ASA FAQ: How can I specify the ASA source interface for syslogs sent over a VPN tunnel?

Contents

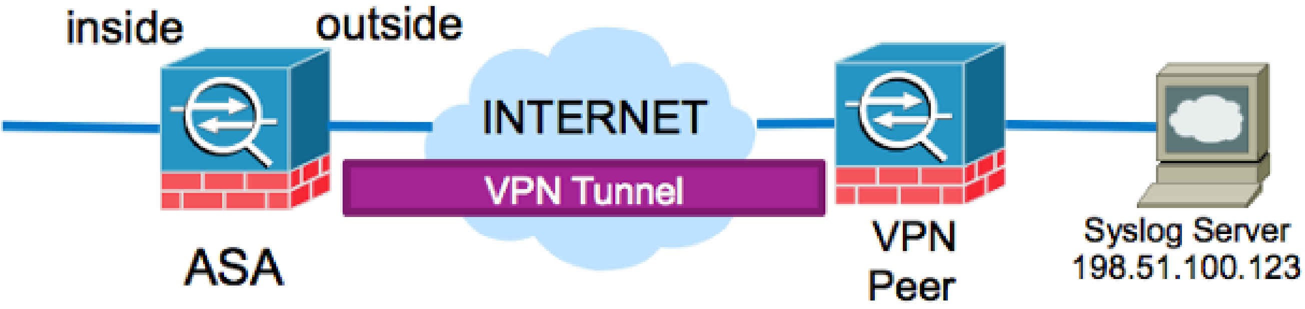
Introduction

This document describes how to configure the Cisco Adaptive Security Appliance (ASA) in order to send syslogs over a LAN-to-LAN VPN tunnel and source those syslogs from the inside interface IP address.

How can I specify the ASA source interface for syslogs sent over a VPN tunnel?

In order to specify the interface from which to source the syslog traffic sent over the tunnel, enter the **management-access** command.

If your system has this topology and configuration, enter the commands that follow.



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

This configuration attempts to source the syslog traffic from the ASA's outside IP address. This requires that the outside IP address be added to the crypto access-list in order to encrypt the traffic over the tunnel. This configuration change might not be optimal, especially if traffic sourced from the inside interface IP address destined to the syslog server subnet is already set to be encypted by the crypto access-list.

The ASA can be configured to source the syslog traffic destined to the server to be sent over the VPN tunnel from the interface specified with the **management-access** command.

In order to implement this configuration for this specific example, first remove the current **logging host** configuration:

```
no logging host outside 198.51.100.123
```

Reinsert the logging server with the inside interface specified, and the **management-access** command:

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