Ejemplo de Configuración del Tráfico SSL VPN sin Cliente ASA sobre el Túnel LAN a LAN IPSec

Contenido

Introducción

Este documento describe cómo conectarse a un Cisco Adaptive Security Appliance (ASA) Clientless SSLVPN Portal y acceder a un servidor que se encuentra en una ubicación remota conectada a través de un túnel IPsec de LAN a LAN.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración SSL VPN sin cliente.
- Configuración de VPN de LAN a LAN

Componentes Utilizados

La información de este documento se basa en ASA serie 5500-X que ejecuta la versión 9.2(1), pero se aplica a todas las versiones de ASA.

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. Asegúrese de

comprender el impacto potencial de cualquier comando antes de realizar cambios en una red activa.

Antecedentes

Cuando el tráfico de una sesión SSLVPN sin cliente atraviesa un túnel de LAN a LAN, observe que hay dos conexiones:

- Del cliente al ASA
- Desde el ASA al host de destino.

Para la conexión de host de ASA a destino, se utiliza la dirección IP de la interfaz ASA "más cercana" al host de destino. Por lo tanto, el tráfico interesante de LAN a LAN debe incluir una identidad proxy desde esa dirección de interfaz a la red remota.

> **Nota:** Si se utiliza Smart-Tunnel para un marcador, se seguirá utilizando la dirección IP de la interfaz ASA más cercana al destino.

Configurar

En este diagrama, hay un túnel de LAN a LAN entre dos ASA que permite que el tráfico pase de 192.168.10.x a 192.168.20.x.

La lista de acceso que determina el tráfico interesante para ese túnel:

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
```

Si el usuario SSLVPN sin cliente intenta comunicarse con un host en la red 192.168.20.x, ASA1 utiliza la dirección 209.165.200.225 como origen para ese tráfico. Debido a que la lista de control de acceso (ACL) de LAN a LAN no contiene 209.168.200.225 como identidad de proxy, el tráfico no se envía a través del túnel de LAN a LAN.

Para enviar tráfico a través del túnel de LAN a LAN, se debe agregar una nueva entrada de control de acceso (ACE) a la lista de control de tráfico interesante.

ASA1

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

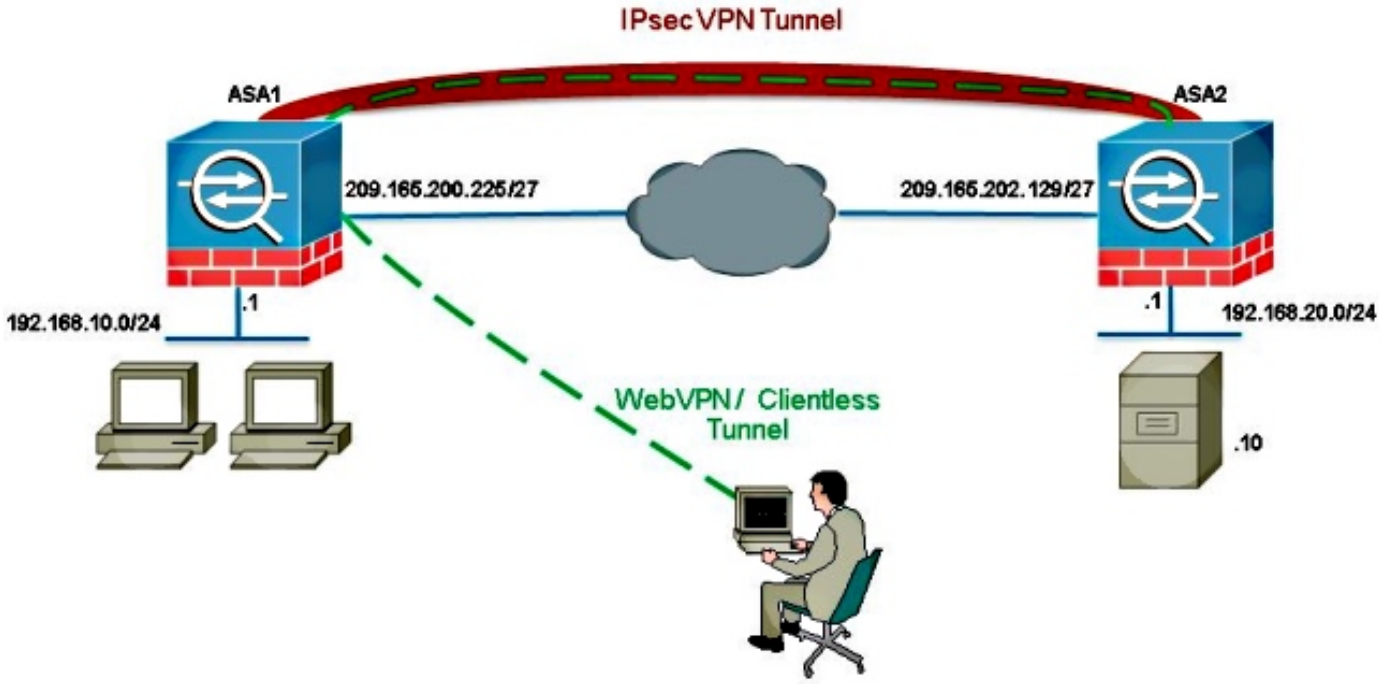
ASA2

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

Este mismo principio se aplica a las configuraciones en las que el tráfico SSLVPN sin cliente necesita **activar u** la misma interfaz en la que entró, incluso si se supone que no debe pasar a través de un túnel de LAN a LAN.

> **Nota:** Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red



Normalmente, ASA2 realiza la traducción de direcciones de puerto (PAT) para el 192.168.20.0/24 para proporcionar acceso a Internet. En ese caso, el tráfico de 192.168.20.0/24 en ASA 2 debe excluirse del proceso PAT cuando vaya a 209.165.200.225. De lo contrario, la respuesta no pasaría por el túnel de LAN a LAN. Por ejemplo:

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
```

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show.

- **show crypto ipsec sa**: verifique con este comando que se haya creado una asociación de seguridad (SA) entre la dirección IP del proxy ASA1 y la red remota. Verifique si los contadores cifrados y descifrados aumentan cuando el usuario de SSLVPN sin cliente accede a ese servidor.

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Si la asociación de seguridad no está generada, puede utilizar la depuración IPSec para la causa del error:

- **debug crypto ipsec <level>**

  Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un comando debug.