Dispositivo do gateway de VPN configurado como o que responde na negociação cripto

Índice

Introdução

Este documento fornece a informação em como configurar um dispositivo do gateway de VPN para atuar sempre como um que responde em uma negociação de IKE. O dispositivo responderá a todas as negociações criptos iniciadas por seus pares.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Roteador Cisco com Software Release 12.4(24)T e Mais Recente de Cisco IOS®
- Ferramenta de segurança adaptável de Cisco (ASA) com versão 7.0 e mais recente

Produtos Relacionados

Este documento pode igualmente ser usado com estes versão de hardware e software:

- Cisco PIX Firewall com versão de software 7.0 e mais atrasado

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Toda a negociação cripto tem dois partidos para jogar os papéis do iniciador e do que responde. O iniciador envia as propostas criptos ao que responde que contém parâmetros diferentes sobre a criptografia, algoritmos de autenticação, re-fechando opções e os valores da vida e assim por diante. O que responde escolhe a proposta direita e uma sessão de criptografia estabelece. O papel jogado por um dispositivo final pode ser visto por este comando output:

```
Router#show crypto isakmp sa1 IKE Peer: XX.XX.XX.XX Type : L2L Role : initiator Rekey : no State
: MM_ACTIVE ASA(config)#show crypto isakmp sa detailIKE Peer Type Dir Rky State Encrypt Hash Auth
Lifetime1 209.165.200.225 User Resp No AM_Active 3des SHA preshrd 86400
```

Benefícios da característica do modo do que responde-Somente IKE

Desde que o advento das características do Virtual Private Network (VPN) que permitem negociações de IKE bidirecionais simultâneas (com ou sem o tráfego interessante), as edições com a manipulação e a recuperação dos dados da duplicata IKE SA ocorreram. O IKE como um protocolo não tem nenhuma capacidade para comparar negociações de IKE para determinar se há já uma negociação da existência ou do em-processo entre dois pares que ocorrem. Estas negociações duplicadas podem ser caras em termos dos recursos e da confusão aos administradores de roteador. Quando um dispositivo é configurado como um dispositivo do que responde-somente, não iniciará modos principais, agressivos, ou rápidos IKE (para o estabelecimento IKE e IPsec SA), nem rekey o IKE e o sas de IPSec. Consequentemente, a probabilidade da duplicata SA é reduzida.

O outro benefício desta característica é permitir apoio controlado para conexões de negócio em um sentido somente em uma encenação da função de balanceamento de carga. Não se recomenda que os server ou o Hubs iniciam conexões de VPN para os clientes ou o spokes porque estes dispositivos são todos que estão sendo alcançados por um endereço IP de Um ou Mais Servidores Cisco ICM NT do único-revestimento como anunciado através do equilibrador da carga. Se o Hubs era iniciar a conexão, estaria fazendo assim usando um endereço IP de Um ou Mais Servidores Cisco ICM NT individual, assim contornando os benefícios do equilibrador da carga. O mesmo é verdadeiro de rekeying os pedidos que são originado do Hubs ou dos server atrás do equilibrador da carga.

Um roteador a ser configurado como um dispositivo do que responde-Somente em uma negociação cripto

O Cisco IOS Software Release 12.4(24)T introduz a funcionalidade do roteador para responder sempre às negociações de IKE iniciadas por seus pares. A limitação principal é que esta característica é configurável somente sob um perfil IPSec e é relevante somente a uma encenação da interface virtual. Nenhum apoio para encenações da estática ou do mapa cripto

dinâmico.

A fim configurar seu roteador como o que responde-somente, execute estas etapas:

```
enable configure terminal crypto ipsec profile <name>   responder-only
```

Um ASA a ser configurado como um dispositivo do que responde-Somente em uma negociação cripto

Em conexões de LAN para LAN gerais do IPsec, o ASA pode funcionar como o iniciador ou o que responde. Em conexões do IPsec cliente-à-LAN, o ASA funciona somente como o que responde. Um ASA pode ser configurado como responde-somente dispositivo em conexões de VPN do LAN para LAN. Contudo, a limitação é que o dispositivo no outro extremo do túnel VPN deve ser um destes:

- Dispositivo do 5500 Series de Cisco ASA
- Concentrador da Cisco VPN 3000 Series
- Series Firewall do Cisco PIX 500 que executa o software 7.0 e mais tarde

A fim configurar seu ASA como o dispositivo do que responde-somente, emita este comando:

resposta-somente ajustada do tipo de conexão do mymap 10 do crypto map do hostname(config)#

Nota: Sugere-se para configurar um dispositivo do gateway de VPN como o que responde-somente onde os pares múltiplos VPN terminam.

Informações Relacionadas

- Configurando um túnel roteador a roteador LAN a LAN com um roteador que inicia o modo assertivo IKE
- Exemplos e TechNotes da configuração ASA Cisco
- Suporte Técnico e Documentação - Cisco Systems