##########

Lorsqu'une fonctionnalité de couche 7 est activée dans l'ACP, Snort passe à l'inspection des en-têtes les plus internes des paquets encapsulés (par exemple, VXLAN, GRE, IP-in-IP).

Analyse technique :
###############
Snort 3 (7.6.2.1) - Comportement défectueux

Sans les règles de couche 7 :

· Snort s'appuie sur les métadonnées de connexion de Lina (moteur de chemin de données ASA).

· Le trafic est autorisé/refusé en fonction des règles d'en-tête du routeur uniquement.

· L'inspection interne de l'en-tête n'est pas effectuée.

Avec les règles de couche 7 :

· Snort effectue des contrôles de PVA et applique l'inspection multicouche.

· L'ordre des règles est important (défaut dans Snort 3).

· Si la règle IP interne apparaît avant la règle L7 → Abandon du trafic Vxlan —> Comportement défectueux

Résultats des travaux pratiques :
LAB FTD — 7.6.2.1 — snort3 — Règle IP ACP interne suivie de la règle L7 — Abandon

Détails de Packet Tracer :

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

Interne(vrfid:0)

RECHERCHE_GROUPE_OBJETS

NGIPS-MODE

| mode ngips

LISTE D'ACCÈS

NGIPS-EGRESS-INTERFACE-LOOKUP

| Résoudre l'interface de sortie

CRÉATION DE FLUX

CONTRÔLE EXTERNE

RENIFLEUR

type :

RENIFLEUR

Résultat :

CHUTE

Config :

Temps écoulé :

814472 ns

Additional Information

Résultat : laisser tomber

Interface d'entrée :

Interne(vrfid:0)

État d'entrée :

ascendant

État de la ligne d'entrée :

ascendant

Interface de sortie :

Externe(vrfid:0)

État de sortie :

ascendant

État de la ligne de sortie :

ascendant

Action :

laisser tomber

Temps écoulé :

928908 ns

Motif du rejet :

(pare-feu) Bloqué par le préprocesseur du pare-feu <— DROP REASON

Détail du dépôt :

Emplacement de dépôt : frame inspect_dp_snort_snp_drop_frame_wcaller:58 flux (NA)/NA

Externe(vrfid:0)

· Si la règle L7 apparaît avant la règle IP interne → Le trafic Vxlan est autorisé

Comportement spécifique à l'entonnoir DNS (Snort 3) :

· DNS Sinkhole déclenche une inspection multicouche même lorsque l'ordre des règles autoriserait autrement le trafic.

Snort 3 (7.6.4+) - Comportement fixe

Post-réparation (CSCwo54753) :

· L'inspection multicouche est activée de manière cohérente lorsque les fonctionnalités de couche 7 sont présentes.

· L'ordre des règles n'affecte pas le comportement.

· L'inspection du trafic est basée sur les en-têtes les plus internes indépendamment de la position de la règle.

· Les en-têtes internes et externes doivent être autorisés dans ACP pour les scénarios de trames d'entaille DNS.

Matrice de comparaison des scénarios de test

Scénario de test	FTD 7.6.2.1 (Snort 3)	FTD 7.6.4+ (Snort 3)	Comportement attendu
Règle L7 suivie de Règle IP interne	Autorisé	Autorisé	Trafic autorisé
Règle IP interne suivie de la règle L7	Abandonné (Défaut)	Autorisé	Trafic autorisé
Règle IP interne uniquement (pas de couche 7)	Bloqué	Bloqué	Bloqué (pas d'autorisation interne)
Règle IP externe uniquement (pas de couche 7)	Autorisé	Bloqué	Snort 3 inspecte l'en-tête interne

Uniquement l'adresse IP externe + la trappe DNS	Bloqué	Bloqué	La règle L7 applique l'inspection interne
Seule l'empreinte IP interne + DNS	Bloqué	Bloqué	La règle L7 applique l'inspection interne

Motif

Ce comportement est dû à la capacité d'inspection multicouche de Snort 3 pour les fonctions de sécurité adaptative. Lorsque l'entaille DNS (partie de Security Intelligence) est activée, Snort 3 effectue une inspection approfondie des paquets qui détecte et évalue les adresses IP les plus internes dans les paquets encapsulés, quelle que soit la couche transport.

Le problème est documenté dans le bogue Cisco ayant l'ID CSCwt12564, qui indique : "Si vous utilisez une condition L7 (filtrage d'URL, ID d'application, géolocalisation, etc.) dans la règle ou une fonctionnalité d'intelligence de sécurité dans l'ACP, vous avez besoin d'une règle ACP avec un en-tête interne pour que les règles correspondent. Avec dns sinkhole, qui fait partie de la politique DNS dans SI, les en-têtes interne et externe sont requis dans un ACP pour que les règles correspondent."

Ce comportement diffère du fonctionnement normal où seuls les en-têtes externes sont évalués pour le trafic VXLAN de transit lorsqu'aucune fonctionnalité de couche 7 ou de sécurité adaptative n'est configurée.

Autres informations utiles

- Guide de configuration de Snort 3
- Assistance technique de Cisco et téléchargements
- ID de bogue Cisco CSCwt12564
- ID de bogue Cisco CSCwt07320
- ID de bogue Cisco CSCwu75396
- ID de bogue Cisco CSCwt58320

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.