Configuración de IPSec - Claves previamente compartidas comodín con Cisco Secure VPN Client y configuración sin modo

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Convenciones](#)
[Configurar](#)
[Diagrama de la red](#)
[Configuraciones](#)
[Verificación](#)
[Troubleshoot](#)
[Comandos para resolución de problemas](#)
[Información Relacionada](#)

Introducción

Esta configuración de ejemplo ilustra un router configurado para claves previamente compartidas comodín: todos los clientes de PC comparten una clave común. Un usuario remoto ingresa a la red, manteniendo su propia dirección IP; los datos entre la PC de un usuario remoto y el router están cifrados.

Prerequisites

Requirements

No hay requisitos previos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las versiones de software y hardware indicadas a continuación.

- Versión 12.2.8.T1 del software del IOS® de Cisco
- Cisco Secure VPN Client versión 1.0 o 1.1—Fin de vida útil
- Router de Cisco con imagen DES o 3DES

La información que se presenta en este documento se originó a partir de dispositivos dentro de un

ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

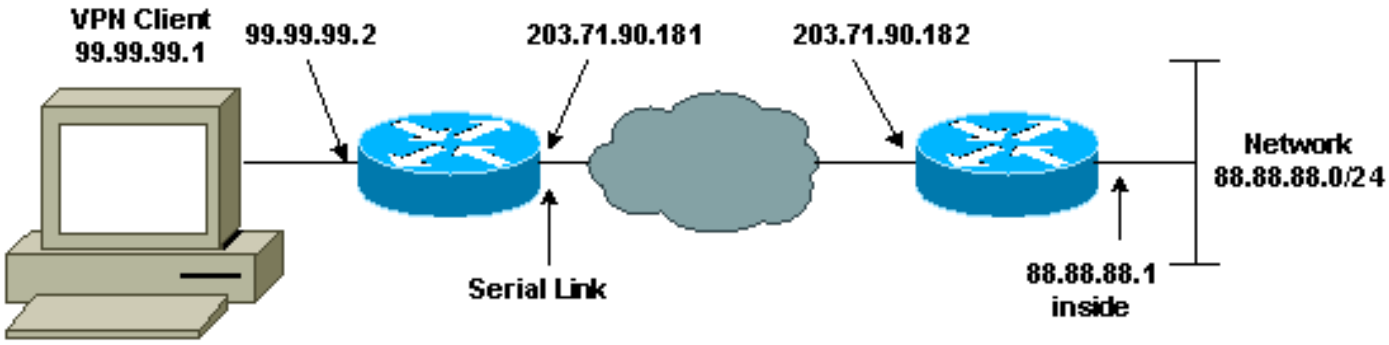
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Para encontrar información adicional sobre los comandos usados en este documento, utilice la Command Lookup Tool (sólo clientes registrados) .

Diagrama de la red

Este documento utiliza la instalación de red que se muestra en el siguiente diagrama.



Configuraciones

Este documento usa las configuraciones detalladas a continuación.

- Configuración del router
- Configuración de cliente VPN

Configuración del router

```
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
```

Configuración de cliente 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
```

Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- **show crypto ipsec sa — Muestra las asociaciones de seguridad de la fase 1.**
- **show crypto ipsec sa** —Muestra las asociaciones de seguridad de la Fase 1 y la información de proxy, encapsulación, cifrado, desencapsulación y descifrado.
- **show crypto engine connections active** —Muestra las conexiones actuales y la información relacionada con los paquetes cifrados y descifrados.

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Comandos para resolución de problemas

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

Nota: Antes de ejecutar un comando **debug**, consulte Información Importante sobre Comandos Debug.

Nota: Debe borrar las asociaciones de seguridad en ambos pares. Ejecute los comandos del router en modo no activado.

Nota: Debe ejecutar estas depuraciones en ambos pares IPSec.

- **debug crypto ipsec — Muestra errores durante la fase 1.**
- **debug crypto ipsec — Muestra errores durante la fase 2.**
- **debug crypto engine — Muestra información del motor de criptografía.**
- **clear crypto isakmp Elimina las asociaciones de seguridad de fase 1.**
- **clear crypto sa—Elimina las asociaciones de seguridad de la Fase 2.**

Información Relacionada

- Página de soporte de IPSec
- Páginas de soporte del cliente VPN 3000
- Soporte Técnico - Cisco Systems