通过L2L隧道的ASA VPN客户端连接配置示例

目录

简介

本文档介绍如何配置思科自适应安全设备(ASA)以允许从局域网到局域网(L2L)对等地址进行远程VPN客户端连接。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco ASA
- 远程接入 VPN
- LAN到LAN VPN

使用的组件

本文档中的信息基于运行软件版本8.4(7)的Cisco 5520系列ASA。

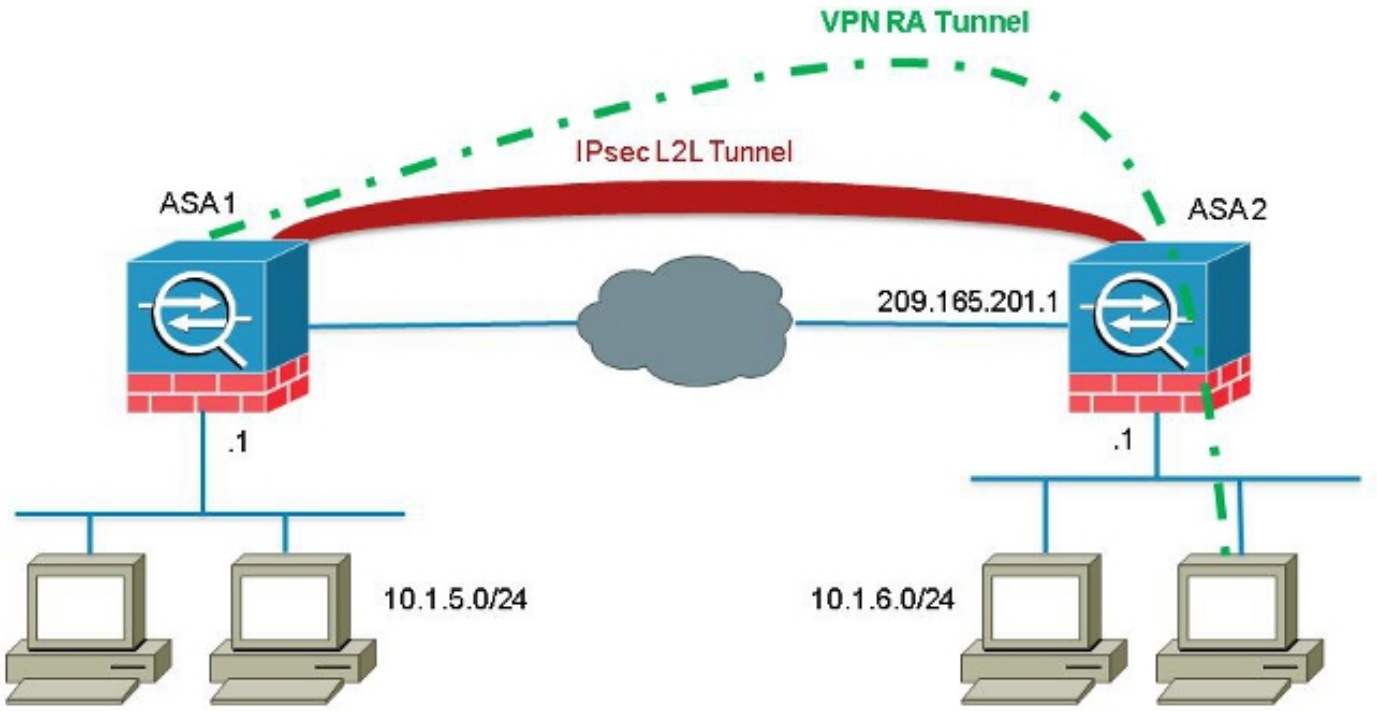
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

虽然VPN客户端尝试通过L2L隧道建立连接的情况并不常见，但管理员可能希望向某些远程用户分

配特定权限或访问限制，并指示他们在需要访问这些资源时使用软件客户端。

> **注意：**此方案在过去有效，但在将头端ASA升级到8.4(6)版或更高版本后，VPN客户端无法再建立连接。



Cisco Bug ID CSCuc75090引入了行为更改。以前，使用专用互联网交换(PIX)，当互联网协议安全(IPSec)代理与加密映射访问控制列表(ACL)不匹配时，它继续检查列表下的条目。这包括与没有指定对等体的动态加密映射匹配。

这被视为一个漏洞，因为远程管理员可以访问头端管理员在配置静态L2L时不打算访问的资源。

已创建修复，该修复添加了检查，以防止在已检查匹配对等体的映射条目时与没有对等体的加密映射条目匹配。但是，这影响了本文档中讨论的场景。具体而言，尝试从L2L对等地址连接的远程VPN客户端无法连接到头端。

配置

使用此部分可配置ASA，以允许从L2L对等地址进行远程VPN客户端连接。

添加新动态条目

要允许来自L2L对等地址的远程VPN连接，必须添加包含相同对等IP地址的新动态条目。

> **注意：**您还必须保留另一个没有对等体的动态条目，以便来自互联网的任何客户端也可以连接。

以下是先前动态加密映射工作配置的示例：

```
crypto dynamic-map ra-dyn-map 10 set ikev1 transform-set ESP-AES-128-SHA

crypto map outside_map 1 match address outside_cryptomap_1
crypto map outside_map 1 set peer 209.165.201.1
crypto map outside_map 1 set ikev1 transform-set ESP-AES-128-SHA
crypto map outside_map 65535 ipsec-isakmp dynamic ra-dyn-map
```

以下是配置了新动态条目的动态加密映射配置：

```
crypto dynamic-map ra-dyn-map 10 set ikev1 transform-set ESP-AES-128-SHA
crypto dynamic-map ra-dyn-map 10 set peer 209.165.201.1
crypto dynamic-map ra-dyn-map 20 set ikev1 transform-set ESP-AES-128-SHA

crypto map outside_map 1 match address outside_cryptomap_1
crypto map outside_map 1 set peer 209.165.201.1
crypto map outside_map 1 set ikev1 transform-set ESP-AES-128-SHA
crypto map outside_map 65535 ipsec-isakmp dynamic ra-dyn-map
```

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。