ASA无客户端在IPSec LAN到LAN隧道配置示例的SSL VPN流量

目录

简介

本文描述如何连接到Cisco可适应安全工具(ASA)无客户端门户的SSLVPN和访问在IPSec LAN到LAN隧道连接的远程位置查找的服务器。

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对LAN VPN配置

使用的组件

运行版本9.2(1)的本文档中的信息根据5500-X系列的ASA，但是运用对所有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。保证您了解所有命令潜在影响，在您在真实网络前做变动。

背景信息

当从无客户端SSLVPN会话的流量横断LAN-to-LAN隧道时，请注意有两连接：

- 从ASA的客户端
- 从ASA到目的地主机。

对于ASA对目的地主机连接，“最接近”目的地主机使用ASA接口的IP地址。所以，LAN对LAN关注数据流必须包括从该接口地址的一个代理身分到远程网络。

Note: 如果SMART通道使用书签，最接近目的地仍然使用ASA接口的IP地址。

配置

在此图表中，有允许流量从192.168.10.x通过到192.168.20.x在两ASA之间的一个LAN-to-LAN隧道。

access-list确定该通道的关注数据流：

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用户设法用在192.168.20.x网络的一台主机通信，ASA1使用209.165.200.225地址作为来源该流量。由于LAN对LAN访问控制表(ACL)不包含209.168.200.225作为代理身分，流量没有在LAN-to-LAN隧道发送。

为了发送在LAN-to-LAN隧道的流量，必须添加一个新的访问控制项(ACE)到触发流量的ACL。

ASA1

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

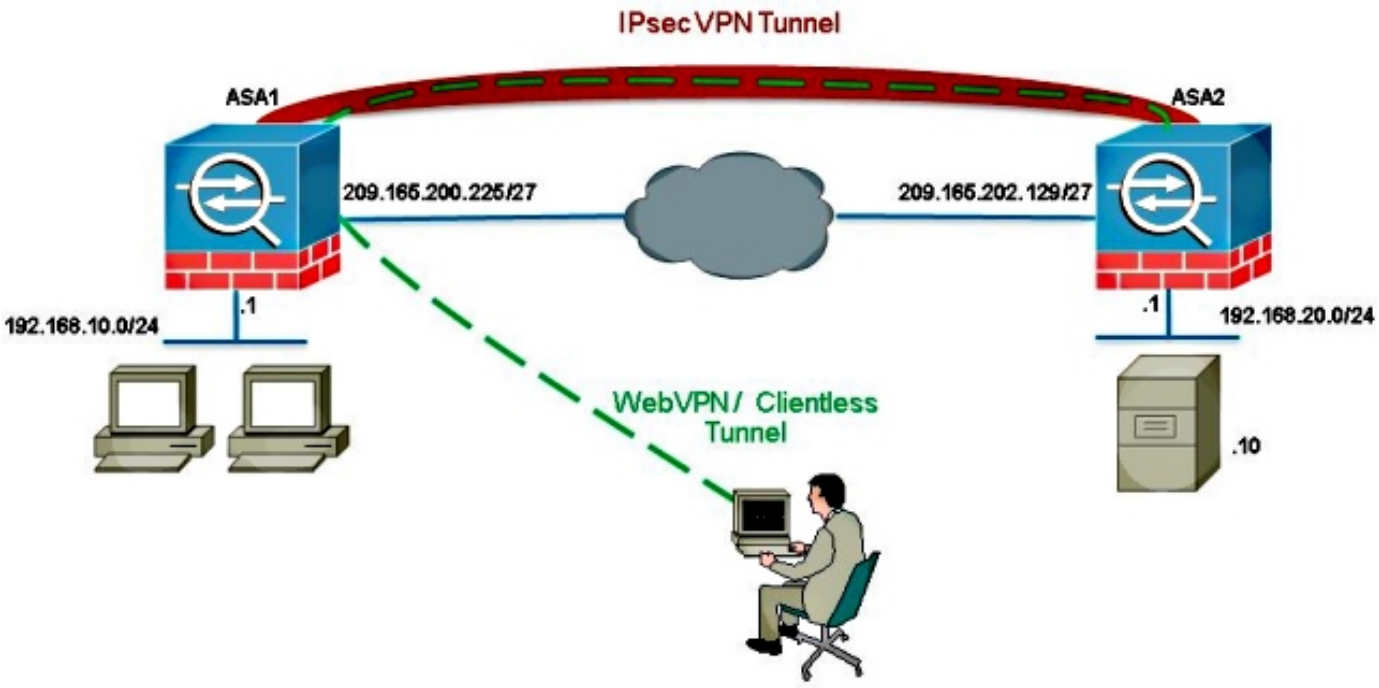
ASA2

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

此同样原理适用对无客户端SSLVPN流量需要**U字型转向**同一个接口进来的配置，即使不应该通过LAN-to-LAN隧道。

Note: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



一般， ASA2执行192.168.20.0/24的端口地址转换(PAT)为了提供互联网访问。在那种情况下，当去209.165.200.225时，应该从PAT进程然后排除从192.168.20.0/24的流量在ASA 2。否则，答复不会通过LAN-to-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。

- **显示crypto ipsec sa**-用此命令验证在ASA1代理IP地址和远程网络之间的安全关联(SA)创建。检查已加密和解密的计数器是否增加，当服务器的无客户端SSLVPN用户访问。

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。

如果安全关联没有被建立，您能使用IPSec调试到失败的原因：

- **debug crypto ipsec <level>**

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