Comprendre les messages de paquet ICMP " ; inaccessible - filtre" ; interdit par l'administrateur

Table des matières

Problème

Comprendre les informations de paquet jointes aux paquets ICMP (Internet Control Message Protocol) « inaccessible - filtre interdit par l'administrateur ».

Exemple de capture Cisco Secure Firewall Threat Defense (FTD) :

<#root>

```
device#

show capture CAPO



106 packets captured

   1: 08:12:45.864243       198.51.100.205.7351 > 192.0.2.2.47668:  udp 111
   2: 08:12:46.400812       198.51.100.205.7351 > 192.0.2.2.47668:  udp 124
   3: 08:12:46.406320       192.0.2.2 > 198.51.100.205 icmp: host 192.0.2.2

unreachable - admin prohibited filter



   4: 08:12:47.936856       198.51.100.205.7351 > 192.0.2.2.47668:  udp 124
   5: 08:12:47.943936       192.0.2.2 > 198.51.100.205 icmp: host 192.0.2.2

 unreachable - admin prohibited filter



   6: 08:12:49.216739       198.51.100.205.7351 > 192.0.2.2.47668:  udp 124
   7: 08:12:49.222278       192.0.2.2 > 198.51.100.205 icmp: host 192.0.2.2

 unreachable - admin prohibited filter



   8: 08:12:50.096079       198.51.100.205.7351 > 192.0.2.2.47668:  udp 124
   9: 08:12:50.106363       192.0.2.2 > 198.51.100.205 icmp: host 192.0.2.2
```

unreachable - admin prohibited filter

Environnement

Il peut être vu dans l'un de ces produits :

- FTD
- Appliance de sécurité adaptable (ASA)

Résolution

Présentation des messages ICMP de type 3, code 13

Les messages ICMP « inaccessible - filtre interdit par l'administrateur » correspondent à ICMP Type 3, Code 13 (Destination inaccessible - communication administrativement interdite). Ces messages indiquent que le trafic a été explicitement refusé par une stratégie de sécurité ou une liste de contrôle d'accès (ACL), au lieu d'être inaccessible en raison de problèmes de connectivité réseau.

Analyse des informations de capture de paquets

Étape 1 : identification de la source des messages de refus ICMP

Examinez la capture de paquets pour identifier les périphériques qui génèrent les réponses ICMP

de type 3, code 13. Dans ce cas, les messages de refus proviennent d'adresses IP spécifiques (192.0.2.2).

Étape 2 : examen des en-têtes de paquet d’origine

Les messages de refus ICMP contiennent des informations sur les paquets d'origine qui ont été bloqués. Cela inclut les adresses IP source et de destination d’origine, les informations de protocole et les numéros de port qui ont déclenché l’interdiction administrative.

Étape 3. Corrélation des messages de refus avec les modèles de trafic

Associez les réponses ICMP aux flux de trafic spécifiques refusés. Par exemple, le trafic UDP vers le port 7351 était rejeté par le périphérique avec l'adresse IP 192.0.2.2 dans la capture CAPO.

Limites de l’analyse de capture de paquets

Lors de l'utilisation de captures de paquets exportées en texte, l'analyse détaillée paquet par paquet peut être limitée par rapport aux fichiers pcap binaires. Pour une analyse complète, les fichiers binaires de capture de paquets (format pcap) fournissent des informations plus complètes, notamment :

- En-têtes de paquet complets et informations utiles
- Informations de synchronisation précises
- Fonctionnalités complètes de décodage de protocole
- Options de filtrage et d'analyse améliorées

Motif

La cause principale est généralement l'une des suivantes :

- ACL configurées pour refuser des flux de trafic spécifiques
- Règles de pare-feu bloquant certains protocoles, ports ou adresses IP

Dans cet exemple, le message a été provoqué par une liste de contrôle d’accès en aval.

Autres informations utiles

- https://datatracker.ietf.org/doc/html/rfc792
- https://datatracker.ietf.org/doc/html/rfc1812
- https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215092-analyze-firepower-firewall-captures-to-e.html

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.