Configurando el IPSec - Claves comodín previamente compartidas con el Cliente Cisco Secure VPN y los Config Ninguno-MODE

Contenido

Introducción

Esta configuración de muestra ilustra a un router configurado para las claves comodín previamente compartidas — todos los PC cliente comparten una clave común. Un usuario remoto ingresa la red, guardando su propio IP Address; los datos entre el PC de un usuario remoto y el router se cifran.

prerrequisitos

Requisitos

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.

- Software Release 12.2.8.T1 de Cisco IOS®
- Versión 1.0 o 1.1 del Cliente Cisco Secure VPN — Fin de vida
- Router Cisco con la 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. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). 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.

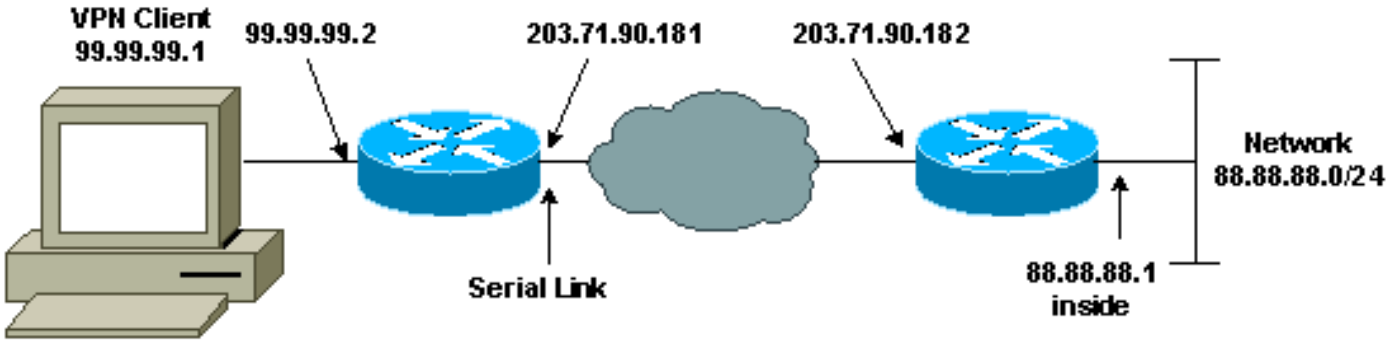
Configurar

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

Nota: Para obtener información adicional sobre los comandos que se utilizan en este documento, use la Command Lookup Tool (solo para 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

```
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
```

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.
- **muestre IPSec crypto sa** — Asociaciones de seguridad y proxy de la fase 1 de las demostraciones, encapsulación, cifrado, decapsulation, y información de descifrado.
- **active del show crypto engine connections** — Conexiones actuales e información de las demostraciones con respecto a los paquetes encriptados y desencriptados.

Troubleshooting

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 de depuración, consulte Información importante sobre comandos de depuración.

Nota: Usted debe borrar las asociaciones de seguridad en ambos pares. Realice los comandos router en el modo no activado.

Nota: Usted debe ejecutar estos debugs en ambos peeres 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 VPN 3000 Client
- Soporte Técnico - Cisco Systems