Résoudre l'avertissement VA " ; est dans un état d'attention" ;

Table des matières

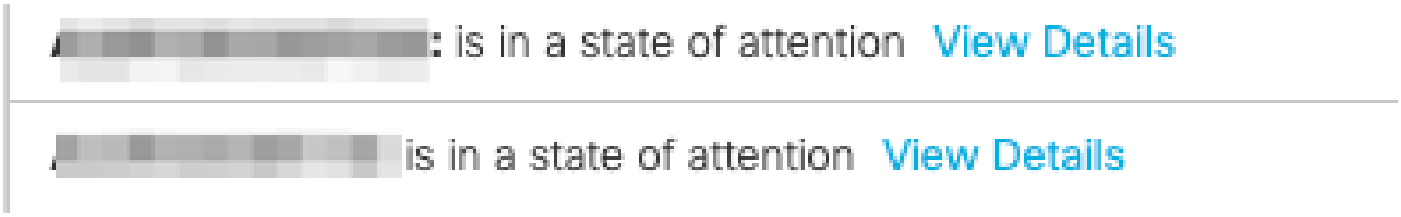
Introduction

Ce document décrit comment résoudre l'avertissement VA indiquant que votre VA "est en état d'attention" lié à l'activation de DNSCrypt.

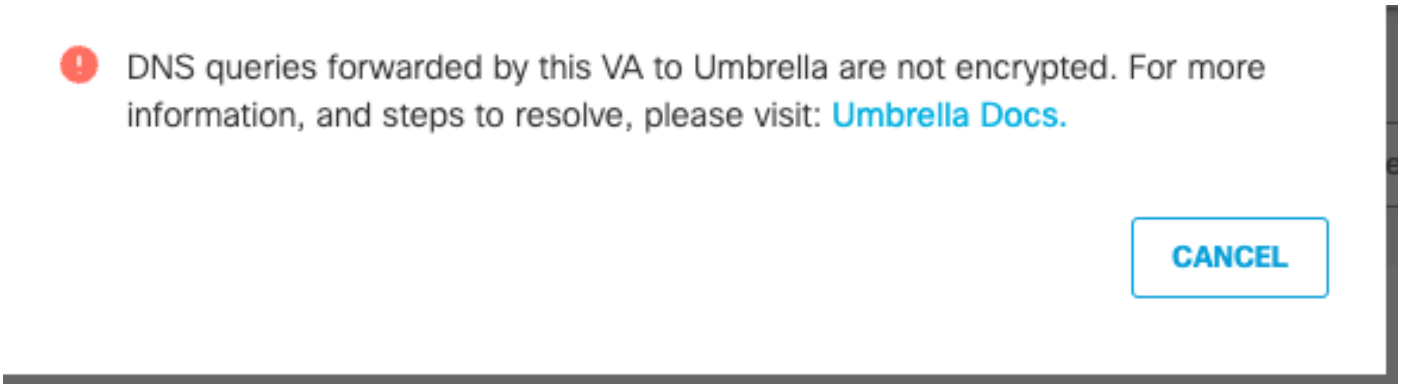
Aperçu

L'appliance virtuelle (VA) prend en charge le cryptage DNSCrypt entre elle-même et les résolveurs DNS (Domain Name System) publics OpenDNS. DNSCrypt crypte les paquets DNS transmis par l'AV, empêchant ainsi l'interception d'informations sensibles. DNSCrypt est activé par défaut pour une protection optimale, mais vous pouvez rencontrer des problèmes si un pare-feu bloque le trafic chiffré entre votre VA et les résolveurs DNS publics.

Le trafic DNS non crypté représente un risque de sécurité que vous devez gérer. Lorsque le cryptage ne peut pas être établi entre votre VA et OpenDNS, votre tableau de bord Umbrella affiche un avertissement indiquant que l'appliance virtuelle concernée « est en état d'attention » pour vous assurer de maintenir la meilleure protection possible.



Si vous cliquez sur Afficher les détails, vous voyez un message indiquant que les requêtes DNS transférées par cette VA à OpenDNS ne sont pas chiffrées.

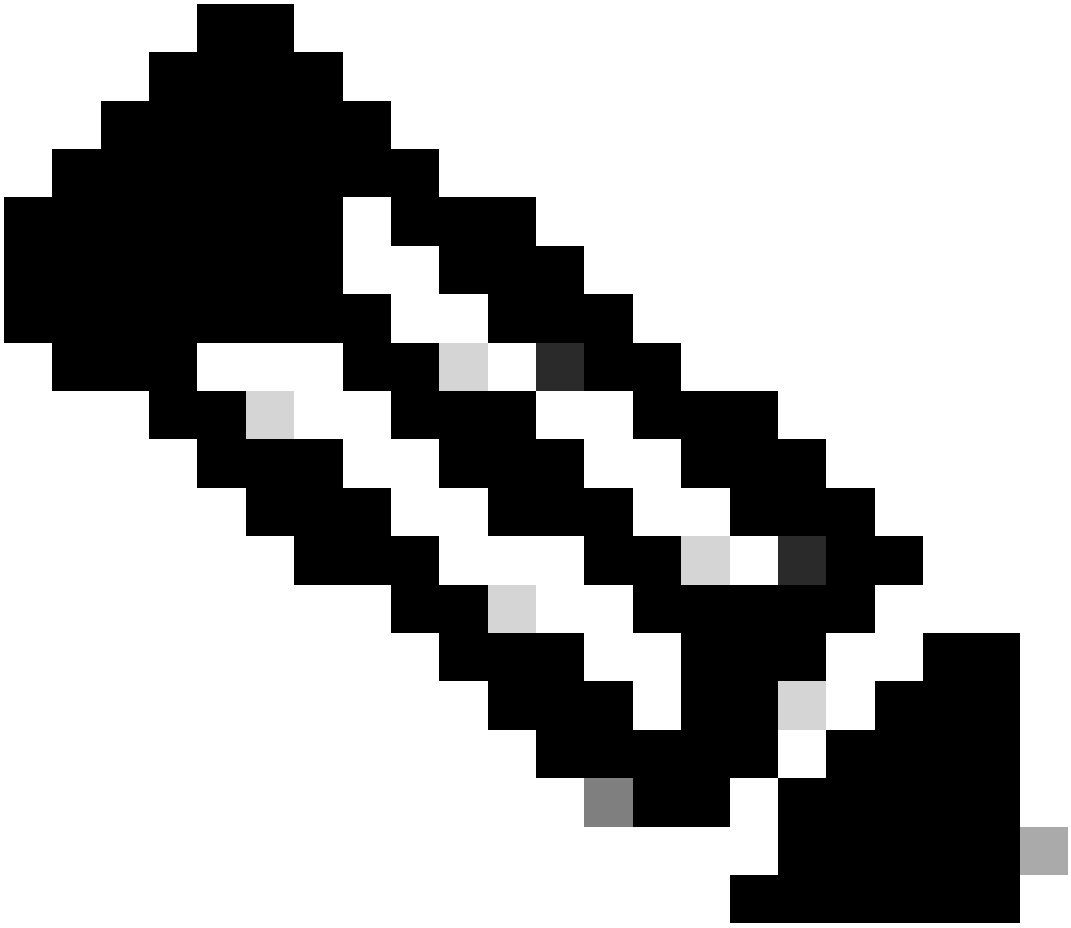


Remarque : DNSCrypt est disponible uniquement dans les appliances virtuelles exécutant la version 1.5.x ou ultérieure. Si vous n'avez qu'une seule appliance virtuelle et qu'elle n'a pas été mise à niveau, ce message apparaît également.

Résoudre l'avertissement DNSCrypt

Pour résoudre l'avertissement et restaurer la protection DNSCrypt :

1. Vérifiez la configuration de votre pare-feu ou de votre système de prévention des intrusions (IPS)/système de détection des intrusions (IDS).
2. Assurez-vous que votre pare-feu ou IPS/IDS autorise le trafic DNSCrypt crypté pour la baie virtuelle.
3. Autorisez le trafic sortant et entrant sur le port 53 (UDP/TCP) vers les adresses IP OpenDNS suivantes :
    - 208.67.220.220
    - 208.67.222.222
    - 208.67.222.220
    - 208.67.220.222
4. Si vous utilisez un pare-feu ou IPS/IDS avec inspection approfondie des paquets, vérifiez qu'il ne bloque pas les paquets DNSCrypt chiffrés et n'interfère pas avec eux. Certains périphériques peuvent bloquer ces paquets s'ils n'attendent que le trafic DNS standard sur le port 53.
5. Vérifiez que le trafic chiffré peut circuler à la fois en sortie et en entrée entre votre réseau et les résolveurs OpenDNS sur tous les périphériques du chemin.



Remarque : Si votre pare-feu ou IPS/IDS bloque le trafic DNSCrypt, la résolution DNS peut échouer pour les utilisateurs derrière le VA.

Si vous pensez que votre pare-feu autorise déjà ce trafic mais que l'avertissement persiste, ouvrez un dossier d'assistance pour obtenir de l'aide.

Pour plus d'informations sur le comportement du pare-feu Cisco ASA et les messages d'erreur possibles liés à l'inspection approfondie des paquets et à DNSCrypt, voir : Pourquoi le pare-feu Cisco ASA bloque-t-il la fonctionnalité DNSCrypt de l'appareil virtuel Umbrella ?

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.