Router-naar-router dynamisch-naar-statische IPSec configureren met NAT

Inhoud

Inleiding

In deze voorbeeldconfiguratie ontvangt een externe router een IP-adres via een deel van PPP met de naam IP Control Protocol (IPCP). De externe router gebruikt het IP-adres om verbinding te maken met een hubrouter. Deze configuratie maakt het mogelijk dat de hubrouter dynamische IPSec-verbindingen accepteert. De externe router maakt gebruik van Network Address Translation (NAT) om de persoonlijk geadresseerde apparaten erachter aan te sluiten op het persoonlijk geadresseerde netwerk achter de hubrouter. De externe router kent het eindpunt en kan verbindingen met de hubrouter initiëren. Maar de hub router kent het eindpunt niet, zodat kan het geen verbindingen met de verre router in werking stellen.

In dit voorbeeld, dr_whoovie is de externe router en sam-i-am is de hub router. Een toegangslijst specificeert welk verkeer moet worden versleuteld, zodat dr_whoovie weet welk verkeer moet worden versleuteld en waar hetzelfde-i-am eindpunt zich bevindt. De externe router moet de verbinding tot stand brengen. Beide kanten doen NAT-overbelasting.

Voorwaarden

Vereisten

Dit document vereist een basisbegrip van het IPSec-protocol. Als u meer wilt weten over IPSec, raadpleegt u Een inleiding tot IP security (IPSec) encryptie.

Gebruikte componenten

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

- Cisco IOS®-softwarerelease 12.2(24a)XR
- Cisco 2500 Series 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 Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

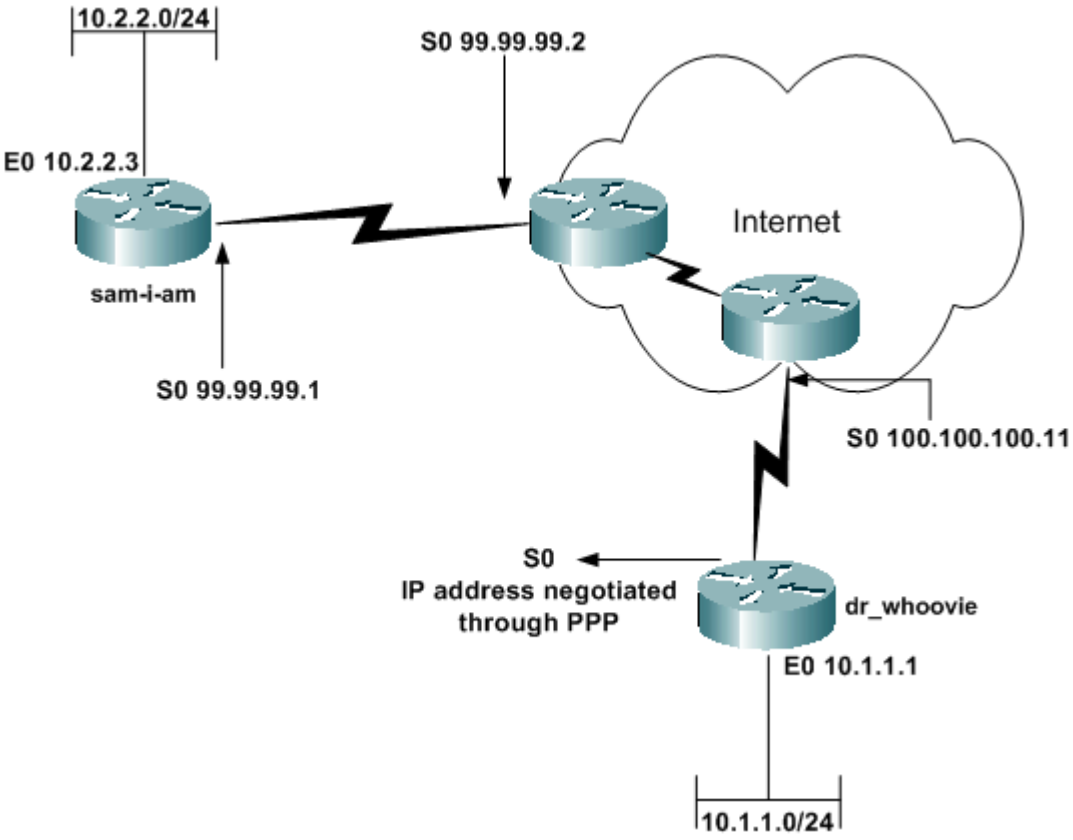
Configureren

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

Opmerking: Gebruik de Command Lookup Tool (alleen voor geregistreerde klanten) voor meer informatie over de opdrachten die in dit document worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Configuraties

Dit document gebruikt de volgende configuraties:

- sam-i-am
- dr_whoovie

```
<#root>

Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log up time
no service password-encryption
!
hostname sam-i-am
!
ip subnet-zero
!

!--- These are the IKE policies.

crypto isakmp policy 1

!--- Defines an Internet Key Exchange (IKE) policy. !--- Use the

crypto isakmp policy

 command !--- in global configuration mode. !--- IKE policies define a set of parameters to be used !--

hash md5
authentication pre-share

!--- Specifies pre-shared keys as the authentication method.

crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0

!--- Configures a pre-shared authentication key, !--- used in global configuration mode.

!

!--- These are the IPSec policies.

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

!--- A transform set is an acceptable combination !--- of security protocols and algorithms. !--- This

crypto dynamic-map rtpmap 10

!--- Use dynamic crypto maps to create policy templates !--- that can be used to process negotiation re

set transform-set rtpset

!--- Configure IPSec to use the transform set "rtpset" !--- that was defined previously.

match address 115
```

```
!--- Assign an extended access list to a crypto map entry !--- that is used by IPSec to determine which

crypto map rtptrans 10 ipsec-isakmp dynamic rtpmap

!--- Specifies that this crypto map entry is to reference !--- a preexisting dynamic crypto map.

!
interface Ethernet0
 ip address 10.2.2.3 255.255.255.0
 no ip directed-broadcast

ip nat inside

 !--- This indicates that the interface is connected to the !--- inside network, which is subject to NA

 no mop enabled
!
interface Serial0
 ip address 99.99.99.1 255.255.255.0
 no ip directed-broadcast

ip nat outside

 !--- This indicates that the interface is connected !--- to the outside network.

crypto map rtptrans

!--- Use the
crypto map
 interface configuration command !--- to apply a previously defined crypto map set to an interface.
!
ip nat inside source route-map nonat interface Serial0 overload

!--- Except the private network from the NAT process.

ip classless
ip route 0.0.0.0 0.0.0.0 Serial0
no ip http server
!
access-list 115 permit ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 115 deny ip 10.2.2.0 0.0.0.255 any

!--- Include the private-network-to-private-network traffic !--- in the encryption process.
```

```
access-list 120 deny ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 120 permit ip 10.2.2.0 0.0.0.255 any


!--- Except the private network from the NAT process.


route-map nonat permit 10
 match ip address 120

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

dr_whoovie

```
<#root>

Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname dr_whoovie
!
ip subnet-zero
!

!--- These are the IKE policies.


crypto isakmp policy 1


!--- Defines an Internet Key Exchange (IKE) policy. !--- Use the

crypto isakmp policy

 command !--- in global configuration mode. !--- IKE policies define a set of parameters to be used !--



hash md5
authentication pre-share


!--- Specifies pre-shared keys as the authentication method.


crypto isakmp key cisco123 address 99.99.99.1
```

```
!--- Configures a pre-shared authentication key, !--- used in global configuration mode.
!
!--- These are the IPSec policies.
crypto ipsec transform-set rtpset esp-des esp-md5-hmac
!--- A transform set is an acceptable combination !--- of security protocols and algorithms. !--- This
!
crypto map rtp 1 ipsec-isakmp
!--- Creates a crypto map and indicates that IKE will be used !--- to establish the IPSec SAs for prote
set peer 99.99.99.1
!--- Use the
set peer
 command to specify an IPSec peer in a crypto map entry.
set transform-set rtpset
!--- Configure IPSec to use the transform set "rtpset" !--- that was defined previously.
match address 115
!--- Include the private-network-to-private-network traffic !--- in the encryption process.
!
interface Ethernet0
ip address 10.1.1.1 255.255.255.0
 no ip directed-broadcast
ip nat inside
 !--- This indicates that the interface is connected to the !--- inside network, which is subject to NA
 no mop enabled
!
interface Serial0
 ip address negotiated
```

```
 !--- Specifies that the IP address for this interface !--- is obtained via PPP/IPCP address negotiatio

 no ip directed-broadcast

ip nat outside

 !--- This indicates that the interface is connected !--- to the outside network.

 encapsulation ppp
 no ip mroute-cache
 no ip route-cache

crypto map rtp

 !--- Use the

crypto map

 interface configuration command !--- to apply a previously defined crypto map set to an interface.

ip nat inside source route-map nonat interface Serial0 overload

!--- Except the private network from the NAT process.

ip classless
ip route 0.0.0.0 0.0.0.0 Serial0
no ip http server
!
access-list 115 permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
access-list 115 deny ip 10.1.1.0 0.0.0.255 any

!--- Include the private-network-to-private-network traffic !--- in the encryption process.

access-list 120 deny   ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
access-list 120 permit ip 10.1.1.0 0.0.0.255 any

!--- Except the private network from the NAT process.

dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
route-map nonat permit 10
 match ip address 120
!
line con 0
 transport input none
line aux 0
line vty 0 4
 password ww
 login
!
end
```

Verifiëren

Deze sectie bevat informatie die u kunt gebruiken om te controleren of 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.**

- **ping** â€"**gebruikt** om basisnetwerkconnectiviteit te diagnosticeren

  Dit voorbeeld laat een ping zien van de 10.1.1.1 Ethernet-interface op dr_whoovie naar de 10.2.2.3 Ethernet-interface op dezelfde server.

  <#root>

  dr_whoovie#

  ping

  ```
  Protocol [ip]:
  Target IP address: 10.2.2.3
  Repeat count [5]:
  Datagram size [100]:
  Timeout in seconds [2]:
  Extended commands [n]: y
  Source address or interface: 10.1.1.1
  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 10.2.2.3,
    timeout is 2 seconds:
  Packet sent with a source address of 10.1.1.1
  !!!!!
  Success rate is 100 percent (5/5),
    round-trip min/avg/max = 36/38/40 ms
  ```

- **toon crypto ipsec sa** â€"Toont de fase 2 security associaties (SA).
- **show crypto isakmp sa** â€"Toont de fase 1 SAs.

voorbeelduitvoer

Deze output is van de **show crypto ipsec als** bevel dat op de hubrouter wordt uitgegeven.

<#root>

sam-i-am#

show crypto ipsec sa

```
interface: Serial0
    Crypto map tag: rtptrans, local addr. 99.99.99.1


local  ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)

   current_peer: 100.100.100.1
     PERMIT, flags={}
    #pkts encaps: 6, #pkts encrypt: 6, #pkts digest 6
    #pkts decaps: 6, #pkts decrypt: 6, #pkts verify 6
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 0, #recv errors 0


local crypto endpt.: 99.99.99.1, remote crypto endpt.: 100.100.100.1

     path mtu 1500, ip mtu 1500, ip mtu interface Serial0
     current outbound spi: 52456533


inbound esp sas:

      spi: 0x6462305C(1684156508)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: rtptrans
        sa timing: remaining key lifetime (k/sec): (4607999/3510)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:


outbound esp sas:

      spi: 0x52456533(1380279603)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: rtptrans
        sa timing: remaining key lifetime (k/sec): (4607999/3510)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:
```

Deze opdracht toont IPSec SAâ€™s die tussen de peer-apparaten zijn gebouwd. De versleutelde tunnel verbindt de interface 100.100.100.1 op dr_whoovie en de interface 99.9.99.1 op sam-i-am. Deze tunnel vervoert verkeer tussen de netten 10.2.2.3 en 10.1.1.1. Twee Encapsulating Security payload (ESP) SAâ€™s zijn inkomende en uitgaande gebouwd. De tunnel wordt gevestigd alhoewel sam-i-am het peer IP adres (100.100.100.1) niet kent. Verificatieheader (AH) SAâ€™s worden niet gebruikt omdat er geen AH

geconfigureerd is.

Deze outputsteekproeven tonen aan dat seriële interface 0 op dr_whoovie een IP adres van 100.100.100.1 door IPCP ontvangt.

- Voordat over het IP-adres wordt onderhandeld:

```
<#root>

dr_whoovie#

show interface serial0

Serial0 is up, line protocol is up
  Hardware is HD64570

Internet address will be negotiated using IPCP

  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
```

- Nadat het IP-adres is bepaald:

```
<#root>

dr_whoovie#

show interface serial0

Serial0 is up, line protocol is up
  Hardware is HD64570

Internet address is 100.100.100.1/32

  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
```

Dit voorbeeld is in een lab ingesteld met de opdracht **peer standaard IP-adres** om een IP-adres toe te wijzen aan het externe uiteinde van de seriële interface met 0 op dr_whoovie. De IP-pool wordt gedefinieerd met de opdracht **lokale ip-pool** aan het externe uiteinde.

Problemen oplossen

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

Opdrachten voor troubleshooting

De Output Interpreter Tool (OIT) (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met **show**. Gebruik de OIT om een analyse te bekijken van de output van de opdracht **show**.

N.B.: Raadpleeg Belangrijke informatie over debug-opdrachten voordat u **debug**-opdrachten gebruikt.

- **debug crypto ipsec** â€”Toont de IPSec onderhandelingen van fase 2.
- **debug crypto isakmp** â€”Toont de Internet Security Association en Key Management Protocol (ISAKMP) onderhandelingen van fase 1.
- **debug crypto engine** â€”Toont het verkeer dat is versleuteld.
- **debug ip NAT gedetailleerd** â€” (Optioneel) verifieert de werking van de NAT-functie door informatie weer te geven over elk pakket dat de router vertaalt.

  Waarschuwing: deze opdracht genereert een grote hoeveelheid uitvoer. Gebruik deze opdracht alleen wanneer het verkeer op het IP-netwerk laag is.
- **clear crypto isakmp** â€”Clears de SA's met betrekking tot fase 1.
- **clear crypto sa** â€”Clears de SA's met betrekking tot fase 2.
- **duidelijke IP NAT-**vertaling: hiermee worden dynamische NAT-vertalingen uit de vertaaltabel gewist.

Gerelateerde informatie

- **Ondersteuning van IPSec-pagina**
- **Technische ondersteuning â€“ Cisco Systems**

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.