Conexão de cliente de VPN ASA com um exemplo da configuração de túnel L2L

Índice

Introdução

Este documento descreve como configurar a ferramenta de segurança adaptável de Cisco (ASA) a fim permitir uma conexão de cliente de VPN remota (L2L) de um endereço de peer LAN-à-LAN.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco ASA
- Acessos remoto VPN
- LAN para LAN VPN

Componentes Utilizados

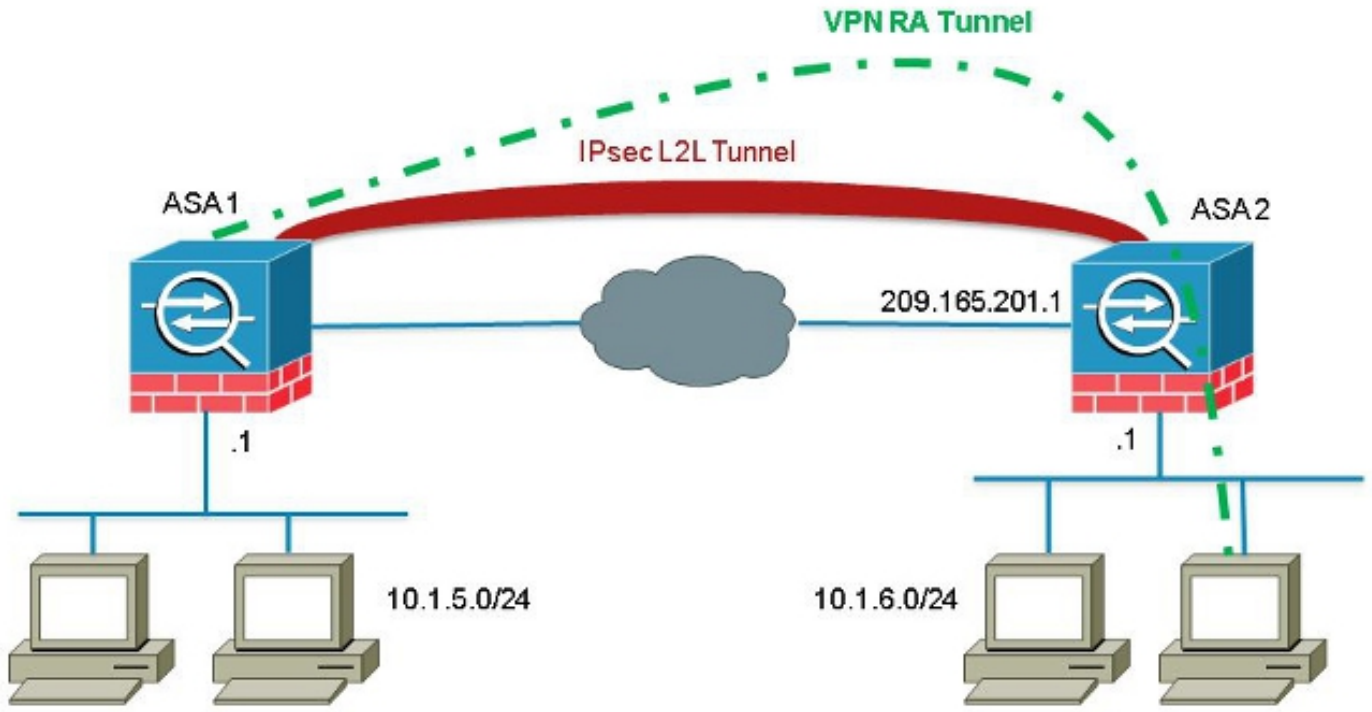
A informação neste documento é baseada no Cisco 5520 Series ASA que executa a versão de software 8.4(7).

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Embora não fossem comuns encontrar uma encenação onde um cliente VPN tentasse estabelecer uma conexão através de um túnel L2L, os administradores puderam querer atribuir privilégios ou restrições de acesso específicas a determinados usuários remotos e instrui-los para usar o cliente de software quando o acesso a estes recursos é exigido.

> Nota: Esta encenação trabalhada no passado, mas depois que uma elevação do final do cabeçalho ASA à versão 8.4(6) ou mais recente, o cliente VPN é já não possa estabelecer a conexão.



A identificação de bug Cisco CSCuc75090 introduziu uma mudança do comportamento. Previamente, com o intercâmbio de Internet privada (PIX), quando o proxy da segurança de protocolo do Internet (IPsec) não combinou um Access Control List do mapa cript. (ACL), continuou a verificar entradas mais abaixo da lista. Isto incluiu os fósforos com um mapa cripto dinâmico sem o par especificados.

Isto foi considerado uma vulnerabilidade, porque os administradores remotos poderiam aceder aos recursos que o administrador do final do cabeçalho não pretendeu quando o L2L estático foi configurado.

Um reparo foi criado que adicionasse uma verificação a fim impedir fósforos com uma entrada do mapa cript. sem um par quando já verificou uma entrada de mapa que combinasse o par. Contudo, isto afetou a encenação que é discutida neste documento. Especificamente, um cliente VPN remoto que tente conectar de um endereço de peer L2L não pode conectar ao final do cabeçalho.

Configurar

Use esta seção a fim configurar o ASA a fim permitir uma conexão de cliente de VPN remota de um endereço de peer L2L.

Adicionar uma entrada dinâmica nova

A fim permitir conexões de VPN remotas dos endereços de peer L2L, você deve adicionar uma entrada dinâmica nova que contenha o mesmo endereço IP do peer.

> Nota: Você deve igualmente deixar uma outra entrada dinâmica sem um par de modo que todo o cliente do Internet possa conectar também.

Está aqui um exemplo da configuração em funcionamento precedente do mapa cripto dinâmico:

```
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
```

Está aqui a configuração do mapa cripto dinâmico com a entrada dinâmica nova 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
```

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.