Dépannage du blocage FTD des URL IP privées en raison d'un problème d'analyse SI

Table des matières

Problème

Les périphériques FTD ont commencé à bloquer le trafic interne de production lorsque l'hôte URL contient une adresse IP privée après avoir reçu des mises à jour de flux réseau/URL Security Intelligence de Talos.

Le trafic affecté inclut des URL telles que http://10.54.1.7:8200/v1/sys/health et http://172.31.14.7:9100. Le trafic est classé comme « Adresses IP privées en tant qu'hôte » et bloqué par les politiques de sécurité adaptative Talos avec des verdicts tels que « URL Block », « blacklist » et « si, force_block ». Ce comportement a un impact sur les communications de service internes et les opérations commerciales.

Lors de l'examen des traces de prise en charge du système FTD, ce comportement de blocage a été observé :

```
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 Firewall: allow rule, 'Access_Rule', allow
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 InsightUrlListEventHandler: num_list_matched
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 Generating an EOF event with rule_id = 26845
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 SI: URL security intelligence list id 104862
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 Verdict: blacklist
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 Verdict Reason: si, force_block
```

Environnement

- Cisco FTD version 7.6.4 (géré par FMC)
- Flux Security Intelligence activés avec les catégories d'URL malveillantes
- Services de production internes utilisant des adresses IP privées dans des URL

- Problème survenu après les mises à jour des flux réseau/URL Security Intelligence de Talos

Présentation des journaux de suivi de support système :

```
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 InsightUrlListEventHandler: num_list_matched
```

- Dans les journaux de suivi de prise en charge système, la valeur de catégorie est imprimée.
- Valeur de catégorie : [1048627]
- Le mappage de la valeur de catégorie et du fichier de flux SI correspondant est disponible dans FTD à l'emplacement suivant :

Emplacement dans FTD : /ngfw/var/sf/siurl_download/url.rules

Emplacement dans le fichier Tshoot : /file-contents/var/sf/siurl_download/url.rules

<#root>

```
kkhapeka@tex-7db6f6c675-8kcnb:.../siurl_download$
```

cat url.rules

```
# security intelligence manifest file
si,5915d129-0d33-4e9c-969a-eab3cde32156.lf,1048589,white,any
si,ac0ef862-1cff-11ef-a575-4cf8bc134a1f.lf,1074790408,block,any
si,005056bf-1643-0ed3-0000-030068648887.lf,1048646,block,any
si,127dc4a2-1ea3-4423-a02d-1f02069828ac.lf,1048590,block,any
si,c87fe5d4-5868-11ef-8843-a8b3afb1bf74.lf,1048645,block,any
si,7c51a74a-d984-11ef-8637-e77eccc0d672.lf,1048649,block,any
si,1b117672-7453-478c-be31-b72e89ca4bfc.lf,1048616,block,any
si,2b15cb6f-a3fc-4e0e-a342-ccc5e5806394.lf,1048619,block,any
si,30f9e69c-d64c-479c-821d-0e4edab852ab.lf,1048620,block,any
si,5f8148f1-e5e4-427a-aa3b-ee1c2745f481.lf,1048623,block,any
si,8af156ca-8020-4608-9278-01b8745811b7.lf,1048626,block,any
si,d3899830-d481-4773-b4e2-7daa7acf8f75.lf,1048633,block,any
si,03709ed4-faab-47af-bade-4435f8da11f5.lf,1048615,block,any
si,bde824fd-36dd-4a7c-9cc1-80e40ac7db66.lf,1048632,block,any
si,a27c6aae-8e52-4174-a81a-47c59fecf1c3.lf,1048629,block,any
si,6ba968f4-7a25-4793-a2c8-7cc77f1f1256.lf,1048625,block,any
si,02213098-6d94-4680-8ce8-2d081638d087.lf,1048613,block,any
si,5a0b6d6b-e2c3-436f-b4a1-48248b333b57.lf,1048622,block,any
si,3e2af68e-5fc8-4b1c-b5bc-b4e7cab5c9eb.lf,1048621,block,any
si,2ccda18e-ddff-4f5c-af9a-f0098521b525.lf,1048618,block,any
si,60f4e2ab-d96c-44a0-bd38-830252b67077.lf,1048624,block,any
si,23f2a124-8278-4c03-8c9d-d28fe08b8fc9.lf,1048617,block,any
```

```
si,937cf5e8-76d1-4ba2-a83c-475dc80c6976.lf,1048628,block,any
si,032ba433-c295-11e4-a919-d4ae5275d599.lf,1048614,block,any
si,d7d996a6-6b92-4a56-8f10-e8506e434dd6.lf,1048634,block,any
si,abdc925f-4f85-4504-90a7-c891979af648.lf,1048630,block,any
```

si,8c3e31be-ca41-43c8-87cb-82a35b0f5213.lf,1048627,block,any >>>>>>matching category ID

```
si,b1df3aa8-2841-4c88-8e64-bfaacec71300.lf,1048631,block,any
si,ac0f6900-1cff-11ef-a575-4cf8bc134a1f.lf,1074790407,monitor,any
ac,5846a44a-3d2a-11f0-a12d-7a89a4a10ab3.lf,1048650
kkhapeka@tex-7db6f6c675-8kcnb:.../siurl_download$ pwd
```

Comment interpréter la ou les lignes précédentes :

- Un ID de catégorie a été attribué au contenu du fichier portant le nom « 8c3e31be-ca41-43c8-87cb-82a35b0f5213.lf » : 1048627
- Pour vérifier quelle est la catégorie réelle, ouvrez le fichier à l'aide de vi et de n'importe quel outil d'édition, et le nom de la catégorie est en haut.

<#root>

```
kkhapeka@KKHAPEKA-M-F6H2 Downloads %
```

cat -n 8c3e31be-ca41-43c8-87cb-82a35b0f5213| more

```
     1  #Cisco DNS and URL intelligence feed: URL Malicious >>>>>name of the category
     2  fadoz.metrs.workers.dev/sell/2641c1ef
     3  oauth-opensea.com
     4  account8133944-complaince.com
```

- L'utilisation du chemin logique correspondant aux fichiers de flux d'intelligence de sécurité peut être retracée, et l'un des aspects importants de la collecte de preuves est de télécharger manuellement les fichiers de flux d'intelligence de sécurité de FTD à une machine locale.
- Les flux Security Intelligence sont mis à jour à intervalles réguliers et, lors de la mise à jour des flux, aucun journal des modifications n'existe sur FMC et FTD indiquant les modifications apportées.
- En téléchargeant le flux Security Intelligence, vous pouvez prendre un instantané du flux à ce moment-là et le fournir ultérieurement à la BU/TALOS.

Résolution

La résolution implique la mise à jour des flux Security Intelligence et la mise en oeuvre d'une solution de contournement temporaire en attendant un correctif logiciel permanent.

Étape 1: Mettre à jour les flux Security Intelligence

Mettez à jour les flux Security Intelligence pour obtenir le contenu du flux corrigé de Talos :

Accédez à Stratégies > Intelligence de sécurité dans FMC et déclenchez manuellement une mise à jour de flux, ou attendez que le cycle de mise à jour automatique se termine.

Étape 2: Mettre en oeuvre une solution de contournement temporaire (si le problème persiste)

Si le problème persiste après la mise à jour du flux, ajoutez les URL ou domaines affectés à la liste « Ne pas bloquer » comme solution de contournement temporaire :

Accédez à Policies > Security Intelligence et ajoutez les URL IP privées à la liste « Do not block » sous l'onglet URL.

Étape 3: Réactiver la catégorie d'URL malveillante

Après avoir confirmé que la mise à jour du flux résout le problème, ajoutez à nouveau la catégorie « URL malveillante » à la configuration Security Intelligence :

Accédez à Politiques > Security Intelligence et réactivez la catégorie "URL malveillante" sous la Liste de blocage.

Étape 4: Supprimer les entrées de solution

Supprimez les URL/domaines affectés de la liste « Ne pas bloquer » une fois que le correctif permanent est confirmé et opérationnel.

Étape 5: Validation

Vérifiez que les destinations d'URL IP privées ne sont plus bloquées par Security Intelligence en testant les URL précédemment affectées et en surveillant les événements de connexion dans FMC.

Motif

Le problème provient d'un problème d'analyse du contenu des flux Security Intelligence qui a eu un impact sur le comportement FTD. Dans le flux Security Intelligence, il y avait des URL de plus de 2047 caractères.

Lorsqu'une entrée dépasse la longueur prise en charge, une partie de ce problème peut être due au fait qu'elle a été incorrectement chargée en tant qu'entrée malveillante distincte, ce qui peut bloquer le trafic non lié. Ce comportement est suivi sous l'ID de bogue Cisco : CSCww1135. Le problème a été résolu grâce à des modifications correctives apportées par l'équipe Talos au contenu du flux, avec un correctif logiciel permanent prévu pour une version ultérieure afin d'ajouter des garde-corps empêchant les occurrences futures.

Autres informations utiles

- ID de bogue Cisco : CSCww11335
- 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.