

# Configuración de IPSec router a router completamente mallado

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshooting](#)

[Comandos para resolución de problemas](#)

[Información Relacionada](#)

## [Introducción](#)

Esta configuración de muestra muestra la encriptación totalmente mallada entre tres Routers con el uso de una correspondencia de criptografía en cada router a las redes detrás de cada uno de sus dos pares.

Se debe realizar el encriptación desde:

- red 160.160.160.x a red 170.170.170.x
- 160.160.160.x red a 180.180.180.x red
- red 170.170.170.x a la red 180.180.180.x

## [prerrequisitos](#)

### [Requisitos](#)

No hay requisitos específicos para este documento.

### [Componentes Utilizados](#)

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

- Software Release 12.2.7C y 12.2.8(T)4 de Cisco IOS®

- Cisco 2500 y 3600 Router

La información que contiene este documento se creó a partir de los dispositivos en 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 cualquier comando.

## [Convenciones](#)

Para obtener más información sobre las convenciones del documento, consulte las [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 configuración de red que se muestra en el siguiente diagrama.

## [Configuraciones](#)

Este documento usa estas configuraciones.

- [Configuración Dr\\_Whoovie](#)
- [Configuración yertle](#)
- [Configuración thidwick](#)

**Nota:** Estas configuraciones fueron probadas recientemente con el código actual (noviembre de 2003) dentro del documento.

### Configuración Dr\_Whoovie

```
Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname dr_whoovie
!
enable secret 5 $1$KxKv$cbqKsZtQTLJLGPn.tErFZ1
enable password ww
!
ip subnet-zero
!
cns event-service server
!
!--- Internet Key Exchange (IKE) Policies: crypto isakmp
policy 1 authentication pre-share crypto isakmp key
```

```

cisco123 address 150.150.150.3 crypto isakmp key
cisco123 address 150.150.150.2 ! !--- IPsec Policies:
crypto ipsec transform-set 170cisco esp-des esp-md5-hmac
crypto ipsec transform-set 180cisco esp-des esp-md5-hmac
! crypto map ETH0 17 ipsec-isakmp set peer 150.150.150.2
set transform-set 170cisco !--- Include the
160.160.160.x to 170.170.170.x network !--- in the
encryption process. match address 170 crypto map ETH0 18
ipsec-isakmp set peer 150.150.150.3 set transform-set
180cisco !--- Include the 160.160.160.x to 180.180.180.x
network !--- in the encryption process. match address
180 ! interface Ethernet0 ip address 150.150.150.1
255.255.255.0 no ip directed-broadcast no ip route-cache
no ip mroute-cache no mop enabled crypto map ETH0 !
interface Ethernet1 no ip address no ip directed-
broadcast shutdown ! interface Serial0 ip address
160.160.160.1 255.255.255.0 no ip directed-broadcast no
ip mroute-cache no fair-queue ! interface Serial1 no ip
address no ip directed-broadcast clockrate 4000000 ! ip
classless ip route 170.170.170.0 255.255.255.0
150.150.150.2 ip route 180.180.180.0 255.255.255.0
150.150.150.3 no ip http server ! !--- Include the
160.160.160.x to 170.170.170.x network !--- in the
encryption process. access-list 170 permit ip
160.160.160.0 0.0.0.255 170.170.170.0 0.0.0.255 !---
Include the 160.160.160.x to 180.180.180.x network !---
in the encryption process. access-list 180 permit ip
160.160.160.0 0.0.0.255 180.180.180.0 0.0.0.255 dialer-
list 1 protocol ip permit dialer-list 1 protocol ipx
permit ! line con 0 transport input none line aux 0 line
vty 0 4 password ww login ! end

```

## Configuración yertle

```

Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname yertle
!
enable secret 5 $1$me5Q$2kF5zKlPPTvHEBdGiEZ9m/
enable password ww
!
ip subnet-zero
!
cns event-service server
!
!--- IKE Policies: crypto isakmp policy 1 authentication
pre-share crypto isakmp key cisco123 address
150.150.150.3 crypto isakmp key cisco123 address
150.150.150.1 ! !--- IPsec Policies: crypto ipsec
transform-set 160cisco esp-des esp-md5-hmac crypto ipsec
transform-set 180cisco esp-des esp-md5-hmac ! crypto map
ETH0 16 ipsec-isakmp set peer 150.150.150.1 set
transform-set 160cisco !--- Include the 170.170.170.x to
160.160.160.x network !--- in the encryption process.
match address 160 crypto map ETH0 18 ipsec-isakmp set
peer 150.150.150.3 set transform-set 180cisco !---
Include the 170.170.170.x to 180.180.180.x network !---
in the encryption process. match address 180 ! interface
Ethernet0 ip address 150.150.150.2 255.255.255.0 no ip
directed-broadcast no ip route-cache no ip mroute-cache

```

```

no mop enabled crypto map ETH0 ! interface Serial0 no ip
address no ip directed-broadcast no ip mroute-cache
shutdown no fair-queue ! interface Serial1 ip address
170.170.170.1 255.255.255.0 no ip directed-broadcast !
ip classless ip route 160.160.160.0 255.255.255.0
150.150.150.1 ip route 180.180.180.0 255.255.255.0
150.150.150.3 no ip http server ! !--- Include the
170.170.170.x to 160.160.160.x network !--- in the
encryption process. access-list 160 permit ip
170.170.170.0 0.0.0.255 160.160.160.0 0.0.0.255 !---
Include the 170.170.170.x to 180.180.180.x network !---
in the encryption process. access-list 180 permit ip
170.170.170.0 0.0.0.255 180.180.180.0 0.0.0.255 dialer-
list 1 protocol ip permit dialer-list 1 protocol ipx
permit ! line con 0 transport input none line aux 0 line
vty 0 4 password ww login ! end

```

## Configuración thidwick

```

Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname thidwick
!
enable secret 5 $1$Pcpo$fj4FNS1dEDY9lGg3Ne6FK1
enable password ww
!
ip subnet-zero
!
isdn switch-type basic-5ess
isdn voice-call-failure 0
cns event-service server
!
!--- IKE Policies: crypto isakmp policy 1 authentication
pre-share crypto isakmp key cisco123 address
150.150.150.1 crypto isakmp key cisco123 address
150.150.150.2 ! !--- IPSec Policies: crypto ipsec
transform-set 160cisco esp-des esp-md5-hmac crypto ipsec
transform-set 170cisco esp-des esp-md5-hmac ! crypto map
ETH0 16 ipsec-isakmp set peer 150.150.150.1 set
transform-set 160cisco !--- Include the 180.180.180.x to
160.160.160.x network !--- in the encryption process.
match address 160 crypto map ETH0 17 ipsec-isakmp set
peer 150.150.150.2 set transform-set 170cisco !---
Include the 180.180.180.x to 170.170.170.x network !---
in the encryption process. match address 170 ! interface
Ethernet0 ip address 150.150.150.3 255.255.255.0 no ip
directed-broadcast no ip route-cache no ip mroute-cache
no mop enabled crypto map ETH0 ! interface Serial0 no ip
address no ip directed-broadcast no ip mroute-cache no
fair-queue clockrate 4000000 ! interface Serial1 ip
address 180.180.180.1 255.255.255.0 no ip directed-
broadcast clockrate 4000000 ! interface BRI0 no ip
address no ip directed-broadcast shutdown isdn switch-
type basic-5ess ! ip classless ip route 160.160.160.0
255.255.255.0 150.150.150.1 ip route 170.170.170.0
255.255.255.0 150.150.150.2 no ip http server ! !---
Include the 180.180.180.x to 160.160.160.x network !---
in the encryption process. access-list 160 permit ip
180.180.180.0 0.0.0.255 160.160.160.0 0.0.0.255 !---
Include the 180.180.180.x to 170.170.170.x network !---

```

```
in the encryption process. access-list 170 permit ip
180.180.180.0 0.0.0.255 170.170.170.0 0.0.0.255 dialer-
list 1 protocol ip permit dialer-list 1 protocol ipx
permit ! line con 0 transport input none line aux 0 line
vty 0 4 password ww 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.

- **muestre IPsec crypto sa** — Muestra las configuraciones usadas por las asociaciones de seguridad actuales del [IPsec].
- **muestre isakmp crypto sa** — Muestra todas las asociaciones de seguridad actuales IKE en un par.

## Troubleshooting

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

### Comandos para resolución de problemas

**Nota:** [Antes de ejecutar un comando de depuración, consulte Información importante sobre comandos de depuración.](#)

- **IPsec del debug crypto** — Visualiza los IPsec Negotiations de la fase 2.
- **isakmp del debug crypto** — Visualiza las negociaciones del Internet Security Association and Key Management Protocol (ISAKMP) de la fase 1.
- **debug crypto engine** - Muestra el tráfico cifrado.
- **clear crypto isakmp** — Borra las asociaciones de seguridad relacionadas con la fase 1.
- **borre el sa crypto** — Borra las asociaciones de seguridad relacionadas con la fase 2.

## Información Relacionada

- [Página de soporte de IPsec](#)
- [Configuración de seguridad de red IPsec](#)
- [Configuración del protocolo de seguridad de intercambio de claves de Internet](#)
- [Soporte Técnico - Cisco Systems](#)