Conexión de cliente VPN ASA con un ejemplo de la configuración del túnel L2L

Contenido

Introducción

Este documento describe cómo configurar el dispositivo de seguridad adaptante de Cisco (ASA) para permitir una conexión de cliente VPN remota de una dirección de peer LAN-a-LAN (L2L).

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco ASA
- VPN de accesos remotos
- LAN a LAN VPN

Componentes Utilizados

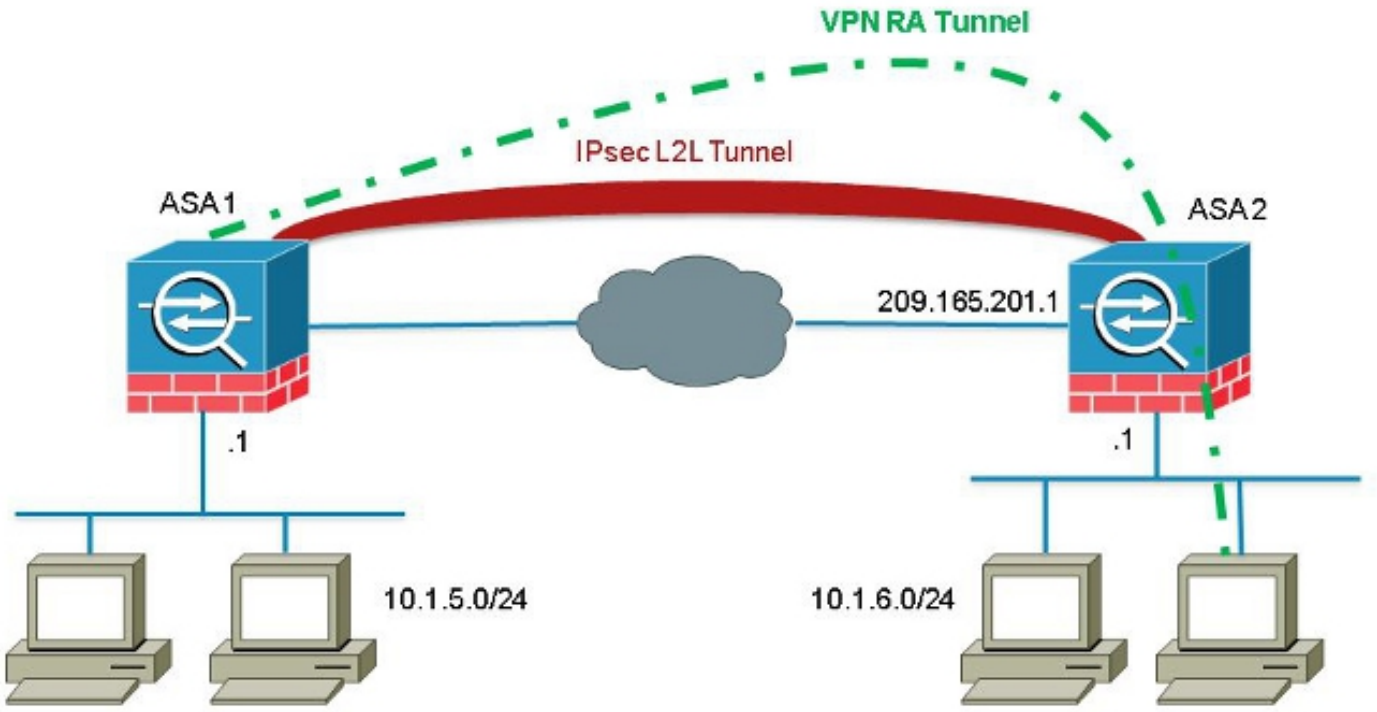
La información en este documento se basa en las Cisco 5520 Series ASA que funciona con la versión de software 8.4(7).

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

Aunque no sea común encontrar un escenario donde un cliente VPN intenta establecer una conexión a través de un túnel L2L, los administradores pudieron querer asignar los privilegios o las restricciones de acceso específicos a ciertos usuarios remotos y darlos instrucciones para utilizar al software cliente cuando el acceso a estos recursos se requiere.

> Nota: Este escenario trabajado en el pasado, pero después de que sea una actualización del headend ASA a la versión 8.4(6) o posterior, el cliente VPN pueda no más establecer la conexión.



El Id. de bug Cisco CSCuc75090 introdujo un cambio del comportamiento. Previamente, con el private internet exchange (PIX), cuando el proxy de la seguridad de protocolos en Internet (IPSec) no hizo juego una lista de control de acceso (ACL) del crypto-mapa, continuó marcando las entradas más lejos abajo de la lista. Esto incluyó las coincidencias con una correspondencia cifrada dinámica sin el par especificada.

Esto era considerada una vulnerabilidad, pues los administradores remotos podrían acceder a los recursos que el administrador del headend no pensó cuando el L2L estático fue configurado.

Un arreglo fue creado que agregó un control para prevenir las coincidencias con una entrada de correspondencia de criptografía sin un par cuando marcó ya una entrada de mapeo que correspondió con al par. Sin embargo, esto afectó al escenario que se discute en este documento. Específicamente, un cliente VPN remoto que intenta conectar de una dirección de peer L2L no puede conectar con el headend.

Configurar

Utilice esta sección para configurar el ASA para permitir una conexión de cliente VPN remota de una dirección de peer L2L.

Agregue una nueva entrada dinámica

Para permitir las conexiones VPN remotas de las direcciones de peer L2L, usted debe agregar una nueva entrada dinámica que contenga el mismo IP Address de Peer.

> Nota: Usted debe también salir de otra entrada dinámica sin un par de modo que cualquier cliente de Internet pueda conectar también.

Aquí está un ejemplo de la configuración en funcionamiento anterior de la correspondencia cifrada dinámica:

```
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
```

Aquí está la configuración de la correspondencia cifrada dinámica 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.

Troubleshooting

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