Configurando o IPsec - Chaves pré-compartilhada curinga com Cisco Secure VPN Client e configuração Nenhum-MODE

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Convenções
Configurar
Diagrama de Rede
Configurações
Verificar
Troubleshooting
Comandos para Troubleshooting
Informações Relacionadas

Introdução

Esta configuração de exemplo ilustra um roteador configurado para chaves pré-compartilhada curinga — todos os clientes PC compartilham de uma chave comum. Um usuário remoto incorpora a rede, mantendo seu próprio endereço IP de Um ou Mais Servidores Cisco ICM NT; os dados entre o PC de um usuário remoto e o roteador são cifrados.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nas versões de software e hardware abaixo.

- Software Release 12.2.8.T1 de Cisco IOS®
- Versão 1.0 ou 1.1 do Cisco Secure VPN Client — Fim da vida útil
- Roteador Cisco com imagem DES ou 3DES

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 você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Para localizar informações adicionais sobre os comandos usados neste documento, utilize a Ferramenta Command Lookup (somente clientes registrados).

Diagrama de Rede

Este documento utiliza a instalação de rede mostrada no diagrama abaixo.

Configurações

Este documento utiliza as configurações mostradas abaixo.

- Configuração do roteador
- Configuração de cliente de VPN

Configuração do roteador

```
Current configuration:
!
version 12.2

service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RTCisco
!
enable password hjwwkj
!
!
ip subnet-zero
ip domain-name cisco.com
ip name-server 203.71.57.242
!
!
crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key mysecretkey address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set mypolicy esp-des esp-md5-hmac
!
```

```
crypto dynamic-map dyna 10
set transform-set mypolicy
!
crypto map test 10 ipsec-isakmp dynamic dyna
!
!
interface Serial0
ip address 203.71.90.182 255.255.255.252
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
crypto map test
!
interface Ethernet0
ip address 88.88.88.1 255.255.255.0
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 203.71.90.181
!
!
line con 0
transport input none
line aux 0
transport input all
line vty 0 4
password cscscs
login
!
end
```

Configuração de cliente de VPN

```
Current configuration:
!
version 12.2

service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RTCisco
!
enable password hjwwkj
!
!
ip subnet-zero
ip domain-name cisco.com
ip name-server 203.71.57.242
!
!
crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key mysecretkey address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set mypolicy esp-des esp-md5-hmac
!
crypto dynamic-map dyna 10
set transform-set mypolicy
!
crypto map test 10 ipsec-isakmp dynamic dyna
!
!
```

```
interface Serial0
ip address 203.71.90.182 255.255.255.252
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
crypto map test
!
interface Ethernet0
ip address 88.88.88.1 255.255.255.0
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 203.71.90.181
!
!
line con 0
transport input none
line aux 0
transport input all
line vty 0 4
password cscscs
login
!
end
```

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

- show crypto isakmp sa — Mostra as associações de segurança da Fase 1.
- **mostre IPsec cripto sa** — Associações de segurança e proxy da fase 1 das mostras, encapsulamento, criptografia, decapsulation, e informação de descriptografia.
- **active do show crypto engine connections** — Conexões atual e informação das mostras em relação aos pacotes criptografado e decriptografado.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Comandos para Troubleshooting

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

Nota: Antes de emitir comandos de depuração, consulte as informações importantes sobre eles.

Nota: Você deve cancelar associações de segurança em ambos os pares. Execute os comandos router no modo não habilitado.

Nota: Você deve executar estes debuga em ambos os ipsec peer.

- debug crypto isakmp — Exibe erros durante a Fase 1.
- debug crypto ipsec — Exibe erros durante a Fase 2.
- debug crypto engine — Exibe informações a partir do cripto mecanismo.
- **cancele o isakmp cripto** — Cancela as associações de segurança da fase 1.
- clear crypto sa —— Limpa as associações de segurança da Fase 2.

Informações Relacionadas

- Página de suporte do IPSec
- Páginas de suporte do VPN 3000 Client
- Suporte Técnico - Cisco Systems