Désactiver le proxy ARP sur les interfaces FTD en utilisant FlexConfig

Problème

Les hôtes d’une interface FTD ne peuvent pas utiliser les adresses IP attribuées de manière statique et signaler les erreurs de « doublon d’adresse IP » avant de revenir aux adresses 169.254.x.x. L’analyse de capture de paquets révèle que lorsque l’hôte envoie un ARP gratuit (sonde ARP) pour sa propre adresse IP, le pare-feu répond en revendiquant la propriété de cette adresse IP, empêchant ainsi l’attribution statique d’adresses IP.

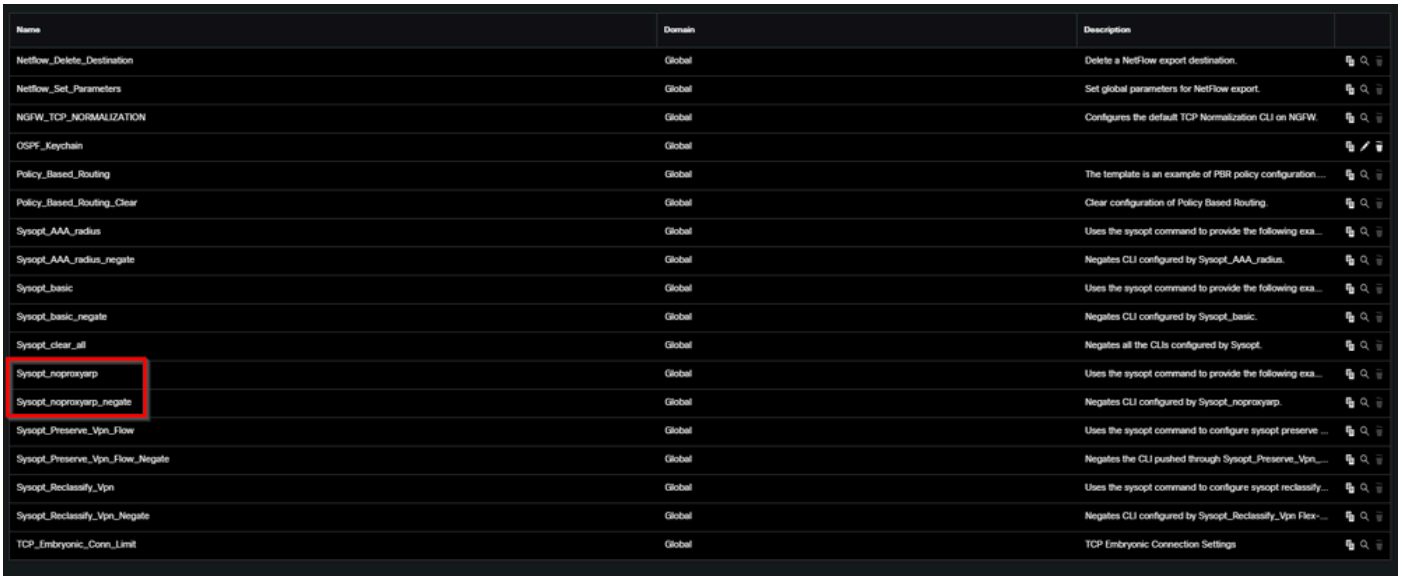
Environnement

- Cisco Secure Firewall 2120 exécutant la version 7.4.4 du logiciel FTD (applicable à toutes les versions et à tous les modèles)
- Cisco Secure Firewall Management Center (FMC) pour la gestion des périphériques
- Proxy ARP activé sur FTD par défaut.

Résolution

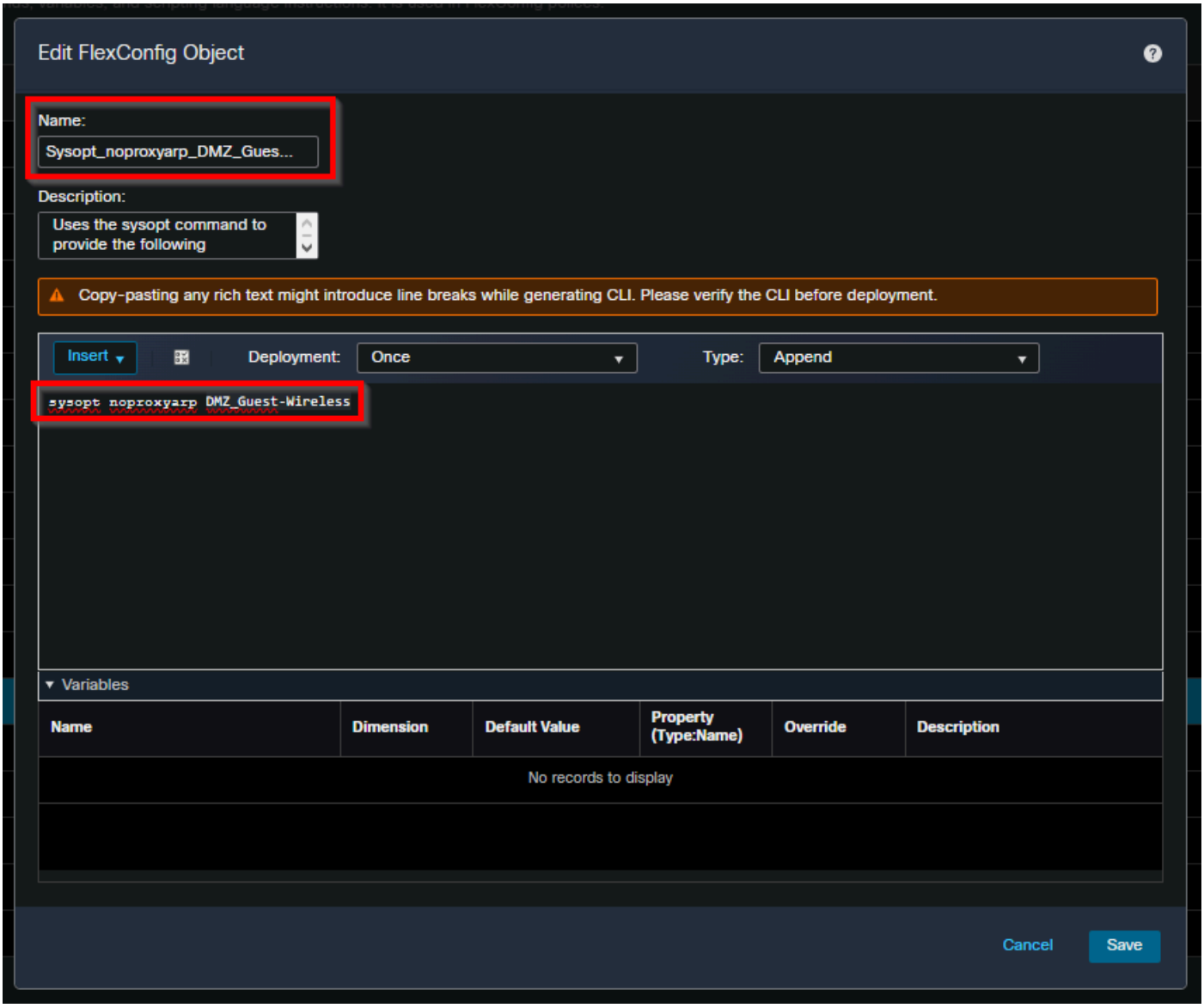
Le problème est résolu en désactivant le proxy ARP sur l'interface affectée à l'aide d'une stratégie FlexConfig déployée via FMC. Cela empêche le pare-feu de répondre aux sondes ARP pour les adresses IP qu'il ne possède pas explicitement.

1 : Accédez à la section FlexConfig dans FMC et créez une nouvelle stratégie FlexConfig pour désactiver le proxy ARP sur l'interface spécifique. Sysopt_noproxyarp et Sysopt_noproxyarp_negate sont des objets par défaut dans FMC et peuvent être clonés pour une utilisation personnalisée.



image_en_ligne_0.png

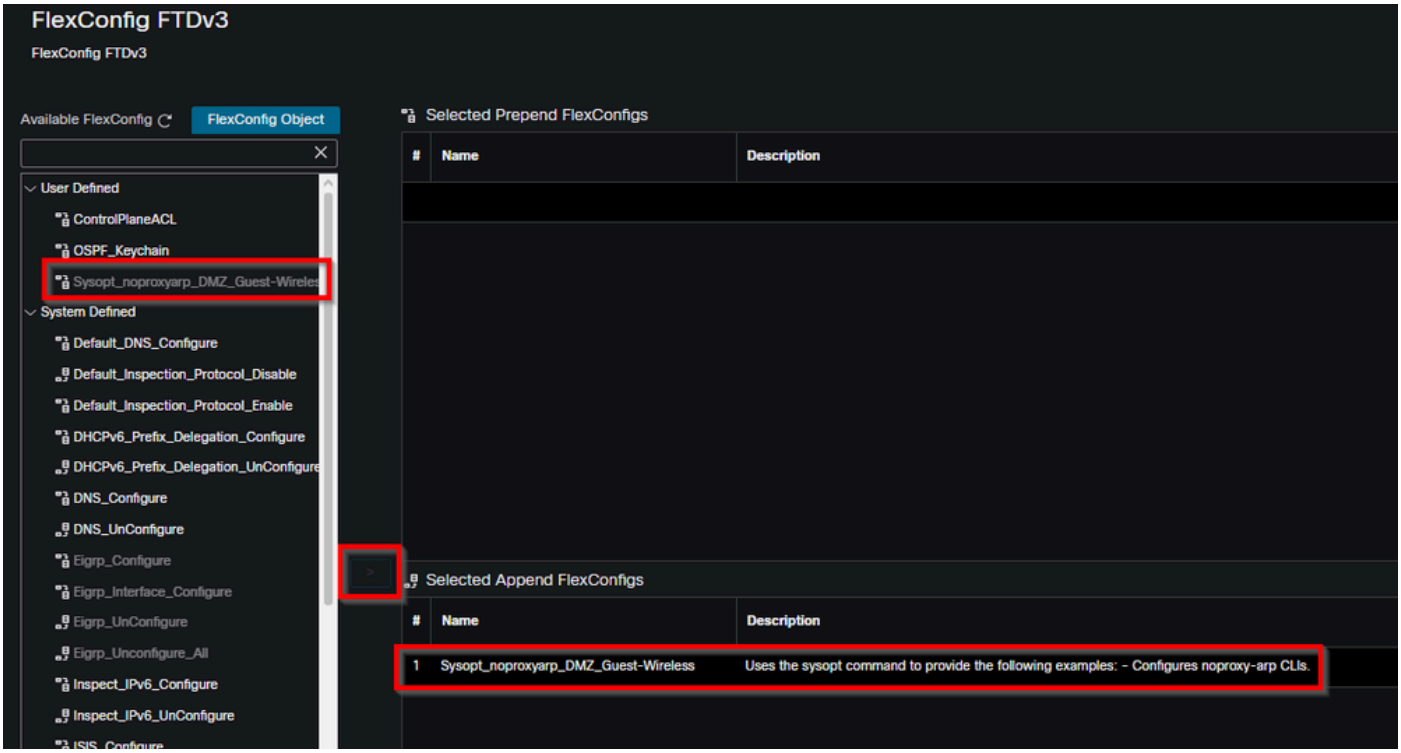
2 : Ajoutez la commande de configuration à la stratégie FlexConfig sysopt noproxyarp IFNAME :



image_inline_1.png

Remplacez IFNAME par le nom réel de votre interface affectée.

3 : Associez le nouvel objet à la stratégie FlexConfig du FTD et déployez-le via FMC. La configuration est appliquée pour désactiver le comportement ARP proxy sur l'interface spécifiée.



image_en_ligne_2.png

4 : Après le déploiement, testez l'affectation d'adresses IP statiques sur l'hôte affecté. Le pare-feu ne doit plus être en mesure de répondre aux sondes ARP pour les adresses IP non attribuées, ce qui permet aux hôtes d'utiliser correctement leurs configurations d'adresses IP statiques sans erreurs d'adresses IP en double.

Le cas échéant, envisagez de désactiver le protocole ARP proxy au niveau de la règle NAT plutôt qu'au niveau de l'interface afin de minimiser l'impact involontaire sur d'autres fonctions réseau. Cela permet un contrôle plus granulaire du comportement du protocole ARP proxy.

Motif

Le protocole ARP (Proxy Address Resolution Protocol) a été activé sur l'interface FTD, ce qui a amené le pare-feu à répondre aux sondes ARP pour les adresses IP qu'il ne possédait pas explicitement. Ce comportement a entraîné la détection par les hôtes d'une condition d'adresse IP dupliquée lors de l'attribution d'adresses statiques. La fonctionnalité ARP proxy du pare-feu répondait avec sa propre adresse MAC lorsque les hôtes exécutaient des requêtes ARP gratuites,

donnant l'impression que l'adresse IP souhaitée était déjà utilisée par un autre périphérique.

Autres informations utiles

- 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.