DOMANDE FREQUENTI SULL'APPLIANCE ASA: Come posso specificare l'interfaccia di origine ASA per i syslog inviati su un tunnel VPN?

Sommario

[Introduzione](#)
[Come posso specificare l'interfaccia di origine ASA per i syslog inviati su un tunnel VPN?](#)

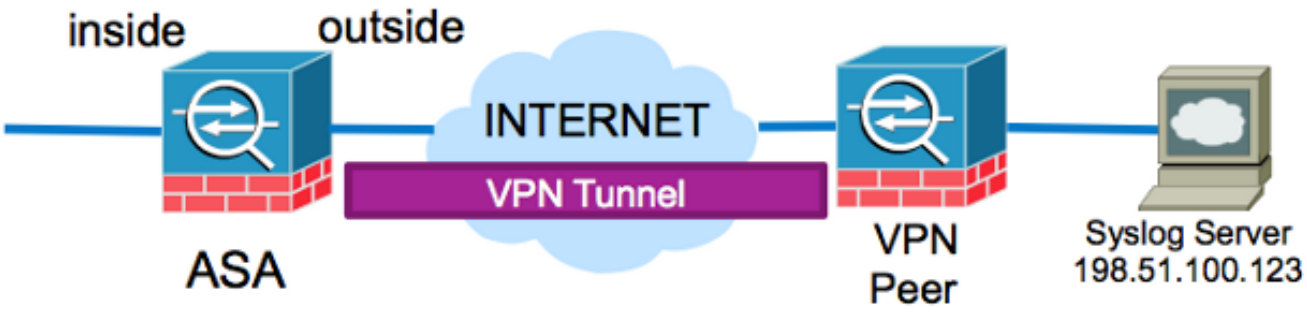
Introduzione

In questo documento viene descritto come configurare Cisco Adaptive Security Appliance (ASA) in modo che invii i syslog su un tunnel VPN da LAN a LAN e come originarli dall'indirizzo IP dell'interfaccia interna.

Come posso specificare l'interfaccia di origine ASA per i syslog inviati su un tunnel VPN?

Per specificare l'interfaccia dalla quale originare il traffico syslog inviato attraverso il tunnel, immettere il comando **management-access**.

Se il sistema dispone di questa topologia e configurazione, immettere i comandi seguenti.




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

Questa configurazione cerca di originare il traffico syslog dall'indirizzo IP esterno dell'appliance ASA. A tal fine, è necessario aggiungere l'indirizzo IP esterno all'elenco degli accessi crittografici per crittografare il traffico sul tunnel. La modifica della configurazione potrebbe non essere ottimale, in particolare se il traffico proveniente dall'indirizzo IP dell'interfaccia interna e destinato alla subnet del server syslog è già impostato per essere crittografato dall'elenco degli accessi

crittografato.

L'ASA può essere configurata in modo da originare il traffico syslog destinato al server da inviare sul tunnel VPN dall'interfaccia specificata con il comando **management-access**.

Per implementare questa configurazione per questo esempio specifico, rimuovere prima la configurazione corrente dell'**host di log**:

```
no logging host outside 198.51.100.123
```

Reinserire il server di log con l'interfaccia interna specificata e il comando **management-access**:

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