# Gestion des paquets ICMP fragmentés à accès sécurisé Cisco

## Table des matières

## Problème

Les requêtes d'écho ICMP supérieures à la MTU ne reçoivent pas de réponse lorsqu'elles sont envoyées avec le bit DF (Don't Fragment) désactivé. Ce comportement se produit dans deux scénarios spécifiques :

- Depuis les terminaux RAVPN sur l'interface VPN lors de l'envoi de paquets ICMP qui dépassent la taille MTU de l'interface VPN avec le bit DF effacé
- À partir de terminaux sur site via un tunnel IPsec entre un routeur de site et Cisco Secure Access (CSA) lors de l'envoi de paquets ICMP qui dépassent la taille MTU de l'interface de tunnel IPsec avec le bit DF effacé

Dans les deux cas, aucune réponse ICMP n’est reçue, ce qui amène à se demander si CSA abandonne les paquets fragmentés avec le bit DF désactivé.

## Environnement

- Cisco Secure Access (CSA)
- Terminaux RAVPN (Remote Access VPN)
- Tunnels IPsec entre les routeurs de site et CSA
- Trafic ICMP dépassant les tailles MTU d'interface
- Scénarios de paquets fragmentés avec bit DF effacé

## Résolution

Cisco Secure Access supprime les paquets fragmentés dans les scénarios sous-jacents et

superposés. Ce comportement est documenté dans la documentation d'aide de Cisco Secure Access, qui indique explicitement : "Les paquets fragmentés dans la couche sous-jacente ou la couche de superposition sont abandonnés."

### Comportement attendu

Cisco Secure Access est conçu pour supprimer les paquets fragmentés, qu'ils se trouvent sur le réseau sous-jacent ou superposé. Ceci s'applique à :

- Paquets ICMP envoyés à partir de terminaux RAVPN qui dépassent le MTU de l'interface VPN avec bit DF effacé
- Paquets ICMP envoyés à partir de points d'extrémité sur site via des tunnels IPsec qui dépassent le MTU de l'interface de tunnel avec le bit DF effacé

Ce comportement est cohérent dans tous les scénarios impliquant des paquets fragmentés au sein de l'infrastructure d'accès sécurisé Cisco.

La demande de fonctionnalité CSE-I-5739 a été créée pour cela.

## Motif

L'architecture Cisco Secure Access permet d'abandonner les paquets fragmentés pour des raisons de sécurité et de performances. Ce comportement est mis en oeuvre pour empêcher les vulnérabilités de sécurité potentielles et la surcharge de traitement associée au réassemblage de paquets dans les scénarios de réseau sous-jacent et de réseau superposé.

## Autres informations utiles

- Documentation d'aide de Cisco Secure Access - Gestion des paquets fragmentés
- 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.