

# Configuración de la Sobrecarga NAT Precompartida, de Router a Router IPSec entre una Red Privada y una Pública

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Ejemplo de resultado del comando show](#)

[Troubleshoot](#)

[Comandos para resolución de problemas](#)

[Información Relacionada](#)

## Introducción

Esta configuración de ejemplo muestra cómo cifrar el tráfico entre una red privada (10.103.1.x) y una red pública (98.98.98.x) con el uso de IPSec. La red 98.98.98.x conoce a la red 10.103.1.x por las direcciones privadas. La red 10.103.1.x conoce a la red 98.98.98.x por las direcciones públicas.

## Prerequisites

### Requirements

Este documento requiere una comprensión básica del protocolo IPSec. Si desea más información sobre IPSec, consulte [Introducción al encriptación de seguridad IP \(IPSec\)](#).

### Componentes Utilizados

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

- Software Cisco IOS® versión 12.3(5)

- Routers Cisco 3640

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). If your network is live, make sure that you understand the potential impact of any command.

## Convenciones

Para obtener más información sobre las convenciones del documento, consulte [Convenciones de Consejos Técnicos de Cisco](#).

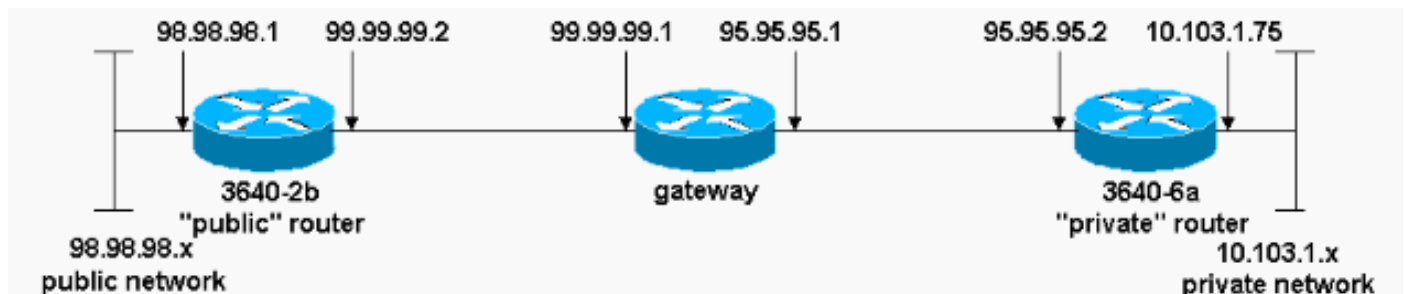
## Configurar

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

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

## Diagrama de la red

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



## Configuraciones

En este documento, se utilizan estas configuraciones:

- [Router "público" 3640-2b](#)
- [Router "privado" 3640-6a](#)

```
<#root>
rp-3640-2b#
show running config
Building configuration...
```

Current configuration:

```
!  
version 12.3  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption
```

```
!  
hostname rp-3640-2b
```

```
!  
ip subnet-zero
```

```
!  
!
```

*!--- Defines the Internet Key Exchange (IKE) policies.*

```
crypto isakmp policy 1
```

*!--- Defines an IKE policy. Use the*

```
crypto isakmp policy
```

*!--- command in global configuration mode. IKE policies !--- define a set of parameters !--- that are*

```
hash md5  
authentication pre-share
```

*!--- Specifies preshared keys as the authentication method.*

```
crypto isakmp key cisco123 address 95.95.95.2
```

*!--- Configures a preshared authentication key, used in !--- global configuration mode.*

```
!
```

```
crypto ipsec transform-set rtpset esp-des esp-md5-hmac
```

*!--- Defines a transform-set. This is an acceptable !--- combination of security protocols and algorit*

```
!
```

```
crypto map rtp 1 ipsec-isakmp
```

*!--- Indicates that IKE is used to !--- establish the IPSec security associations (SAs) that protect !*

```
set peer 95.95.95.2
```

*!--- Sets the IP address of the remote end.*

```
set transform-set rtpset
```

*!--- Configures IPsec to use the transform-set !--- "rtpset" defined earlier.*

```
match address 115
```

*!--- This is used to assign an extended access list to a !--- crypto map entry which is used by IPsec*

```
!  
interface Ethernet0/0  
ip address 98.98.98.1 255.255.255.0  
no ip directed-broadcast  
!
```

```
interface Ethernet0/1  
ip address 99.99.99.2 255.255.255.0  
no ip directed-broadcast  
no ip route-cache
```

*!--- Enable process switching for !--- IPsec to encrypt outgoing packets. !--- This command disables f*

```
no ip mroute-cache
```

```
crypto map rtp
```

*!--- Configures the interface to use !--- the crypto map "rtp" for IPsec.*

```
!
```

```
.  
.
```

*!--- Output suppressed.*

```
.  
.
```

```
ip classless
ip route 0.0.0.0 0.0.0.0 99.99.99.1

!--- Default route to the next hop address.

no ip http server
!
access-list 115 permit ip 98.98.98.0 0.0.0.255 10.103.1.0 0.0.0.255

!--- This access-list option causes all IP traffic !--- that matches the specified conditions to be !---

crypto map
  command statements.

access-list 115 deny ip 98.98.98.0 0.0.0.255 any

!
line con 0
transport input none
line aux 0
line vty 0 4
login
!
end
```

Router

```
<#root>
rp-3640-6a#
show running config
Building configuration...

Current configuration:
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname rp-3640-6a
!
!
ip subnet-zero
```

*!--- Defines the IKE policies.*

!

```
crypto isakmp policy 1
```

*!--- Defines an IKE policy. !--- Use the*

```
crypto isakmp policy
```

*!--- command in global configuration mode. IKE policies !--- define a set of parameters !--- that are*

```
hash md5
```

```
authentication pre-share
```

*!--- Specifies preshared keys as the authentication method.*

```
crypto isakmp key cisco123 address 99.99.99.2
```

*!--- Configures a preshared authentication key, !--- used in global configuration mode.*

!

```
crypto ipsec transform-set rtpset esp-des esp-md5-hmac
```

*!--- Defines a transform-set. This is an !--- acceptable combination of security protocols and algorithm*

```
crypto map rtp 1 ipsec-isakmp
```

*!--- Indicates that IKE is used to establish !--- the IPSec SAs that protect the traffic !--- specified*

```
set peer 99.99.99.2
```

*!--- Sets the IP address of the remote end.*

```
set transform-set rtpset
```

*!--- Configures IPsec to use the transform-set !--- "rtpset" defined earlier.*

```
match address 115
```

*!--- Used to assign an extended access list to a !--- crypto map entry which is used by IPsec !--- to*

```
.  
.
```

*!--- Output suppressed.*

```
.  
.  
!
```

```
interface Ethernet3/0  
ip address 95.95.95.2 255.255.255.0  
no ip directed-broadcast  
  
ip nat outside
```

*!--- Indicates that the interface is !--- connected to the outside network.*

```
no ip route-cache
```

*!--- Enable process switching for !--- IPsec to encrypt outgoing packets. !--- This command disables f*

```
no ip mroute-cache
```

```
crypto map rtp
```

*!--- Configures the interface to use the !--- crypto map "rtp" for IPsec.*

```
!  
interface Ethernet3/2  
ip address 10.103.1.75 255.255.255.0  
no ip directed-broadcast  
  
ip nat inside
```

*!--- Indicates that the interface is connected to !--- the inside network (the network subject to NAT*

```
!
```

```
ip nat pool FE30 95.95.95.10 95.95.95.10 netmask 255.255.255.0
```

*!--- Used to define a pool of IP addresses for !--- NAT. Use the*

```
ip nat pool
```

```
command in !--- global configuration mode.
```

```
ip nat inside source route-map nonat pool FE30 overload
```

*!--- Used to enable NAT of !--- the inside source address. Use the*

```
ip nat inside source
```

```
!--- command in global configuration mode. !--- The 'overload' option enables the router to use one g
```

```
ip classless
```

```
ip route 0.0.0.0 0.0.0.0 95.95.95.1
```

*!--- Default route to the next hop address.*

```
no ip http server
```

```
!
```

```
access-list 110 deny ip 10.103.1.0 0.0.0.255 98.98.98.0 0.0.0.255
```

```
access-list 110 permit ip 10.103.1.0 0.0.0.255 any
```

*!--- Addresses that match this ACL are NATed while !--- they access the Internet. They are not NATed !-*

```
access-list 115 permit ip 10.103.1.0 0.0.0.255 98.98.98.0 0.0.0.255
```

*!--- This access-list option causes all IP traffic that !--- matches the specified conditions to be !-*

```
crypto map
```

```
command statements.
```

```
access-list 115 deny ip 10.103.1.0 0.0.0.255 any
```

```
route-map nonat permit 10
```

```
match ip address 110
```

```
!
```



```
!  
line con 0  
  
line vty 0 4  
  
!  
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.

Para verificar esta configuración, pruebe un comando ping extendido originado en la interfaz Ethernet en el router privado 10.103.1.75, destinado a la interfaz Ethernet en el router público 98.98.98.1

- [ping](#) — Se utiliza para diagnosticar la conectividad básica de la red.

```
<#root>  
  
rp-3640-6a#  
  
ping  
  
Protocol [ip]:  
Target IP address: 98.98.98.1  
Repeat count [5]:  
Datagram size [100]:  
Timeout in seconds [2]:  
Extended commands [n]: y  
Source address or interface: 10.103.1.75  
Type of service [0]:  
Set DF bit in IP header? [no]:  
Validate reply data? [no]:  
Data pattern [0xABCD]:  
Loose, Strict, Record, Timestamp, Verbose[none]:  
Sweep range of sizes [n]:  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 98.98.98.1, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/64/68 ms
```

- [show crypto ipsec sa](#): muestra la configuración utilizada por las SA (IPSec) actuales.
- [show crypto isakmp sa](#) — Muestra todas las IKE SAs actuales en un par.

- [show crypto engine](#): muestra un resumen de la información de configuración para los motores criptográficos. Utilice el comando show crypto engine en el modo EXEC privilegiado.

## Ejemplo de resultado del comando show

Este resultado proviene del comando show crypto ipsec sa ejecutado en el router hub.

```
<#root>
rp-3640-6a#
show crypto ipsec sa

interface: Ethernet0/0
  Crypto map tag: rtp, local addr. 95.95.95.2

  protected vrf:
    local ident (addr/mask/prot/port): (
10.103.1.0
/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (
98.98.98.0
/255.255.255.0/0/0)
    current_peer: 99.99.99.2:500
      PERMIT, flags={origin_is_acl,}
      #pkts encaps: 5, #pkts encrypt: 5, #pkts digest 5
      #pkts decaps: 14, #pkts decrypt: 14, #pkts verify 14
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts compr. failed: 0
      #pkts not decompressed: 0, #pkts decompress failed: 0
      #send errors 0, #recv errors 0

local crypto endpt.: 95.95.95.2, remote crypto endpt.: 99.99.99.2

  path mtu 1500, media mtu 1500
  current outbound spi: 75B6D4D7

inbound esp sas:

  spi: 0x71E709E8(1910966760)
    transform:

  esp-des esp-md5-hmac

,
  in use settings ={Tunnel, }
  slot: 0, conn id: 2000, flow_id: 1, crypto map: rtp
  sa timing: remaining key lifetime (k/sec): (4576308/3300)
  IV size: 8 bytes
  replay detection support: Y
```

```
inbound ah sas:

inbound pcp sas:

outbound esp sas
:
  spi: 0x75B6D4D7(1974916311)
  transform:
esp-des esp-md5-hmac
,
  in use settings ={Tunnel, }
  slot: 0, conn id: 2001, flow_id: 2, crypto map: rtp
  sa timing: remaining key lifetime (k/sec): (4576310/3300)
  IV size: 8 bytes
  replay detection support: Y

outbound ah sas:

outbound pcp sas:
```

Este comando muestra las SA IPsec generadas entre peers. El túnel cifrado se crea entre 95.95.95.2 y 99.99.99.2 para el tráfico que va entre las redes 98.98.98.0 y 10.103.1.0. Puede ver las dos SA de carga de seguridad de encapsulación (ESP) generadas en sentido entrante y saliente. Las SA de encabezado de autenticación (AH) no se utilizan porque no hay AH.

## 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 los comandos debug, consulte [Información Importante sobre Comandos Debug](#).

- debug crypto ipsec sa: se utiliza para ver las negociaciones IPsec de la fase 2.
- debug crypto isakmp sa: se utiliza para ver las negociaciones ISAKMP de la fase 1.
- debug crypto engine: se utiliza para mostrar las sesiones cifradas.

## Información Relacionada

- [Orden de Funcionamiento de NAT](#)

- [Resolución de problemas de seguridad de IP – Información y uso de los comandos de depuración](#)
- [Página de soporte de IPSec](#)
- [Página de Soporte de NAT](#)
- [Soporte Técnico - Cisco Systems](#)

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).