Configurando IPSec - chaves pré-compartilhadas curinga com Cisco Secure VPN Client e configuração no modo

Contents

Introduction

Esta configuração de exemplo ilustra um roteador configurado para chaves pré-compartilhadas curinga—todos os clientes de PC compartilham uma chave comum. Um usuário remoto entra na rede, mantendo seu próprio endereço IP; os dados entre o PC de um usuário remoto e o roteador são criptografados.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Software Cisco IOS® versão 12.2.8.T1
- Cisco Secure VPN Client versão 1.0 ou 1.1—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. All of the devices used in this document started with a cleared (default)

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

Conventions

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

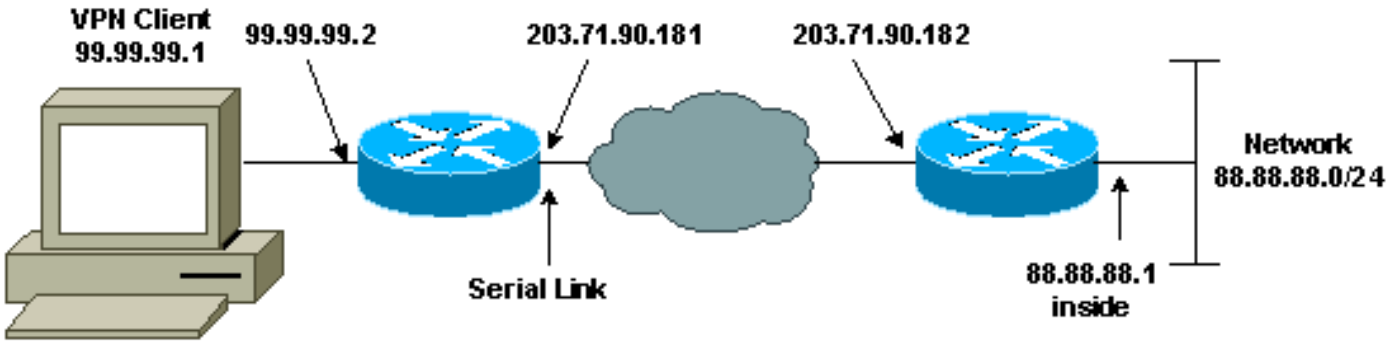
Configurar

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

Observação: para encontrar informações adicionais sobre os comandos usados neste documento, use a ferramenta Command Lookup Tool (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

```
Network Security policy:


1- Myconn
    My Identity
         Connection security: Secure
         Remote Party Identity and addressing
         ID Type: IP subnet
         88.88.88.0
         255.255.255.0
         Port all Protocol all


    Connect using secure tunnel
         ID Type: IP address
         203.71.90.182
```

```
    Authentication (Phase 1)
    Proposal 1

        Authentication method: Preshared key
        Encryp Alg: DES
        Hash Alg: MD5
        SA life:  Unspecified
        Key Group: DH 1

    Key exchange (Phase 2)
    Proposal 1
        Encapsulation ESP
        Encrypt Alg: DES
        Hash Alg: MD5
        Encap: tunnel
        SA life: Unspecified
        no AH

2- Other Connections
       Connection security: Non-secure
       Local Network Interface
         Name: Any
         IP Addr: Any
         Port: All
```

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.**
- **show crypto ipsec sa** —Mostra as associações de segurança da Fase 1 e informações de proxy, encapsulamento, criptografia, desencapsulamento e descriptografia.
- **show crypto engine connections ative** —Mostra as conexões e informações atuais sobre pacotes criptografados e descriptografados.

Troubleshoot

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.

Observação: antes de inserir o comando **debug**, consulte Informações importantes sobre os comandos debug.

Observação: você deve limpar associações de segurança em ambos os pares. Execute os comandos do roteador no modo não habilitado.

Observação: você deve executar essas depurações em ambos os peers de IPSec.

- **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.**
- **clear crypto isakmp** —Limpa 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 ao cliente VPN 3000
- Suporte Técnico - Cisco Systems