De router-to-router van IPSec configureren, voorgedeeld, NAT-overload tussen een privénetwerk en een openbaar netwerk

Inhoud

Inleiding

Deze voorbeeldconfiguratie toont hoe u verkeer tussen een privaat netwerk (10.103.1.x) en een openbaar netwerk (98.98.98.x) met het gebruik van IPSec kunt versleutelen. Het 98.98.98x netwerk kent het 10.103.1.x netwerk door de privé adressen. Het 10.103.1.x netwerk kent het 98.98.98x netwerk door de openbare adressen.

Voorwaarden

Vereisten

Dit document vereist een basisbegrip van IPSec-protocol. Raadpleeg voor meer informatie over IPSec een Inleiding naar IP Security (IPSec) encryptie.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS®-softwarerelease 12.3(5)E
- Cisco 3640 routers

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg voor meer informatie over documentconventies de technische Tips van Cisco.

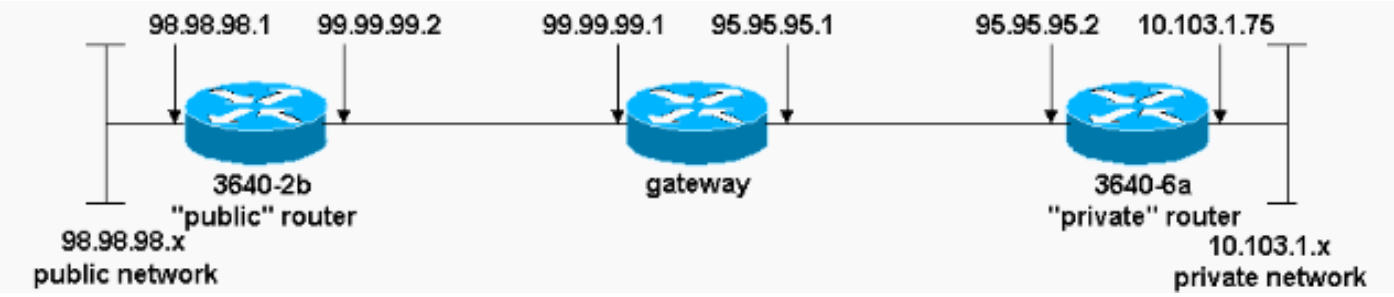
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

N.B.: Als u aanvullende informatie wilt vinden over de opdrachten in dit document, gebruikt u het Opdrachtplanningprogramma (alleen geregistreerd klanten).

Netwerkdiagram

Dit document gebruikt de netwerkinstellingen die in dit diagram worden weergegeven.



Configuraties

Dit document gebruikt deze configuraties:

- 3640-2b "openbare" router
- 3640-6a "Private" router

3640-2b "openbare" 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
```

Verifiëren

Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat uw configuratie correct werkt.

Bepaalde opdrachten met **show worden ondersteund door de tool** Output Interpreter (alleen voor geregistreerde klanten). Hiermee kunt u een analyse van de output van opdrachten met **show genereren.**

Om deze configuratie te verifiëren, probeer een uitgebreid **ping** bevel uit de interface van Ethernet op de privé router 10.103.1.75, voorbestemd aan de Ethernet interface op de openbare router 98.98.98.1

- ping - gebruikt om de basisnetwerkconnectiviteit te diagnosticeren.

```
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
```

- toon crypto ipsec sa-toont de instellingen die door huidige (IPSec) SAs worden gebruikt.
- toon crypto isakmp sa - toont alle huidige IKE SAs bij een peer.
- toont de cryptomotor - toont een samenvatting van de configuratie informatie voor de cryptomotoren. Gebruik de opdracht **goochelmotor** in bevoorrechte EXEC-modus.

Uitvoer voorbeeld

Deze output komt van de **show crypto ipsec als** opdracht uitgegeven op de hub router.

```
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:
```

Deze opdracht toont IPSec SAs die tussen gelijken zijn gebouwd. De versleutelde tunnel is gebouwd tussen 95.95.95.2 en 99.99.99.2 voor verkeer tussen netwerken 98.98.98.0 en 10.103.1.0. Je kunt de twee ingesloten security payload-SA's (ESP) zien die in- en uitgaande zijn gebouwd. Verificatieheader (AH) SA's worden niet gebruikt omdat er geen AH's zijn.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Opdrachten voor troubleshooting

Bepaalde opdrachten met **show worden ondersteund door de tool** Output Interpreter (alleen voor geregistreerde klanten). Hiermee kunt u een analyse van de output van opdrachten met **show genereren.**

Opmerking: Voordat u **debug-**opdrachten afgeeft, raadpleegt u Belangrijke informatie over debug-

opdrachten.

- **debug crypto ipsec sa**-Gebruikt om de IPSec onderhandelingen van fase 2 te zien.
- **debug crypto isakmp sa** — Gebruikt om de ISAKMP onderhandelingen van fase 1 te zien.
- **debug van crypto motor** - gebruikt om de versleutelde sessies weer te geven.

Gerelateerde informatie

- NAT-operatievolgorde
- IP-beveiligingsprobleemoplossing - Oplossingen begrijpen en gebruiken van debug-opdrachten
- IPsec-ondersteuningspagina
- NAT-ondersteuningspagina
- Technische ondersteuning - Cisco-systemen