ASA FAQ:VPN tunnel를 통해 전송되는 syslog에 대해 ASA 소스 인터페이스를 지정하려면 어떻게 해야 합니까?

목차

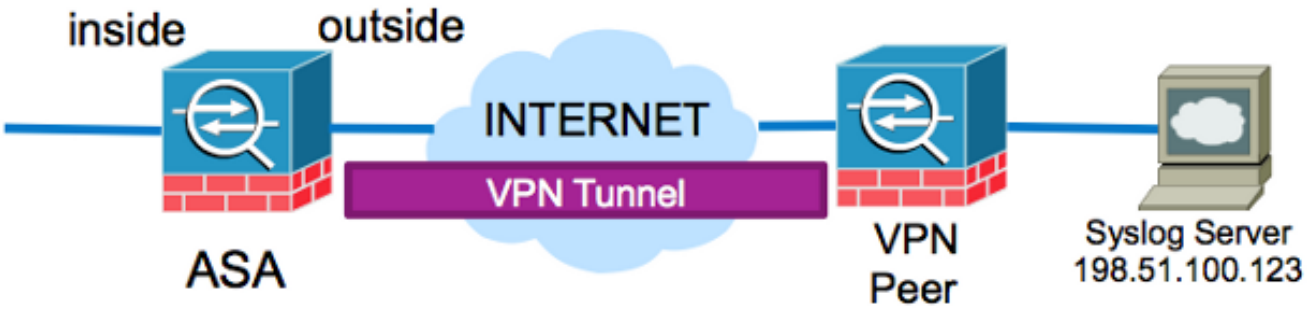
소개

이 문서에서는 LAN-to-LAN VPN 터널을 통해 syslog를 전송하고 내부 인터페이스 IP 주소에서 해당 syslog를 소싱하기 위해 Cisco ASA(Adaptive Security Appliance)를 구성하는 방법에 대해 설명합니다.

VPN 터널을 통해 전송된 syslog에 대해 ASA 소스 인터페이스를 어떻게 지정할 수 있습니까?

터널을 통해 전송된 syslog 트래픽을 소스 지정할 인터페이스를 지정하려면 **management-access** 명령을 입력합니다.

시스템에 이 토폴로지 및 컨피그레이션이 있는 경우 다음 명령을 입력합니다.




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

이 컨피그레이션은 ASA의 외부 IP 주소에서 syslog 트래픽을 소스 지정하려고 시도합니다.이렇게 하려면 터널을 통해 트래픽을 암호화하려면 외부 IP 주소를 암호화 액세스 목록에 추가해야 합니다.이 컨피그레이션 변경은 최적화되지 않을 수 있습니다. 특히 syslog 서버 서브넷으로 향하는 내부 인터페이스 IP 주소에서 제공된 트래픽이 이미 crypto access-list에 의해 암호화되도록 설정된 경우 그렇습니다.

ASA는 **management-access** 명령으로 지정된 인터페이스에서 VPN 터널을 통해 전송될 syslog 트

래픽을 소스로 **전송하도록** 구성할 수 있습니다.

이 특정 예제에 대해 이 컨피그레이션을 구현하려면 먼저 현재 **로깅 호스트** 컨피그레이션을 제거합니다.

```
no logging host outside 198.51.100.123
```

내부 인터페이스가 지정된 로깅 서버를 다시 삽입하고 management-access 명령을 사용합니다.

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