IPsec configureren tussen drie routers en privé-adressen

Inhoud

Inleiding

Dit document beschrijft een volledig afgestemde configuratie met drie routers die privé-adressen gebruiken. Het voorbeeld illustreert deze kenmerken:

- Encapsulation Security payload (ESP) - alleen Data Encryption Standard (DES)
- Vooraf gedeelde toetsen
- Private netwerken achter elke router: 192.168.1.0, 192.168.2.0 en 192.168.3.0
- isakmp-beleid en configuratie van cryptografische kaarten
- Tunnelverkeer gedefinieerd met de opdrachten **toegangslijst** en **routekaart**. Naast Port Address Translation (PAT) kunnen routekaarten worden toegepast op een één-op-één statische Network-adresomzetting (NAT) op Cisco IOS®-softwarerelease 12.2(4)T2 en hoger. Raadpleeg voor meer informatie [NAT - mogelijkheid om routekaarten te gebruiken met overzicht van statische omzettingen](#).

Opmerking: Encryptietechnologie is onderworpen aan exportcontroles. Het is uw verantwoordelijkheid om kennis te nemen van de wetgeving inzake de export van encryptietechnologie. Als u vragen hebt over exportcontrole, gelieve een e-mail te sturen naar export@cisco.com.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

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

- Cisco IOS-softwarerelease 12.3(7)T.
- Cisco-routers ingesteld met IPSec.

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.

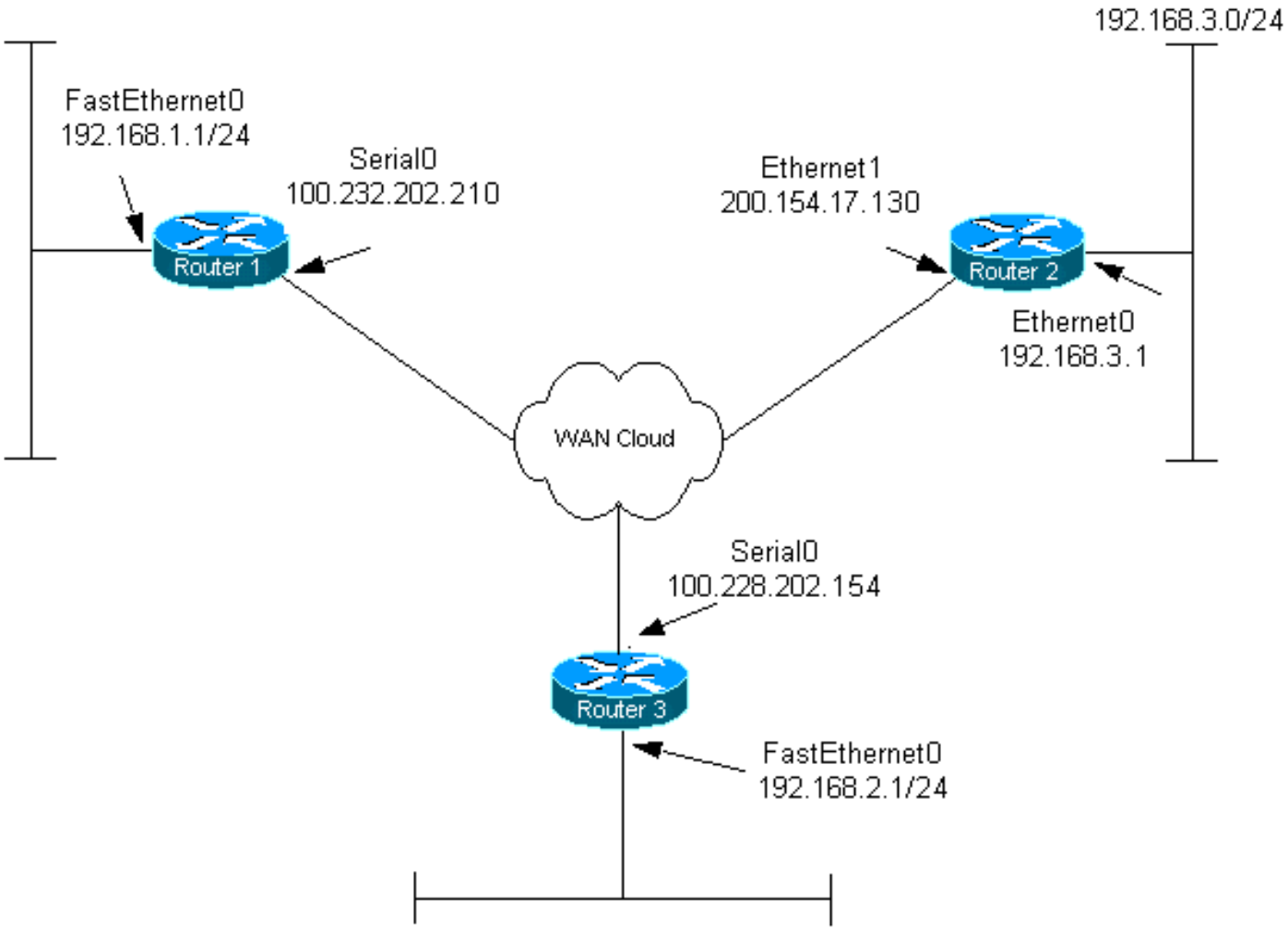
Configureren

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

Het netwerk in dit document is als volgt opgebouwd:



Configuraties

Dit document gebruikt deze configuraties:

- router 1
- router 2
- router 3

router 1

```
Current configuration:
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router1
!
boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
```

```
ip audit po max-events 100
no ftp-server write-enable
!

!--- Configure Internet Key Exchange (IKE) policy and !-
-- pre-shared keys for each peer. !--- IKE policy
defined for peers. crypto isakmp policy 4
authentication pre-share

!--- Pre-shared keys for different peers. crypto isakmp
key xxxxxx1234 address 100.228.202.154
crypto isakmp key xxxxxx1234 address 200.154.17.130
!
!

!--- IPSec policies: crypto ipsec transform-set encrypt-
des esp-des
!
!
crypto map combined local-address Serial0

!--- Set the peer, transform-set and encryption traffic
for tunnel peers. crypto map combined 20 ipsec-isakmp
   set peer 100.228.202.154
   set transform-set encrypt-des
   match address 106
crypto map combined 30 ipsec-isakmp
   set peer 200.154.17.130
   set transform-set encrypt-des
   match address 105
!
!
interface Serial0
   ip address 100.232.202.210 255.255.255.252
   ip nat outside
   serial restart-delay 0

!--- Apply the crypto map to the interface. crypto map
combined
!
interface FastEthernet0
   ip address 192.168.1.1 255.255.255.0
   ip nat inside
!
ip classless
ip route 0.0.0.0 0.0.0.0 100.232.202.209
no ip http server
no ip http secure-server
!

!--- Define traffic for NAT. ip nat inside source route-
map nonat interface Serial0 overload

!--- Access control list (ACL) that shows traffic to
encrypt over the tunnel. access-list 105 permit ip
192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
access-list 106 permit ip 192.168.1.0 0.0.0.255
192.168.2.0 0.0.0.255

!--- ACL to avoid the traffic through NAT over the
tunnel. access-list 150 deny ip 192.168.1.0 0.0.0.255
192.168.2.0 0.0.0.255
access-list 150 deny ip 192.168.1.0 0.0.0.255
192.168.3.0 0.0.0.255
```

```
!--- ACL to perform NAT on the traffic that does not go
over the tunnel. access-list 150 permit ip 192.168.1.0
0.0.0.255 any

!--- Do not perform NAT on the IPSec traffic. route-map
nonat permit 10
  match ip address 150
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
```

router 2

```
Current configuration:
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router2
!
boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!

!--- Configure IKE policy and pre-shared keys for each
peer. !--- IKE policy defined for peers. crypto isakmp
policy 4
    authentication pre-share

!--- Pre-shared keys for different peers. crypto isakmp
key xxxxxx1234 address  100.228.202.154
crypto isakmp key xxxxxx1234 address  100.232.202.210
!
!

!--- IPSec policies. crypto ipsec transform-set encrypt-
des esp-des
!
!
crypto map combined local-address Ethernet1

!--- Set the peer, transform-set and encryption traffic
for tunnel peers. crypto map combined 7 ipsec-isakmp
      set peer 100.232.202.210
```

```
      set transform-set encrypt-des
      match address 105

crypto map combined 8 ipsec-isakmp
      set peer 100.228.202.154
      set transform-set encrypt-des
      match address 106
!
!
!
interface Ethernet0
      ip address 192.168.3.1 255.255.255.0
      ip nat inside
!
interface Ethernet1
      ip address 200.154.17.130 255.255.255.224
      ip nat outside

!--- Apply the crypto map to the interface. crypto map
combined
!
ip classless
ip route 0.0.0.0 0.0.0.0 200.154.17.129
no ip http server
no ip http secure-server
!

!--- Define traffic for NAT. ip nat inside source route-
map nonat interface Ethernet1 overload

!--- ACL shows traffic to encrypt over the tunnel.
access-list 105 permit ip 192.168.3.0 0.0.0.255
192.168.1.0 0.0.0.255
access-list 106 permit ip 192.168.3.0 0.0.0.255
192.168.2.0 0.0.0.255

!--- ACL to avoid the traffic through NAT over the
tunnel. access-list 150 deny ip 192.168.3.0 0.0.0.255
192.168.1.0 0.0.0.255
access-list 150 deny ip 192.168.3.0 0.0.0.255
192.168.2.0 0.0.0.255

!--- ACL to perform NAT on the traffic that does not go
over the tunnel. access-list 150 permit ip any any

!--- Do not perform NAT on the IPSec traffic. route-map
nonat permit 10
  match ip address 150
!
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
```

Configuratie router 3

```
Current configuration:
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router3
!
boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!

!--- Configure IKE policy and pre-shared keys for each
peer. !--- IKE policy defined for peers. crypto isakmp
policy 4
  authentication pre-share


!--- Pre-shared keys for different peers. crypto isakmp
key xxxxxx1234 address 100.232.202.210
crypto isakmp key xxxxxx1234 address 200.154.17.130
!
!

!--- IPSec policies: crypto ipsec transform-set encrypt-
des esp-des
!
!

!--- Set the peer, transform-set and encryption traffic
for tunnel peers. crypto map combined local-address
Serial0
crypto map combined 7 ipsec-isakmp
  set peer 100.232.202.210
  set transform-set encrypt-des
  match address 106
crypto map combined 8 ipsec-isakmp
  set peer 200.154.17.130
  set transform-set encrypt-des
  match address 105
!
!
interface Serial0
  ip address 100.228.202.154 255.255.255.252
  ip nat outside
  serial restart-delay 0

!--- Apply the crypto map to the interface. crypto map
combined
!
  interface FastEthernet0
  ip address 192.168.2.1 255.255.255.0
  ip nat inside
!
```

```
ip classless
ip route 0.0.0.0 0.0.0.0 100.228.202.153
no ip http server
no ip http secure-server
!

!--- Define traffic for NAT. ip nat inside source route-
map nonat interface Serial0 overload

!--- ACL that shows traffic to encrypt over the tunnel.
access-list 105 permit ip 192.168.2.0 0.0.0.255
192.168.3.0 0.0.0.255
access-list 106 permit ip 192.168.2.0 0.0.0.255
192.168.1.0 0.0.0.255

!--- ACL to avoid the traffic through NAT over the
tunnel. access-list 150 deny ip 192.168.2.0 0.0.0.255
192.168.3.0 0.0.0.255
access-list 150 deny ip 192.168.2.0 0.0.0.255
192.168.1.0 0.0.0.255

!--- ACL to perform NAT on the traffic that does not go
over the tunnel. access-list 150 permit ip 192.168.2.0
0.0.0.255 any

!--- Do not perform NAT on the IPSec traffic. route-map
nonat permit 10
  match ip address 150
!
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
 login
!
!
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.**

- **Laat actieve crypto motorverbindingen** zien - toont gecodeerde en gedecrypteerde pakketten tussen IPSec peers.
- **toon crypto isakmp sa**-Toont alle huidige IKE security associaties (SAs) bij een peer.
- **toon crypto ipsec sa**-Toont de instellingen die worden gebruikt door huidige (IPSec) SA's.

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.

Opmerking: de volgende apparaten moeten op beide IPSec-routers (peers) worden uitgevoerd. Schoonmaken van SA's moet op beide peers gebeuren.

- **debug van crypto isakmp**-displays tijdens fase 1.
- **debug van crypto ipsec**-displays tijdens fase 2.
- **debug van crypto motor**—informatie van de crypto motor.
- **duidelijke crypto-verbinding** ***verbinding-id [sleuf]*** | *rsm* | *vip]* —Hiermee wordt een versleutelde sessie beëindigd die momenteel wordt uitgevoerd. Versleutelde sessies eindigen normaal als de sessie voorbij is. Gebruik de opdracht **cisco-verbindingen van de show** om de verbinding-id waarde te leren.
- **duidelijke crypto isakmp** - ontruimt de fase 1 SA's.
- **duidelijke crypto sa** — ontruimt de fase 2 SA's.

Gerelateerde informatie

- IPsec-ondersteuningspagina
- Technische ondersteuning - Cisco-systemen