ASA无客户端SSL VPN通过IPsec LAN到LAN隧道的流量配置示例

目录

简介

本文档介绍如何连接到思科自适应安全设备(ASA)无客户端SSLVPN门户并访问位于通过IPsec LAN到LAN隧道连接的远程位置中的服务器。

先决条件

要求

Cisco 建议您了解以下主题：

- 无客户端SSL VPN配置。
- LAN到LAN VPN配置

使用的组件

本文档中的信息基于运行版本9.2(1)的ASA 5500-X系列，但适用于所有ASA版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。在对实时网络进行更改之前，请确保您了解任何命令的潜在影响。

背景信息

当来自无客户端SSLVPN会话的流量通过LAN到LAN隧道时，请注意有两个连接：

- 从客户端到ASA
- 从ASA到目的主机。

对于ASA到目的主机连接，使用ASA接口“最靠近”目的主机的IP地址。因此，LAN到LAN相关流量必须包含从该接口地址到远程网络的代理身份。

注意： 如果智能隧道用于书签，则仍使用最靠近目标的ASA接口的IP地址。

配置

在此图中，两个ASA之间有一个LAN到LAN隧道，允许流量从192.168.10.x传输到192.168.20.x。

确定该隧道的相关流量的访问列表：

ASA1

```
access-list l2l-list extended permit ip 192.168.10.0 255.255.255.0 192.168.20.0
255.255.255.0
```

ASA2

```
access-list l2l-list extended permit ip 192.168.20.0 255.255.255.0 192.168.10.0
255.255.255.0
```

如果无客户端SSLVPN用户尝试与192.168.20.x网络上的主机通信，则ASA1将209.165.200.225地址用作该流量的源。由于LAN到LAN访问控制列表(ACL)不包含209.168.200.225作为代理身份，因此流量不会通过LAN到LAN隧道发送。

为了通过LAN到LAN隧道发送流量，必须向相关流量ACL添加新的访问控制条目(ACE)。

ASA1

```
access-list l2l-list extended permit ip host 209.165.200.225 192.168.20.0
255.255.255.0
```

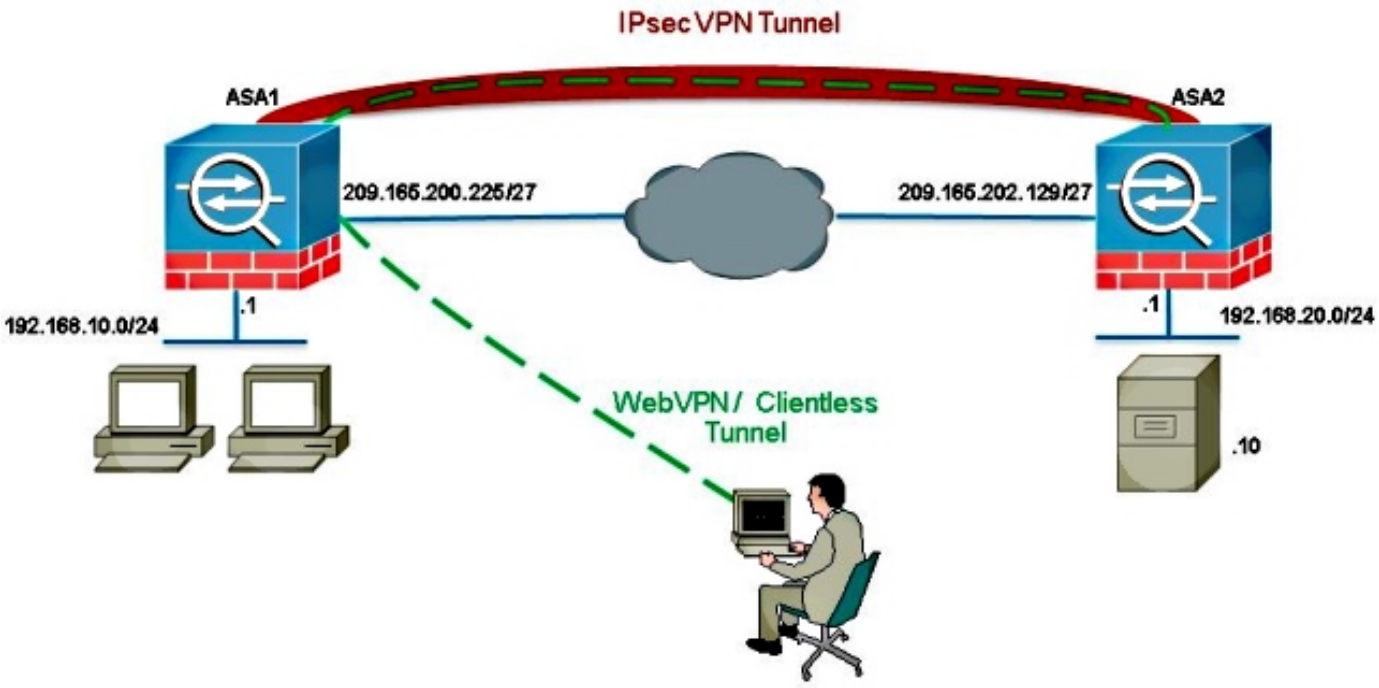
ASA2

```
access-list l2l-list extended permit ip 192.168.20.0 255.255.255.0 host
209.165.200.225
```

同样的原则适用于无客户端SSLVPN流量需要**u-turn** 从其进入的相同接口输出的配置，即使它不应通过LAN到LAN隧道。

注意：使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图



通常，ASA2对192.168.20.0/24执行端口地址转换(PAT)以提供互联网访问。在这种情况下，当ASA2上来自192.168.20.0/24的流量进入209.165.200.225时，应从PAT进程中排除。否则，响应不会通过LAN到LAN隧道。例如：

ASA2

```
nat (inside,outside) source static obj-192.168.20.0 obj-
192.168.20.0 destination
static obj-209.165.200.225 obj-209.165.200.225
!
object network obj-192.168.20.0
nat (inside,outside) dynamic interface
```

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序工具（仅限注册用户）支持某些 show 命令。使用输出解释器工具来查看 show 命令输出的分析。

- **show crypto ipsec sa** — 使用此命令验证ASA1代理IP地址和远程网络之间的安全关联(SA)已创建。检查无客户端SSLVPN用户访问该服务器时加密和解密的计数器是否增加。

故障排除

本部分提供了可用于对配置进行故障排除的信息。

如果未建立安全关联，则可以使用IPsec调试来查找故障原因：

- **debug crypto ipsec <level>**

  注意：使用 **debug 命令之前，请参阅**有关 Debug 命令的重要信息。