Verificatie via automatische proxy met IPsec en VPN-clientconfiguratie met NAT en Cisco IOS-firewall

Inhoud

Inleiding

Deze voorbeeldconfiguratie maakt het mogelijk dat een VPN-client toegang heeft tot een server op een ander netwerk via een IPsec-tunnel nadat de gebruikersverificatie heeft plaatsgevonden.

Een PC op 99.99.99.5 brengt het web browser op om toegang tot inhoud op de server te krijgen op 10.13.1.98. Aangezien de VPN-client op de PC is ingesteld om door tunneleindpunt 99.99.99.1 te gaan naar het 10.13.1.x-netwerk, wordt de IPsec-tunnel gebouwd en de PC IP-adres uit de pool "ourpool" genoemd (omdat u mode-configuratie doet). De 3640 router vraagt om authenticatie. Nadat de gebruiker een gebruikersnaam en wachtwoord heeft ingevoerd (opgeslagen op de TACACS+ server op 172.18.124.97) wordt de toegangslijst die van de server is doorgegeven toegevoegd aan toegangslijst 117.

Opmerking: De **ip-auth-proxy** opdracht is geïntroduceerd in Cisco IOS® Software release 12.0.5.T.

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 12.0.7.T
- Cisco 3640 router (c3640-jo3s56i-mz.121-2.3.T)
- Cisco Secure VPN-client 1.0 (weergegeven als 2.0.7 in het menu IRE client Help > Info) of Cisco Secure VPN-client 1.1 (weergegeven als 2.1.12 in het menu IRE client Help > Info)

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 de Cisco Technical Tips Convention voor meer informatie over documentconventies.

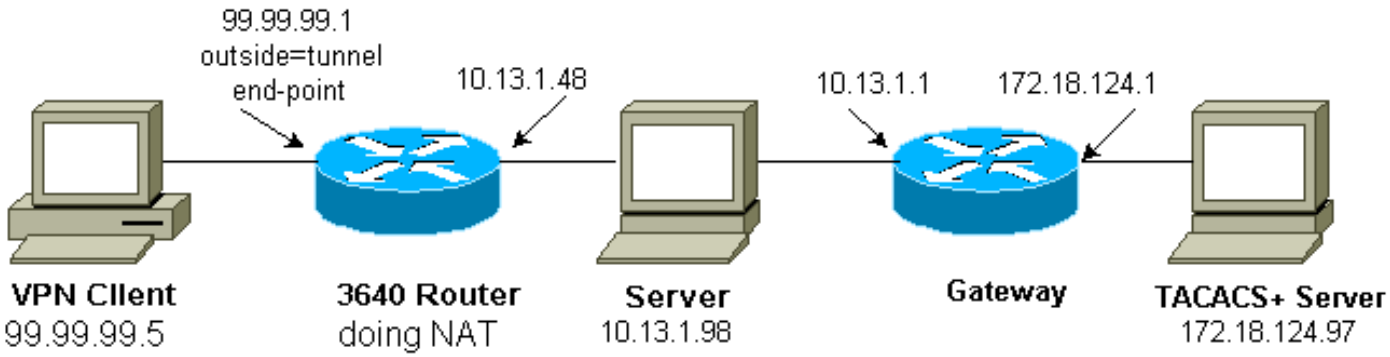
Configureren

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

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Configuraties

Dit document gebruikt deze configuratie:

Cisco 3640 routerconfiguratie

```
Current configuration:
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname carter
```

```
!
aaa new-model
aaa authentication login default group tacacs+ none
aaa authorization exec default group tacacs+ none
aaa authorization auth-proxy default group tacacs+
enable secret 5 $1$cSvL$F6VxA7kBFAGHvhBbRlNS20
enable password ww
!
ip subnet-zero
!
ip inspect name myfw cuseeme timeout 3600
ip inspect name myfw ftp timeout 3600
ip inspect name myfw http timeout 3600
ip inspect name myfw rcmd timeout 3600
ip inspect name myfw realaudio timeout 3600
ip inspect name myfw smtp timeout 3600
ip inspect name myfw sqlnet timeout 3600
ip inspect name myfw streamworks timeout 3600
ip inspect name myfw tftp timeout 30
ip inspect name myfw udp timeout 15
ip inspect name myfw tcp timeout 3600
ip inspect name myfw vdolive
ip auth-proxy auth-proxy-banner
ip auth-proxy auth-cache-time 10
ip auth-proxy name list_a http
ip audit notify log
ip audit po max-events 100
cns event-service server
!
crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key cisco1234 address 0.0.0.0 0.0.0.0
crypto isakmp client configuration address-pool local
ourpool
!
crypto ipsec transform-set mypolicy esp-des esp-md5-hmac
!
crypto dynamic-map dyna 10
set transform-set mypolicy
!
crypto map test client configuration address initiate
crypto map test client configuration address respond
crypto map test 5 ipsec-isakmp dynamic dyna
!
interface Loopback0
ip address 1.1.1.1 255.255.255.0
!
interface Ethernet0/0
ip address 10.13.1.48 255.255.255.0
ip nat inside
ip inspect myfw in
ip route-cache policy
no ip mroute-cache
ip policy route-map nonat
no mop enabled
!
interface TokenRing0/0
no ip address
shutdown
ring-speed 16
!
interface Ethernet2/0
ip address 99.99.99.1 255.255.255.0
```

```
ip access-group 117 in
ip nat outside
ip auth-proxy list_a
no ip route-cache
no ip mroute-cache
no mop enabled
crypto map test
!
interface TokenRing2/0
no ip address
shutdown
ring-speed 16
!
ip local pool ourpool 10.2.1.1 10.2.1.254
ip nat pool outsidepool 99.99.99.50 99.99.99.60 netmask
255.255.255.0
ip nat inside source route-map rmap pool outsidepool
ip classless
ip route 0.0.0.0 0.0.0.0 99.99.99.20
ip route 172.18.124.0 255.255.255.0 10.13.1.1
no ip http server
!
access-list 110 deny ip 10.13.1.0 0.0.0.255 10.2.1.0
0.0.0.255
access-list 110 permit ip 10.13.1.0 0.0.0.255 any
access-list 117 permit esp any any
access-list 117 permit udp any any eq isakmp
access-list 120 permit ip 10.13.1.0 0.0.0.255 10.2.1.0
0.0.0.255
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
route-map rmap permit 10
match ip address 110
!
route-map nonat permit 10
match ip address 120
set ip next-hop 1.1.1.2
!
route-map nonat permit 20
!
tacacs-server host 172.18.124.97
tacacs-server key cisco
!
line con 0
transport input none
line aux 0
line vty 0 4
password ww
!
end
```

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Raadpleeg de verificatieproxy voor probleemoplossing voor informatie over probleemoplossing.

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug**-opdrachten gebruikt.

Gerelateerde informatie

- Cisco VPN-client
- IPsec-onderhandeling/IKE-protocollen
- Cisco IOS-firewalltechnische ondersteuning
- Technische ondersteuning en documentatie – Cisco Systems