Échec du déploiement FTD du pare-feu sécurisé

Problème

Des interruptions et des pannes de réseau ont été observées sur Cisco Firewall Firepower Threat Defense (FTD). Les incidents répétés ont entraîné un refus du trafic, y compris des communications SNMP, et ont nécessité le redémarrage des périphériques et une surveillance continue pour identifier la cause première et limiter l'impact ultérieur.

Environnement

- Appliances Cisco Secure Firewall Firepower 1140 (impact sur tout modèle FTD)
- Versions du logiciel FTD : 7.4.2.4 (d'autres versions sont également affectées)
- Politiques de contrôle d'accès (ACP) dynamiques basées sur les objets
- Déploiements fréquents de politiques

Résolution

Pour résoudre les problèmes récurrents de basculement et de déploiement de politiques sur les périphériques Cisco Secure Firewall FTD, respectez un ensemble complet d'étapes de dépannage et de correction. Le workflow répertorié est structuré de manière à fournir une séparation et une explication claires de chaque étape, y compris la surveillance, la collecte de données, les diagnostics et les conseils de mise à niveau.

1 : Utilisez des traceurs de paquets pour vérifier le routage et l'accès pour le trafic prévu.

```
firepower# packet-tracer input INPUTNAMEIF tcp SRCIP 54321 DSTIP 443
firepower# packet-tracer input INPUTNAMEIF icmp SRCIP 8 0 DSTIP
```

2 : Utilisez les captures au niveau du FTD pour déterminer si des paquets sont abandonnés lors de l'entrée « par règle configurée » même si une règle et une route valides existent pour le trafic.

```
firepower# capture 1 interface INPUTIFNAME trace detail trace-count 1000 match ip host SRCIP host DSTIP
firepower# capture x type asp-drop all match ip host SRCIP host DSTIP
firepower# show capture
capture 1 type raw-data trace detail trace-count 1000 interface inside [Capturing - 31565 bytes]
  match ip 10.1.1.0 255.255.255.0 any
capture x type asp-drop all [Capturing - 31565 bytes]
  match ip 10.1.1.0 255.255.255.0 any
```

3 : Vérifiez les journaux de messages FTD pour la preuve de défaut ID bogue Cisco CSCwo78475.

```
> expert
admin@FTD-1:~$ sudo su
Password:
root@FTD-1:/Volume/home/admin# cat /ngfw/var/log/messages | grep -E "New inspector|did not finish|swapp
Feb 10 18:35:03 FTD-device SF-IMS[28366]: New inspector is not initializing Identity API because it's a
Feb 10 18:35:03 FTD-device SF-IMS[28366]: New inspector has different policy groups or ABP name to ID m
Feb 10 18:35:10 FTD-device SF-IMS[28366]: Reading the muster data snapshot did not finish in time: 4 se
Feb 10 18:36:22 FTD-device SF-IMS[28366]: Identity API state swapped
```

4 : Associez les horodatages de ces journaux à ceux des journaux de déploiement dans le FTD.

```
Feb 10 18:34:45 FTD-device policy_apply.pl[18923]: INFO  Deployment type is NORMAL_DEPLOYMENT and devic
Feb 10 18:37:03 FTD-device policy_apply.pl[30894]: INFO  finalizeDeviceDeployment - sandbox = /var/cisc
```

5 : Si les FTD sont en haute disponibilité, basculez vers le FTD de secours et vérifiez les mêmes après pour assurer la récupération du trafic.

6 : Si des journaux et des conditions correspondants sont trouvés dans le FTD, le périphérique est affecté par le défaut et peut être mis à niveau vers la version 7.4.3. Entre-temps, les déploiements peuvent être limités aux heures d'ouverture afin de réduire l'impact sur le trafic.

Motif

La cause sous-jacente des impacts observés sur le trafic et des problèmes de déploiement des

politiques est attribuée à un défaut connu affectant le logiciel FTD, notamment :

- ID de bogue Cisco CSCwo78475 : Le trafic rencontre des règles de stratégie de contrôle d'accès (ACP) incorrectes pendant le déploiement de la stratégie sur les périphériques FTD avec des objets dynamiques. Cela peut entraîner un refus du trafic légitime, même si des règles appropriées existent dans la configuration en cours. Corrigé dans la version 7.4.3.

Autres informations utiles

- ID de bogue Cisco CSCwo78475 : Le trafic rencontre des règles ACP incorrectes pendant le déploiement de la stratégie sur FTD avec des objets dynamiques
- Assistance technique de Cisco et téléchargements: 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.