

Pare-feu sécurisé FTD - Liste de blocage audio du téléphone avec zoom ; en raison de VDB plus ancien

Table des matières

Problème

Les utilisateurs rencontrent des problèmes audio avec les appels Zoom Phone lorsque les appels se connectent mais que l'audio est manquant. Le FTD supprime les paquets de support UDP des plages IP de zoom, les affichant comme des blocs répertoriés par Snort dans les captures de paquets et les compteurs de suppression ASP.

Les symptômes spécifiques comprenaient :

- Le pare-feu exécute Cisco Vulnerability Database (VDB) version 427 ou antérieure.
- Le pare-feu contient une règle d'accès qui doit autoriser le trafic Zoom en fonction des ID d'application Zoom/RTP par défaut fournis par la base de données Firepower. La règle doit autoriser tous ces ports via les AppID de zoom, selon appid.cisco.com :
 - Zoom utilisateur (6243) : 80 443/TCP
 - Téléchargement avec zoom (4628) : 80 443/TCP
 - Téléchargement avec zoom (4627) : 80 443/TCP
 - Réunion Zoom (4629) : 80/TCP
 - Audio RTP (2475) : 5004/udp
 - SIP (426) : 5060/udp
- Cependant, la sortie de packet-tracer montre que le trafic est abandonné par la raison de la liste de blocage « Bloqué ou mis sur liste noire par le préprocesseur du pare-feu ».

<#root>

Phase: 17

Type: SNORT
Subtype: firewall

Result: DROP

Elapsed time: 345716 ns

Config:

Network 0, Inspection 0, Detection 4, Rule ID 268434438

Additional Information:

Starting rule matching, zone 3 -> 3, geo 840 -> 840, vlan 0, src sgt: 0, src sgt type: unknown, ds

Matched rule ids 268434438 - Block

Result:

input-interface: Outside(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: 640578 ns

Drop-reason: (firewall) Blocked or blacklisted by the firewall preprocessor, Drop-location: frame

- Les captures de paquets montrent les abandons avec la raison : "liste noire de sniffeurs".

<#root>

40: 22:52:36.383692 206.247.118.57.60030 > 10.X.X.1.9178: udp 103

Drop-reason: (snort-blacklist) Packet is blacklisted by snort

, Drop-location: frame inspect_dp_snort_snp_drop_frame_wcaller:61 flow (NA)/NA

141: 22:52:36.383723 206.247.118.57.60030 > 10.X.X.1.9178: udp 103

Drop-reason: (snort-blacklist) Packet is blacklisted by snort

, Drop-location: frame inspect_dp_snort_snp_drop_frame_wcaller:61 flow (NA)/NA

142: 22:52:36.385188 206.247.118.57.60030 > 10.X.X.1.9178: udp 44

Drop-reason: (snort-blacklist) Packet is blacklisted by snort

, Drop-location: frame inspect_dp_snort_snp_drop_frame_wcaller:61 flow (NA)/NA

- Dans les sorties de suivi de prise en charge système, le trafic est différé pendant la mise en correspondance des règles en raison de l'identification d'application en attente. Cependant, le trafic est mal identifié et bloqué. L'adresse IP est une adresse IP publique Zoom nécessitant un accès conformément à l'article Zoom [Zoom sur le pare-feu réseau ou les paramètres du serveur proxy](#).

<#root>

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1

pending rule order 12, 'allow-outbound', AppID

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1

Deferring trust until a rule is matched

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1

match rule order 28, 'Default Block', action Block

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1 MidRecovery data sent for rule id: 26843

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1 Matched a rule, stop deferring trust

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1 Generating an SOF event with rule_id = 2

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1

deny action

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1 Deleting Firewall session flags=0x20, 1c

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Packet 17168248: UDP, 04/14-14:44:53.110

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Firewall: starting rule matching, zone 1

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1

Firewall: block rule, 'Default Block', force_block

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1

AppID: service: (-1), client: (0), payload: (0), misc: (0)

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Stream: pending block, drop

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Policies: Network 0, Inspection 0, Detect

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1

Verdict: blacklist

- Les traces de prise en charge du système indiquent les messages « RTP client candidate return error-invalid (-11) » et « 3rd party return unknown (0) » lorsque les adresses IP de zoom tentent de répondre.

<#root>

206.247.118.55 54808 -> 10.X.X.1 9824 17 AS=0 ID=2 GR=1-1 New AppId session

206.247.118.55 54808 -> 10.X.X.1 9824 17 AS=0 ID=2 GR=1-1

3rd party returned unknown (0)

206.247.118.55 54808 -> 10.X.X.1 9824 17 AS=0 ID=2 GR=1-1

RTP client candidate returned error-invalid (-11)

10.X.X.1 9824 -> 206.247.118.55 54808 17 AS=0 ID=2 GR=1-1 app event changes: created

- La commande FTD show asp drop montre l'incrémentation rapide des abandons de liste de blocs.

<#root>

Frame drop:

-----ABBREVIATED-----

Blocked or blacklisted by the firewall preprocessor (firewall)	11224
Blocked or blacklisted by the stream preprocessor (stream)	2354
Fragment reassembly failed (fragment-reassembly-failed)	3
Packet is blacklisted by snort (snort-blacklist)	27173
Packet is blocked as requested by snort (snort-block)	42

Environnement

- Cisco Firepower FTD version 7.7.11 géré par FMC
- Vulnerability Database (VDB) version 427 ou antérieure
- Snort version 3.3.5.100-66
- Trafic affectant principalement les sous-réseaux IP Zoom 170.114.0.0/16 et 206.247.0.0/16, mais pouvant inclure d'autres IP Zoom

Résolution

Solution de contournement du bogue Cisco CSCwu22106 - Implémentation de la règle de préfiltrage

1: Créez une règle de préfiltre pour le trafic Zoom.

Accédez à Politiques > Access Control > Prefilter et créez une nouvelle règle avec cette configuration :

- Nom de la règle : Zoom-Préfiltre
- Action : FastPath
- Zone source : INTERFACE D'ENTRÉE
- Zone de destination : INTERFACE DE SORTIE
- Adresse source: tous les modèles
- Port source : tous les modèles
- adresse de destination: Effectuez un zoom sur les plages IP (170.114.0.0/16, 206.247.0.0/16) et sur toutes les autres plages indiquées dans les [paramètres du pare-feu réseau ou du serveur proxy](#).
- Port de destination : UDP 10000-64000

2: Configuration d'une autre règle de contrôle d'accès

Si le préfiltrage n'est pas préférable, modifiez la règle de stratégie de contrôle d'accès existante en supprimant les identificateurs d'application Zoom et en utilisant une correspondance IP et port explicite :

- Nom de la règle : Zoom-Autoriser
- Action : Allow
- Zone source : INTERFACE D'ENTRÉE
- Zone de destination : INTERFACE DE SORTIE
- Adresse source: tous les modèles
- Port source : tous les modèles
- adresse de destination: Effectuez un zoom sur les plages IP (170.114.0.0/16, 206.247.0.0/16) et sur toutes les autres plages indiquées dans les [paramètres du pare-feu réseau ou du serveur proxy](#).
- Port de destination : UDP / "Zoom-Phone-Ports" (plage 10000 64000)

- Journalisation: (facultatif, pour la surveillance du trafic autorisé)

3: Déployez les modifications de configuration sur les périphériques FTD et vérifiez que la fonctionnalité audio bidirectionnelle est restaurée.

- Surveillez les compteurs de dépôt ASP pour confirmer que la liste de blocage s'est arrêtée :

```
device# show asp drop
```

- Vérifier les captures de paquets pour le trafic bidirectionnel réussi :

```
device# show capture
```

4: L'ID de bogue Cisco CSCwu22106 a été résolu dans la version 428 de la base de données de vulnérabilités Cisco (VDB). Les périphériques Firepower doivent exécuter les dernières versions de la base de données de vulnérabilités pour éviter l'impact de ce défaut. De même, le bogue Cisco associé ID CSCwn80786 a été résolu dans la version 395 de VDB.

Motif

Un défaut dans les signatures d'identification d'application Cisco Secure Firewall dans la base de données des vulnérabilités (VDB) version 427 entraîne une classification erronée du trafic multimédia du téléphone Zoom et, par la suite, une liste de blocage par le moteur d'inspection Snort. Ce comportement est suivi sous l'ID de bogue Cisco CSCwu22106 et l'ID de bogue associé CSCwn80786, qui documente la gestion incorrecte des adresses IP de zoom et des flux de média lorsque les ID d'application sont utilisés.

Autres informations utiles

- [Zoom sur les paramètres du pare-feu réseau ou du serveur proxy](#)
- [Méthodes conseillées pour le préfiltrage FastPath](#)

- [ID de bogue Cisco CSCwu22106 - Zoom des adresses IP mal gérées dans VDB 427](#)
- [Cisco bug ID CSCwn80786 - Le détecteur d'application Zoom ne détecte pas les réseaux pour le téléphone Zoom](#)
- [Assistance technique de Cisco et téléchargements](#)

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.