ASA VPN客户端连接通过L2L隧道配置示例

目录

简介

本文描述如何配置思科可适应安全工具(ASA)为了允许从LAN对LAN (L2L)对等地址的远程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对LAN VPN

使用的组件

运行软件版本8.4(7)的本文档中的信息根据Cisco 5520系列ASA。

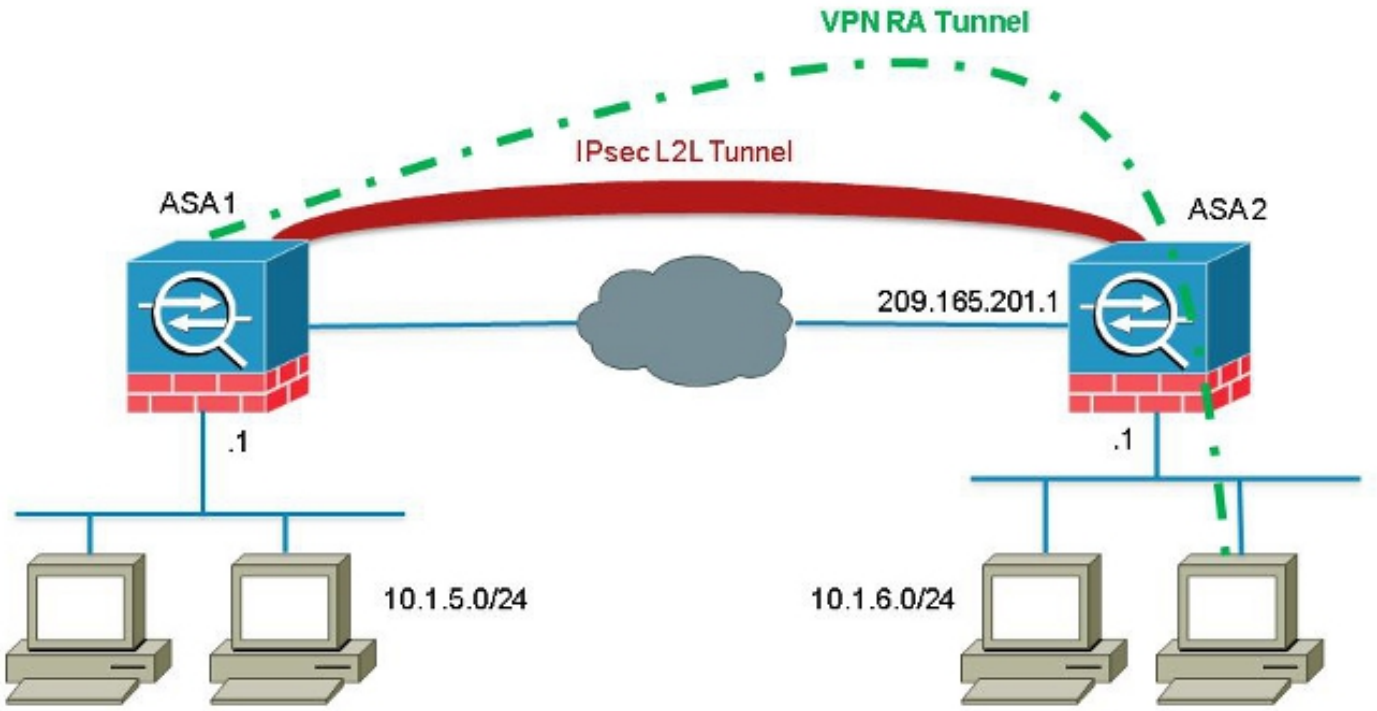
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

虽然它不是普通遇到VPN客户端尝试通过L2L通道建立连接的方案，管理员也许想要分配特定权限

或访问限制对某些远程用户和提示他们使用软件客户端，当对这些资源的访问要求时。

> **注意**：以前工作的此方案，但是，在头端ASA的升级对版本8.4(6)或以上的， VPN客户端是后不再能建立连接。



Cisco Bug ID CSCuc75090介绍行为更改。以前，与专用互联网交换(PIX)，当Internet协议安全性(IPSec)代理没有匹配加密映射访问控制表(ACL)，它继续检查条目进一步在列表下。这与一个动态加密映射的包括的匹配没有对等体指定。

这认为漏洞，因为远程管理员可能获得访问到头端管理员没有打算的资源，当静态L2L配置。

添加一检查为了防止与加密映射项的匹配，不用对等体的修正创建，当已经检查匹配对等体的映射条目。然而，这影响在本文讨论的方案。特别地，尝试从L2L对等地址连接的一远程VPN客户端不能连接到头端。

配置

请使用此部分为了配置ASA为了允许从L2L对等地址的远程VPN客户端连接。

添加新的动态条目

为了允许从L2L对等地址的远程VPN连接，您必须添加包含同样对端IP地址的一新的动态条目。

> **注意**：您必须也留下另一动态条目，不用对等体，以便从互联网的所有客户端能连接。

这是上一个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
```

这是与配置的新的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。