

IPsec configureren - Cisco beveiligde VPN-client voor Central Router Control Access

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Opdrachten voor troubleshooting](#)

[Gerelateerde informatie](#)

[Inleiding](#)

De volgende configuratie zou niet veel gebruikt worden, maar was ontworpen om Cisco Secure VPN-client IPSec-tunnelbeëindiging op een centrale router toe te staan. Aangezien de tunnel omhoog komt, ontvangt de PC zijn IP adres van de het IP adrespool van de centrale router (in ons voorbeeld wordt de router "moss" genoemd), dan kan het poolverkeer het lokale netwerk achter de moss bereiken of worden routed en gecodeerd naar het netwerk achter de uitgaande router (in ons voorbeeld wordt de router "carter" genoemd). Bovendien wordt het verkeer van het particuliere netwerk 10.13.1.X tot en met 10.1.1.X versleuteld. de routers maken NAT-overbelasting.

[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-software-release 12.1.5.T (c3640-io3s56i-mz.121-5.T)
- Cisco Secure VPN-client 12.1

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](#).

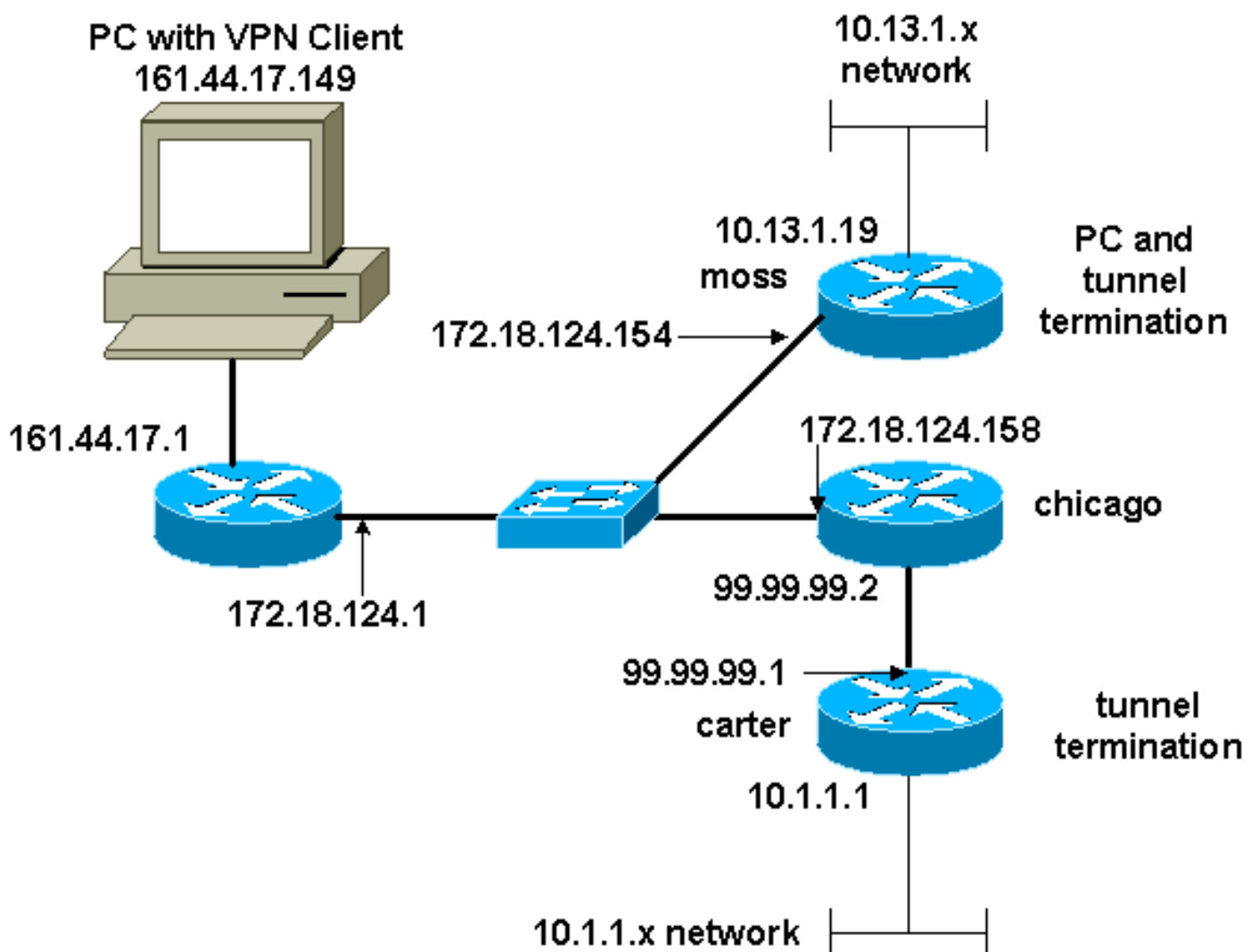
Configureren

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).

Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:



Configuraties

Dit document gebruikt deze configuraties:

- [MOS-configuratie](#)
- [carter-configuratie](#)

MOS-configuratie

```
Version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname moss
!
logging rate-limit console 10 except errors
enable password ww
!
ip subnet-zero
!
no ip finger
!
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key cisco123 address 99.99.99.1
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
crypto isakmp client configuration address-pool local
RTP-POOL
!
crypto ipsec transform-set rtpset esp-des esp-md5-hmac
!
crypto dynamic-map rtp-dynamic 20
set transform-set rtpset
!
crypto map rtp client configuration address initiate
crypto map rtp client configuration address respond
!crypto map sequence for network to network traffic
crypto map rtp 1 ipsec-isakmp
set peer 99.99.99.1
set transform-set rtpset
match address 115
!!--- crypto map sequence for VPN Client network traffic.
crypto map rtp 10 ipsec-isakmp dynamic rtp-dynamic
!
call rsvp-sync
!
interface Ethernet2/0
ip address 172.18.124.154 255.255.255.0
ip nat outside
no ip route-cache
no ip mroute-cache
half-duplex
crypto map rtp
!
interface Serial2/0
no ip address
shutdown
```

```

!
interface Ethernet2/1
ip address 10.13.1.19 255.255.255.0
ip nat inside
half-duplex
!
ip local pool RTP-POOL 192.168.1.1 192.168.1.254
ip nat pool ETH20 172.18.124.154 172.18.124.154 netmask
255.255.255.0
ip nat inside source route-map nonat pool ETH20 overload
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.1
ip route 10.1.1.0 255.255.255.0 172.18.124.158
ip route 99.99.99.0 255.255.255.0 172.18.124.158
no ip http server
!
!--- Exclude traffic from NAT process. access-list 110
deny ip 10.13.1.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 110 deny ip 10.13.1.0 0.0.0.255 192.168.1.0
0.0.0.255
access-list 110 permit ip 10.13.1.0 0.0.0.255 any
!--- Include traffic in encryption process. access-list
115 permit ip 10.13.1.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 115 permit ip 192.168.1.0 0.0.0.255 10.1.1.0
0.0.0.255
route-map nonat permit 10
match ip address 110
!
dial-peer cor custom
!
line con 0
transport input none
line aux 0
line vty 0 4
login
!
end

```

carter-configuratie

```

Current configuration : 2059 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname carter
!
logging rate-limit console 10 except errors
!
ip subnet-zero
!
no ip finger
!
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key cisco123 address 172.18.124.154

```

```

!
crypto ipsec transform-set rtpset esp-des esp-md5-hmac
!
!--- crypto map sequence for network-to-network traffic.
crypto map rtp 1 ipsec-isakmp
set peer 172.18.124.154
set transform-set rtpset
match address 115
!
call rsvp-sync
!
interface Ethernet0/0
ip address 99.99.99.1 255.255.255.0
ip nat outside
half-duplex
crypto map rtp
!
interface FastEthernet3/0
ip address 10.1.1.1 255.255.255.0
ip nat inside
duplex auto
speed 10
!
ip nat pool ETH00 99.99.99.1 99.99.99.1 netmask
255.255.255.0
ip nat inside source route-map nonat pool ETH00 overload
ip classless
ip route 0.0.0.0 0.0.0.0 99.99.99.2
no ip http server
!
!--- Exclude traffic from NAT process. access-list 110
deny ip 10.1.1.0 0.0.0.255 10.13.1.0 0.0.0.255
access-list 110 deny ip 10.1.1.0 0.0.0.255 192.168.1.0
0.0.0.255
access-list 110 permit ip 10.1.1.0 0.0.0.255 any
!--- Include traffic in encryption process. access-list
115 permit ip 10.1.1.0 0.0.0.255 10.13.1.0 0.0.0.255
access-list 115 permit ip 10.1.1.0 0.0.0.255 192.168.1.0
0.0.0.255
route-map nonat permit 10
match ip address 110
!
line con 0
transport input none
line aux 0
line vty 0 4
password ww
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.

- `toon crypto ipsec sa` - shows the fase 2 security associaties.
- `toon crypto isakmp sa` - toont de fase 1 veiligheidsassociaties.

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 Commands](#).

- `debug crypto ipsec` — toont de IPSec onderhandelingen van fase 2.
- `debug crypto isakmp` — toont de ISAKMP-onderhandelingen over fase 1.
- `debug crypto motor` - toont het verkeer dat wordt versleuteld.
- `duidelijke crypto isakmp` — ontslaat de veiligheidsassociaties met betrekking tot fase 1.
- `duidelijke crypto sa` — ontruimt de veiligheidsassociaties met betrekking tot fase 2.

Gerelateerde informatie

- [IPsec-netwerkbeveiliging configureren](#)
- [Het configureren van Internet Key Exchange-beveiligingsprotocol](#)
- [Cisco VPN-clientondersteuningspagina](#)
- [IPsec-ondersteuningspagina](#)
- [Technische ondersteuning - Cisco-systemen](#)