Perguntas frequentes do ASA: Como posso especificar a interface de origem do ASA para syslogs enviados por um túnel VPNi?

Contents

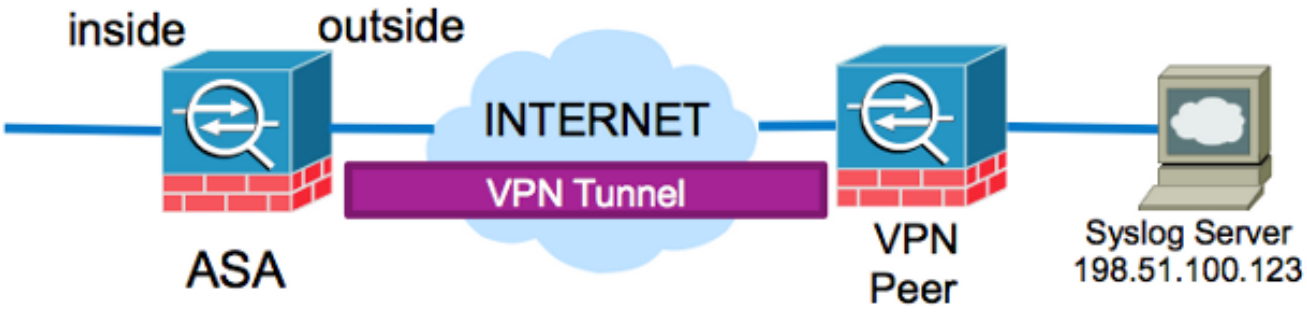
Introduction

Este documento descreve como configurar o Cisco Adaptive Security Appliance (ASA) para enviar syslogs por um túnel VPN LAN para LAN e originar esses syslogs do endereço IP da interface interna.

Como posso especificar a interface de origem do ASA para syslogs enviados por um túnel VPN?

Para especificar a interface de onde a origem do tráfego syslog é enviada pelo túnel, insira o comando **management-access**.

Se o sistema tiver essa topologia e configuração, insira os comandos a seguir.




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

Essa configuração tenta originar o tráfego de syslog do endereço IP externo do ASA. Isso exige que o endereço IP externo seja adicionado à lista de acesso de criptografia para criptografar o tráfego no túnel. Essa alteração de configuração pode não ser ideal, especialmente se o tráfego originado do endereço IP da interface interna destinado à sub-rede do Servidor syslog já estiver definido para ser criptografado pela lista de acesso de criptografia.

O ASA pode ser configurado para originar o tráfego syslog destinado ao servidor para ser enviado

pelo túnel VPN da interface especificada com o comando **management-access**.

Para implementar essa configuração para este exemplo específico, primeiro remova a configuração atual do **host de registro**:

```
no logging host outside 198.51.100.123
```

Reinsira o servidor de registro com a interface interna especificada e o comando **management-access**:

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