Configurer la fonction de désactivation de Cisco ASA pour exempter l'appliance virtuelle

Table des matières

[Introduction](#)

[Fonction « Shun » de détection des menaces](#)

[Exemption de l'appliance virtuelle](#)

[Déterminez si l'appliance a été « désactivée ».](#)

Introduction

Ce document décrit comment configurer Cisco ASA pour exempter l'appliance virtuelle du composant de détection des menaces. Le composant de détection des menaces Cisco ASA effectue l'inspection des paquets sur DNS et d'autres protocoles. La prise en charge d'Umbrella recommande ces modifications de configuration ASA pour éviter tout conflit entre cette fonctionnalité et notre appliance virtuelle :

- Exemptez l'appliance virtuelle de la fonction « shun » de détection des menaces décrite dans cet article.
- Exemptez l'appliance virtuelle de l'inspection des paquets DNS pour autoriser le cryptage DNS (DNScrypt) qui est traité dans cet article : Le pare-feu Cisco ASA bloque DNScrypt.

Fonction « Shun » de détection des menaces

Lorsque la fonction « Shun » est activée, l'ASA peut bloquer complètement une adresse IP source qui déclenche des règles de détection des menaces. Pour plus d'informations, consultez l'article Cisco : Fonctionnalité et configuration de la détection des menaces ASA.

L'appliance virtuelle envoie normalement un nombre très élevé de requêtes DNS aux résolveurs de DNS Umbrella. Dans les cas où il y a un problème local de connexion aux résolveurs (comme une panne de réseau temporaire/latence), ces requêtes peuvent échouer. En raison du volume considérable de requêtes envoyées, même un faible pourcentage d'échecs entraîne la désactivation de l'appliance virtuelle par l'ASA ; ce qui entraîne une panne DNS complète pendant un certain temps.

Exemption de l'appliance virtuelle

Remarque : Les commandes de cet article sont indiquées à titre indicatif uniquement. Il est recommandé de consulter un expert Cisco avant d'apporter des modifications à un environnement de production.

Via CLI :

- Pour exempter l'adresse IP de l'appliance d'être désactivée, exécutez cette commande : **no shun**

Via l'interface ASDM :

- Sélectionnez le volet Configuration > Firewall > Threat Detection.
- Pour exempter l'adresse IP de l'appliance d'être désactivée, saisissez une adresse dans le champ 'Réseaux exclus de la désactivation'. Vous pouvez entrer plusieurs adresses ou sous-réseaux séparés par des virgules.

Déterminez si l'appliance a été « désactivée ».

Si ces étapes n'ont pas été suivies, l'appliance peut être « désactivée » dans certaines circonstances, ce qui entraîne une panne DNS.

Lorsque l'appliance virtuelle n'a pas de connectivité externe, la console Cisco ASA enregistre l'événement comme suit :

4|06 juin 2014 14:00:42|401004: Paquet ignoré : 192.168.1.3 ==> 208.67.222.222 sur l'interface interne
4|06 juin 2014 14:00:42|401004: Paquet exclu : 192.168.1.3 ==> 208.67.222.222 sur l'interface interne

Pour afficher la liste des adresses IP actuellement désactivées, exécutez cette commande sur l'ASA : **show shun**

Pour effacer immédiatement les adresses IP actuellement désactivées, exécutez cette commande sur l'ASA : **clear shun**

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.