

Configurazione del sovraccarico NAT pre-condiviso da router a router IPSec tra una rete privata e una rete pubblica

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Output di esempio](#)

[Risoluzione dei problemi](#)

[Comandi per la risoluzione dei problemi](#)

[Informazioni correlate](#)

[Introduzione](#)

In questa configurazione di esempio viene illustrato come eseguire la crittografia del traffico tra una rete privata (10.103.1.x) e una rete pubblica (98.98.98.x) con l'utilizzo di IPSec. La rete 98.98.98.x conosce la rete 10.103.1.x dagli indirizzi privati. La rete 10.103.1.x conosce la rete 98.98.98.x dagli indirizzi pubblici.

[Prerequisiti](#)

[Requisiti](#)

Questo documento richiede una conoscenza di base del protocollo IPSec. Per ulteriori informazioni su IPSec, vedere [Introduzione alla crittografia IPSec \(IP Security\)](#).

[Componenti usati](#)

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software Cisco IOS® versione 12.3(5)
- Cisco 3640 Router

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

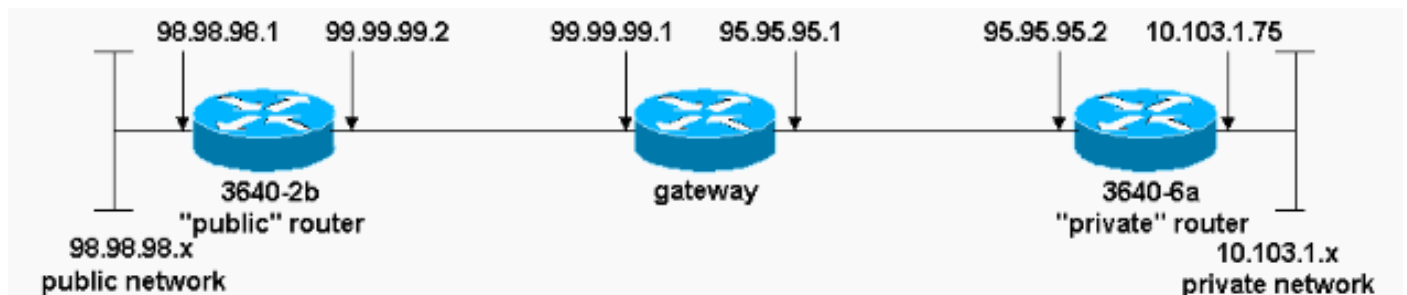
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo [strumento di ricerca dei comandi](#) (solo utenti [registrati](#)).

Esempio di rete

Nel documento viene usata l'impostazione di rete mostrata nel diagramma.



Configurazioni

Nel documento vengono usate queste configurazioni:

- [3640-2b "Public" Router](#)
- [3640-6a "Private" Router](#)

3640-2b "Public" Router

```
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 used  
during the IKE phase I negotiation.  
  
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 algorithms, !---  
which has to be matched on the peer router. ! crypto map  
rtp 1 ipsec-isakmp  
  
!--- Indicates that IKE is used to !--- establish the  
IPSec security associations (SAs) that protect !--- the  
traffic specified by this crypto map entry. 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 !--- to  
determine which traffic should be protected !--- by  
crypto and which traffic does not !--- need crypto  
protection. ! 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 fast  
switching. 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 !---  
protected by IPSec using the policy described by !---
```

the corresponding 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
```

3640-6a "Private" Router

```
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
used during the IKE phase I negotiation.

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 algorithms, !---
which has to be matched on the peer router. crypto map
rtp 1 ipsec-isakmp

!--- Indicates that IKE is used to establish !--- the
IPSec SAs that protect the traffic !--- specified by
this crypto map entry. 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
determine which traffic should be protected !--- by
crypto and which traffic does not !--- need crypto
protection. . . !--- 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 fast
switching. 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
translation). ! 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 global !--- address for
many local addresses.

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 !--- if
they access the 98.98.98.0 network. 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 !---
protected by IPsec using the policy described !--- by
the corresponding 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
```

Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi **show** sono supportati dallo [strumento Output Interpreter \(solo utenti registrati\)](#); lo strumento permette di visualizzare un'analisi dell'output del comando **show**.

Per verificare questa configurazione, provare a usare un comando **ping** esteso inviato dall'interfaccia Ethernet del router privato 10.103.1.75 e destinato all'interfaccia Ethernet del router pubblico 98.98.98.1

- **ping**: utilizzato per diagnosticare la connettività di rete di base.

```
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**: visualizza le impostazioni utilizzate dalle associazioni di protezione (SA) correnti (IPSec).
- **show crypto isakmp sa**: visualizza tutte le associazioni di protezione IKE correnti in un peer.
- **show crypto engine**: visualizza un riepilogo delle informazioni di configurazione per i motori di crittografia. Utilizzare il comando **show crypto engine** in modalità di esecuzione privilegiata.

Output di esempio

Questo output viene generato dal comando **show crypto ipsec sa** emesso sul router hub.

```
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:

```

Con questo comando vengono visualizzate le associazioni di protezione IPsec create tra peer. Il tunnel crittografato è costruito tra la rete 95.95.95.2 e la rete 99.99.99.2 per il traffico che va tra la rete 98.98.98.0 e la rete 10.103.1.0. Si possono vedere le due SA Encapsulating Security Payload (ESP) costruite in entrata e in uscita. Le associazioni di protezione (SA) per le intestazioni di autenticazione non vengono utilizzate poiché non sono presenti associazioni di protezione.

[Risoluzione dei problemi](#)

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

[Comandi per la risoluzione dei problemi](#)

Alcuni comandi **show** sono supportati dallo [strumento Output Interpreter \(solo utenti registrati\)](#); lo

[strumento permette di visualizzare un'analisi dell'output del comando show](#).

Nota: prima di usare i comandi di **debug**, consultare le [informazioni importanti sui comandi di debug](#).

- **debug crypto ipsec sa:** utilizzato per visualizzare le negoziazioni IPsec della fase 2.
- **debug crypto isakmp sa:** utilizzato per visualizzare le negoziazioni ISAKMP della fase 1.
- **debug crypto engine:** utilizzato per visualizzare le sessioni crittografate.

[Informazioni correlate](#)

- [Ordine delle operazioni NAT](#)
- [Risoluzione dei problemi di sicurezza IP - Informazioni e uso dei comandi di debug](#)
- [Pagina di supporto per IPsec](#)
- [Pagina di supporto NAT](#)
- [Supporto tecnico – Cisco Systems](#)