Ejemplo de Configuración de ASA VPN Client Connection a través de un Túnel L2L

Contenido

Introducción

Este documento describe cómo configurar Cisco Adaptive Security Appliance (ASA) para permitir una conexión de cliente VPN remota desde una dirección de peer Lan a Lan (L2L).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco ASA
- VPN de acceso remoto
- VPN de LAN a LAN

Componentes Utilizados

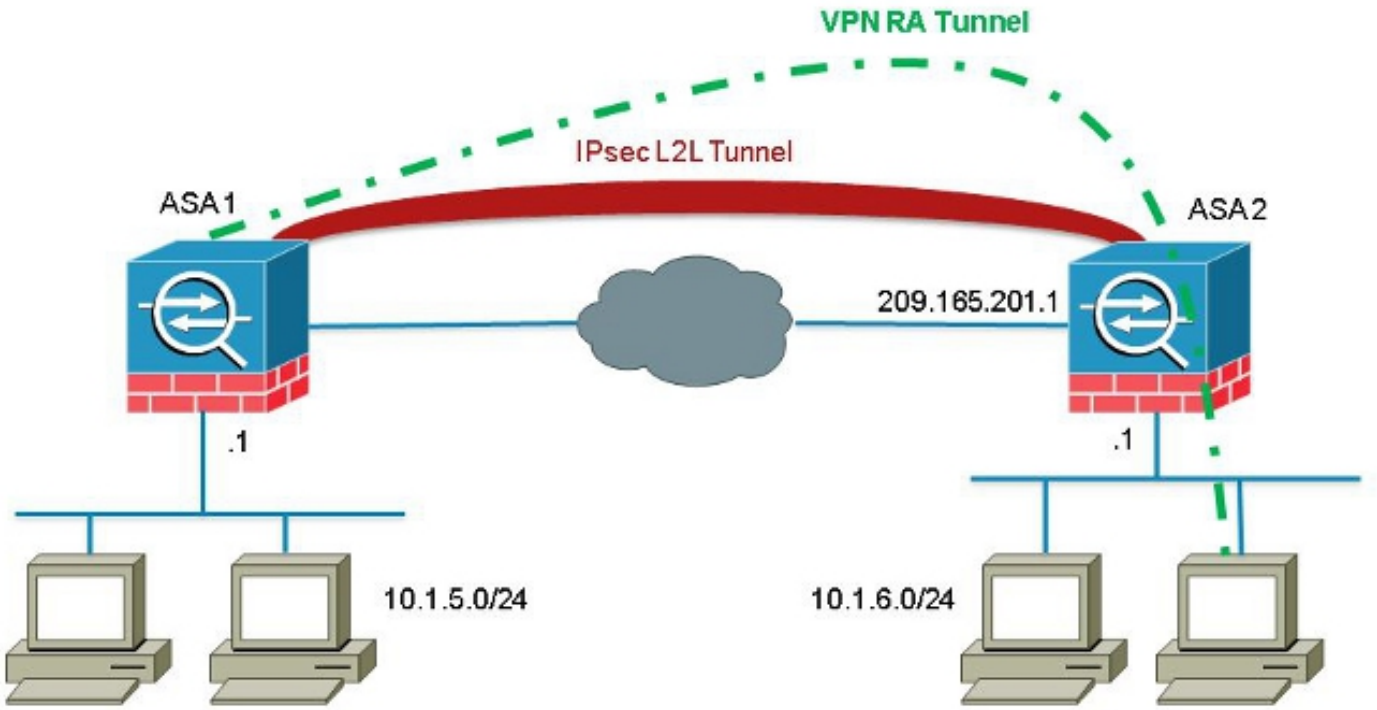
La información de este documento se basa en el Cisco 5520 Series ASA que ejecuta la versión de software 8.4(7).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

Aunque no es común encontrar un escenario en el que un cliente VPN intente establecer una conexión a través de un túnel L2L, los administradores pueden querer asignar privilegios específicos o restricciones de acceso a ciertos usuarios remotos e instruirlos para que utilicen el cliente de software cuando se requiera acceso a estos recursos.

> **Nota:** Esta situación funcionó en el pasado, pero después de una actualización del ASA de cabecera a la versión 8.4(6) o posterior, el cliente VPN ya no puede establecer la conexión.



El ID de bug de Cisco CSCuc75090 introdujo un cambio de comportamiento. Anteriormente, con el intercambio de Internet privado (PIX), cuando el proxy de seguridad de protocolo de Internet (IPSec) no coincidía con una lista de control de acceso (ACL) de mapa criptográfico, siguió comprobando las entradas más abajo en la lista. Esto incluía coincidencias con un crypto-map dinámico sin peer especificado.

Esto se consideró una vulnerabilidad, ya que los administradores remotos podían obtener acceso a recursos que el administrador de cabecera no pretendía cuando se configuró la L2L estática.

Se creó una corrección que agregó una comprobación para evitar coincidencias con una entrada de mapa criptográfico sin un par cuando ya verificó una entrada de mapa que coincidía con el par. Sin embargo, esto afectó al escenario que se discute en este documento. Específicamente, un cliente VPN remoto que intenta conectarse desde una dirección de peer L2L no puede conectarse a la cabecera.

Configurar

Utilice esta sección para configurar el ASA para permitir una conexión de cliente VPN remoto

desde una dirección de peer L2L.

Agregar una nueva entrada dinámica

Para permitir conexiones VPN remotas desde direcciones de peer L2L, debe agregar una nueva entrada dinámica que contenga la misma dirección IP de peer.

> **Nota:** También debe dejar otra entrada dinámica sin un par para que cualquier cliente de Internet pueda conectarse también.

A continuación se muestra un ejemplo de la configuración de trabajo dinámica de crypto map anterior:

```
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
```

Esta es la configuración dinámica de crypto-map con la nueva entrada dinámica configurada:

```
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
```

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.