Résoudre les réponses DNS UDP volumineuses échouant via FTD avec l'inspection DNS activée

Table des matières

Problème

Les paquets DNS de grande taille (environ 1 800 à 4 000 octets) échouent lorsque le trafic transite entre des machines virtuelles de différents VLAN via un pare-feu Cisco Firepower Threat Defense (FTD). Le même trafic DNS réussit lorsque la communication s'établit entre les machines virtuelles du même VLAN sans passer par le pare-feu. Au cours du dépannage, il a été découvert que les paquets de réponse DNS fragmentés étaient entièrement réassemblés par le pare-feu FTD lors de leur sortie et envoyés sous forme de grands paquets uniques dépassant la capacité MTU du client, ce qui a provoqué l'abandon des paquets par le client.

Environnement

- Gamme de produits : D'autres plates-formes peuvent également être affectées par le pare-feu Cisco Secure Firewall 4200.
- Version du logiciel: D'abord vu sur le logiciel FTD version 7.6.2.1, d'autres versions de logiciels peuvent également être affectés.
- MTU de l'interface de pare-feu : 9 000 octets
- Inspection DNS activée.
- Ordinateurs clients affectés configurés avec une MTU standard de 1 500 octets.
- Serveurs DNS générant des réponses fragmentées pour les requêtes d'enregistrement SRV volumineuses.

Résolution

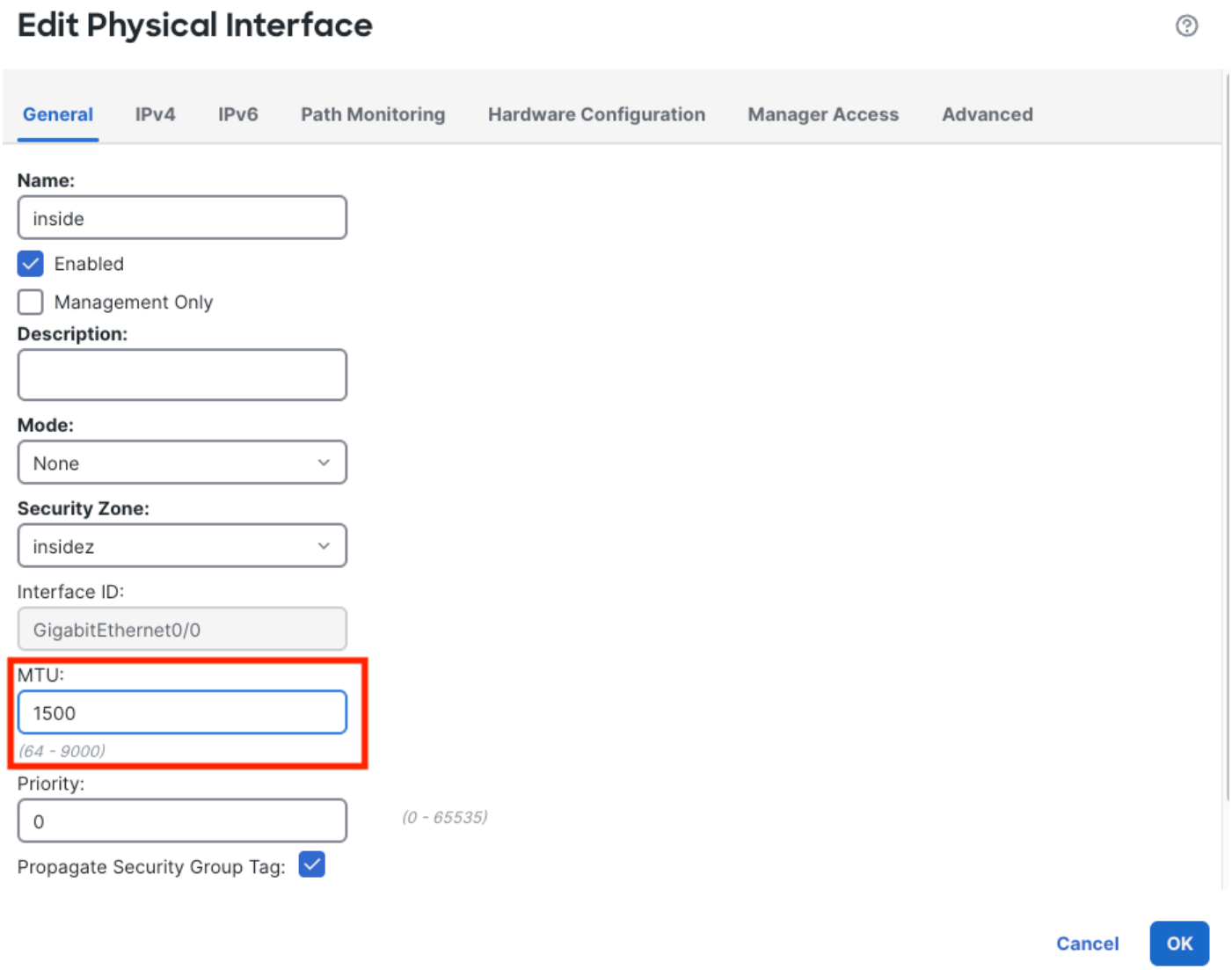
Le problème a été résolu en ajustant la configuration MTU de l'interface de pare-feu. Ces approches peuvent être utilisées pour résoudre ce problème :

Option 1: Ajuster le MTU de l'interface à 1 500 si d'autres périphériques réseau le permettent (recommandé)

Modifiez la MTU de l'interface de sortie du pare-feu de 9 000 à 1 500 octets pour garantir une refragmentation correcte des paquets réassemblés :

```
ASA:
device# configure terminal
device(config)# interface gigabitethernet0/0
device(config-if)# mtu 1500
device(config-if)# exit

FTD:
Change MTU from FMC GUI
```



Vérifiez la configuration MTU :

```
device# show interface gigabitethernet0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is i82580 rev03, BW 1000000 Kbit, DLY 10 usec
  Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
  Available but not configured via nameif
  MAC address 0050.56bb.09c8, MTU 1500
```

Option 2: Désactiver l'inspection DNS (solution de contournement alternative non recommandée)

Remarque : Si la désactivation de l'inspection DNS est acceptable selon les exigences de sécurité et si le pare-feu n'est pas un pare-feu de périmètre, vous pouvez envisager de désactiver l'inspection DNS à partir de la carte de stratégie. (Cela peut également augmenter le nombre total de connexions si le trafic DNS est élevé) :

```
ASA:
device# configure terminal
device(config)# policy-map global_policy
device(config-pmap)# class inspection_default
device(config-pmap-c)# no inspect dns
device(config-pmap-c)# exit

FTD:
> configure inspection dns disable
```

Étapes de vérification

Après avoir implémenté la résolution, vérifiez la fonctionnalité DNS :

Testez la résolution DNS avec des réponses volumineuses :

```
dig @dns_server_ip _ldap._tcp.domain.com SRV
```

Surveiller le traitement des paquets pare-feu :

```
Collect packet packets on ingress and egress interface to analyse in WireShark
```

Motif

Lorsque l'inspection DNS est activée sur FTD, la ligne de pare-feu effectue un réassemblage complet des paquets DNS fragmentés pour permettre au moteur d'inspection (Snort) d'examiner la charge utile DNS complète. Après inspection, si la MTU de l'interface de sortie est supérieure à la taille du paquet réassemblé, le pare-feu transfère le paquet sous la forme d'une seule grande

trame sans le refragmenter.

L'interface de pare-feu est configurée avec une MTU de 9 000 octets, ce qui permet de transmettre des réponses DNS réassemblées (environ 1 884 octets) sous forme de paquets uniques. Cependant, les ordinateurs clients configurés avec une MTU standard de 1 500 octets et n'ont pas pu accepter ces paquets plus volumineux, ce qui a entraîné une perte de trafic.

Le comportement est attendu lorsque l'inspection DNS est activée sur Lina avec des paramètres MTU d'interface supérieurs à la taille de paquet réassemblé.

- Inspection DNS LINA : Effectue un réassemblage complet pour une inspection approfondie des paquets. (Référez-vous à ce défaut DOC CSCwv66007 pour plus de détails.)
- Snort 3 : Réassemblage logique (virtuel) pour inspection sans réassemblage physique.

Autres informations utiles

- Assistance technique de Cisco et téléchargements
- CSCwv66007 (DOC :Clarifier le comportement de réassemblage de fragmentation ASA/FTD avec une fonctionnalité policy-map activée qui nécessite un réassemblage complet)

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.