Exemplo de Configuração de Túnel de LAN para LAN de tráfego SSL sem cliente ASA sobre IPsec

Contents

Introduction

Este documento descreve como se conectar a um Cisco Adaptive Security Appliance (ASA) Client SSLVPN Portal e acessar um servidor localizado em um local remoto conectado em um túnel IPsec LAN-to-LAN.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de VPN SSL sem cliente.
- Configuração de VPN LAN para LAN

Componentes Utilizados

As informações neste documento são baseadas no ASA 5500-X Series que executa a versão 9.2(1), mas se aplicam a todas as versões do 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. Certifique-se de entender o impacto potencial de qualquer comando antes de fazer alterações em uma rede ativa.

Informações de Apoio

Quando o tráfego de uma sessão SSLVPN sem cliente atravessa um túnel de LAN para LAN, observe que há duas conexões:

- Do cliente ao ASA
- Do ASA ao host de destino.

Para a conexão do host ASA com o destino, o endereço IP da interface ASA "mais próxima" do host de destino é usado. Portanto, o tráfego interessante de LAN para LAN deve incluir uma identidade de proxy desse endereço de interface para a rede remota.

> **Note**: Se o Smart-Tunnel for usado para um marcador, o endereço IP da interface ASA mais próxima do destino ainda será usado.

Configurar

Neste diagrama, há um túnel LAN a LAN entre dois ASAs que permite que o tráfego passe de 192.168.10.x para 192.168.20.x.

A lista de acesso que determina o tráfego interessante para esse 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
```

Se o usuário SSLVPN sem cliente tentar se comunicar com um host na rede 192.168.20.x, o ASA1 usa o endereço 209.165.200.225 como origem desse tráfego. Como a lista de controle de acesso (ACL) de LAN para LAN não contém 209.168.200.225 como uma identidade de proxy, o tráfego não é enviado pelo túnel de LAN para LAN.

Para enviar tráfego pelo túnel LAN para LAN, uma nova entrada de controle de acesso (ACE) deve ser adicionada à ACL de tráfego interessante.

ASA1

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

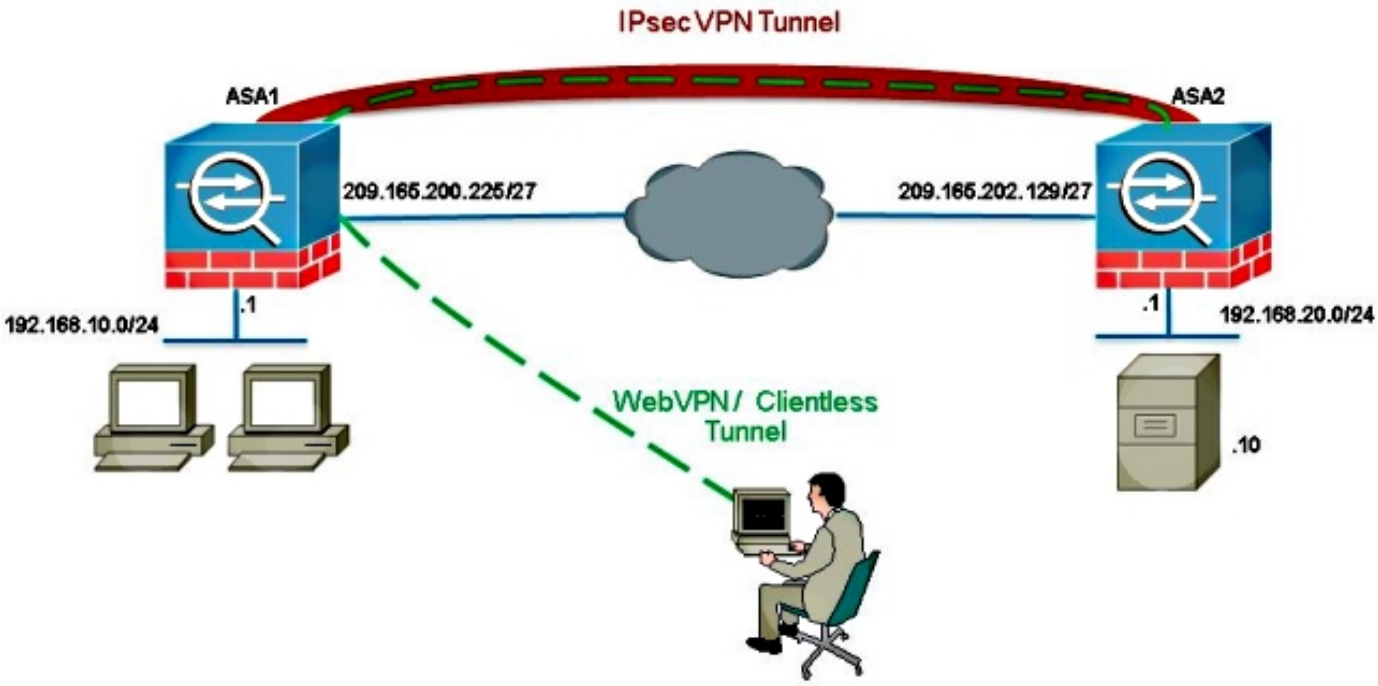
ASA2

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

Este mesmo princípio se aplica às configurações em que o tráfego SSLVPN sem cliente precisa **reativar** a mesma interface em que entrou, mesmo que não seja suposto passar por um túnel de LAN para LAN.

> **Note**: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede



Geralmente, o ASA2 realiza a PAT (Port Address Translation) para o endereço 192.168.20.0/24 para fornecer acesso à Internet. Nesse caso, o tráfego de 192.168.20.0/24 no ASA 2 deve ser excluído do processo PAT quando ele for para 209.165.200.225. Caso contrário, a resposta não passaria pelo túnel de LAN para LAN. Por exemplo:

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
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

- **show crypto ipsec sa**-Verifique com este comando se uma associação de segurança (SA) entre o endereço IP do proxy do ASA1 e a rede remota foi criada. Verifique se os contadores criptografados e descriptografados aumentam quando o usuário de SSLVPN sem cliente acessa esse servidor.

Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

Se a associação de segurança não for criada, você poderá usar a depuração de IPsec para a causa da falha:

- **debug crypto ipsec <level>**

  Note: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug.**