FAQ ASA : Comment puis-je spécifier l'interface source ASA pour les syslogs envoyés via un tunnel VPN l ?

Contenu

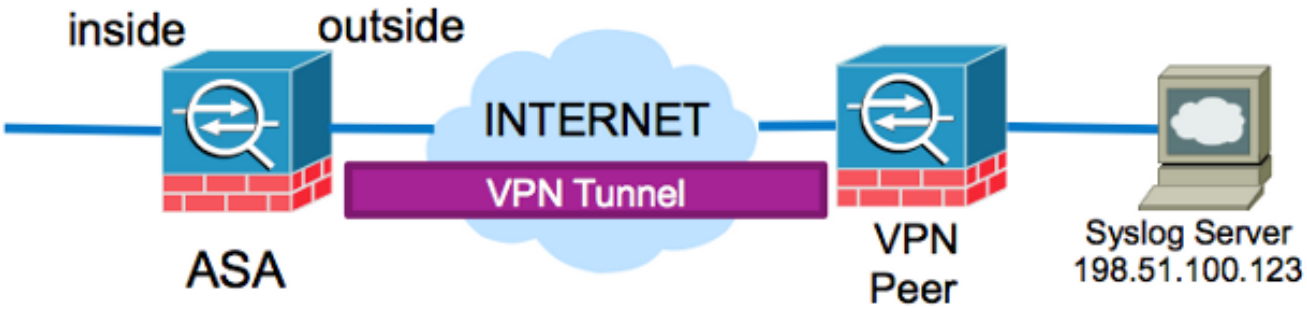
Introduction

Ce document décrit comment configurer le dispositif de sécurité adaptatif Cisco (ASA) afin d'envoyer des syslogs sur un tunnel VPN LAN à LAN et de les source à partir de l'adresse IP de l'interface interne.

Comment puis-je spécifier l'interface source ASA pour les syslogs envoyés via un tunnel VPN ?

Afin de spécifier l'interface à partir de laquelle le trafic syslog envoyé via le tunnel doit être source, entrez la commande **management-access**.

Si votre système possède cette topologie et cette configuration, entrez les commandes suivantes.




```
ASA# show run logging
logging enable
logging timestamp
logging trap debugging
logging host outside 198.51.100.123
```

Cette configuration tente de source du trafic syslog à partir de l'adresse IP externe de l'ASA. Cela nécessite que l'adresse IP externe soit ajoutée à la liste d'accès de chiffrement afin de chiffrer le trafic sur le tunnel. Cette modification de configuration peut ne pas être optimale, en particulier si le trafic provenant de l'adresse IP de l'interface interne destinée au sous-réseau du serveur syslog est déjà configuré pour être encyclique par la liste d'accès cryptographique.

L'ASA peut être configuré pour source le trafic syslog destiné au serveur à envoyer via le tunnel

VPN à partir de l'interface spécifiée avec la commande **management-access**.

Afin d'implémenter cette configuration pour cet exemple spécifique, supprimez d'abord la configuration **d'hôte de journalisation** actuelle :

```
no logging host outside 198.51.100.123
```

Réinsérez le serveur de journalisation avec l'interface interne spécifiée et la commande **management-access** :

```
logging host inside 198.51.100.123
management-access inside
```