Preguntas frecuentes sobre ASA: ¿Cómo puedo especificar la interfaz de origen ASA para los syslogs enviados a través de un túnel VPNi?

Contenido

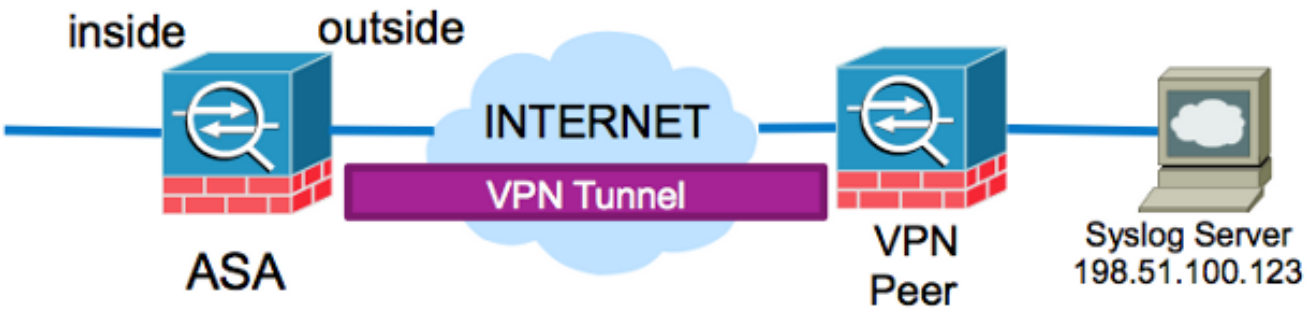
Introducción

Este documento describe cómo configurar Cisco Adaptive Security Appliance (ASA) para enviar syslogs a través de un túnel VPN de LAN a LAN y originar esos syslogs desde la dirección IP de la interfaz interna.

¿Cómo puedo especificar la interfaz de origen ASA para los syslogs enviados a través de un túnel VPN?

Para especificar la interfaz desde la cual se originará el tráfico syslog enviado a través del túnel, ingrese el comando **management-access**.

Si su sistema tiene esta topología y configuración, ingrese los siguientes comandos.




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

Esta configuración intenta originar el tráfico syslog desde la dirección IP externa del ASA. Esto requiere que la dirección IP externa se agregue a la lista de acceso crypto para cifrar el tráfico a través del túnel. Este cambio de configuración puede no ser óptimo, especialmente si el tráfico originado en la dirección IP de la interfaz interna destinada a la subred del servidor syslog ya está configurado para ser codificado por la lista de acceso crypto.

El ASA se puede configurar para originar el tráfico syslog destinado al servidor para ser enviado a través del túnel VPN desde la interfaz especificada con el comando **management-access**.

Para implementar esta configuración para este ejemplo específico, primero elimine la configuración actual del **host de registro**:

```
no logging host outside 198.51.100.123
```

Vuelva a insertar el servidor de registro con la interfaz interna especificada y el comando **management-access**:

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