# NAT 및 정적으로 라우터 IPsec 터널 전용-개인 네트워크 구성

## 목차



## 소개

이 샘플 컨피그레이션에서는 다음을 수행하는 방법을 보여 줍니다.

- 두 프라이빗 네트워크(10.1.1.x 및 172.16.1.x) 간 트래픽을 암호화합니다.
- 네트워크 디바이스에 고정 IP 주소(외부 주소 200.1.1.25)을 10.1.1.3.

ACL(Access Control List)을 사용하여 라우터에 NAT(Network Address Translation)를 프라이빗-프라이빗 네트워크 트래픽에 수행하지 않도록 지시합니다. 그러면 라우터를 떠날 때 이 트래픽이 암호화되어 터널에 배치됩니다.이 샘플 컨피그레이션에서는 10.1.1.x 네트워크의 내부 서버에 대한 고정 NAT도 있습니다.이 샘플 컨피그레이션에서는 NAT 명령에서 route-map 옵션을 사용하여 해당 트래픽이 암호화된 터널을 통해 전송될 경우 NAT가 되는 것을 방지합니다.

## 사전 요구 사항

### 요구 사항

이 문서에 대한 특정 요건이 없습니다.

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® 소프트웨어 릴리스 12.3(14)T
- Cisco 라우터 2개

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

# ACL의 Deny Statement에서 NAT 트래픽을 지정하는 이유는 무엇입니까?

Cisco IOS IPsec 또는 VPN을 사용할 때 네트워크를 터널로 대체하는 개념적인 방법입니다.이 다이어그램에서 200.1.1.1에서 100.1.1.1으로 이동하는 Cisco IOS IPsec 터널로 인터넷 클라우드를 대체합니다.터널을 통해 함께 연결된 두 개의 전용 LAN의 관점에서 이 네트워크를 투명하게 만듭니다.이러한 이유로 인해 하나의 프라이빗 LAN에서 원격 전용 LAN으로 이동하는 트래픽에 NAT를 사용하지 않으려는 경우가 많습니다.패킷이 내부 라우터 3 네트워크에 도달할 때 200.1.1.1 대신 10.1.1.0/24 네트워크에서 소스 IP 주소를 사용하여 라우터 2 네트워크에서 오는 패킷을 확인할 수 있습니다.

NAT 구성 방법에 대한 자세한 내용은 NAT Order of Operation을 참조하십시오.이 문서에서는 패킷이 내부에서 외부로 이동하는 경우 암호화 검사 전에 NAT가 발생함을 보여줍니다.따라서 컨피그레이션에서 이 정보를 지정해야 합니다.

```
ip nat inside source list 122 interface Ethernet0/1 overload
```

```
access-list 122 deny ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
access-list 122 permit ip 10.1.1.0 0.0.0.255 any
```

**참고:** 터널을 구축하고 NAT를 계속 사용할 수도 있습니다.이 시나리오에서 NAT 트래픽을 "IPsec에 대한 흥미로운 트래픽"(이 문서의 다른 섹션에서 ACL 101이라고 함)으로 지정합니다.NAT가 활성 상태일 때 터널을 구축하는 방법에 대한 자세한 내용은 중복 LAN 서브넷이 있는 라우터 간 IPsec 터널 구성을 참조하십시오.

# 고정 NAT는 어떻습니까? IPsec 터널을 통해 해당 주소로 이동할 수 없는 이유는 무엇입니까?

이 설정에는 10.1.1.3의 서버에 대한 고정 일대일 NAT도 포함되어 있습니다. 이는 인터넷 사용자가 액세스할 수 있도록 200.1.1.25 NAT입니다.다음 명령을 실행합니다.

```
ip nat inside source static 10.1.1.3 200.1.1.25
```

이 고정 NAT는 172.16.1.x 네트워크의 사용자가 암호화된 터널을 통해 10.1.1.3에 도달하는 것을

차단합니다.이는 암호화된 트래픽이 ACL 122에서 NAT가 되는 것을 거부해야 하기 때문입니다. 그러나 static NAT 명령은 10.1.1.3와의 모든 연결에 대해 일반 NAT 문보다 우선합니다. static NAT 문은 암호화된 트래픽도 NAT가 되는 것을 특별히 거부하지 않습니다.10.1.1.3의 회신은 172.16.1.x 네트워크의 사용자가 10.1.1.3에 연결할 때 200.1.1.25에 대한 NAT이므로 암호화된 터널을 다시 거치지 않습니다(암호화 전에 NAT가 발생).

고정 NAT 문에서 route-map 명령을 사용하여 암호화된 트래픽이 NAT(정적으로 1대1 NAT도)가 되지 않도록 거부해야 합니다.

**참고:** 고정 NAT의 **route-map** 옵션은 Cisco IOS Software Release 12.2(4)T 이상에서만 지원됩니다.자세한 내용은 NAT - Capacity to Use Route Maps with Static Translations(고정 변환과 함께 경로 맵 사용 기능)를 참조하십시오.

고정 NAT 호스트 10.1.1.3에 대한 암호화된 액세스를 허용하려면 다음 추가 명령을 실행해야 합니다.

```
ip nat inside source static 10.1.1.3 200.1.1.25 route-map nonat
!
access-list 150 deny   ip host 10.1.1.3 172.16.1.0 0.0.0.255
access-list 150 permit ip host 10.1.1.3 any
!
route-map nonat permit 10
 match ip address 150
```

이러한 명령문은 라우터에 ACL 150과 일치하는 트래픽에만 고정 NAT를 적용하도록 지시합니다. ACL 150은 10.1.1.3에서 소싱되고 암호화된 터널을 통해 172.16.1.x로 향하는 트래픽에 NAT를 적용하지 않도록 합니다.그러나 10.1.1.3에서 제공하는 다른 모든 트래픽(인터넷 기반 트래픽)에 적용합니다.

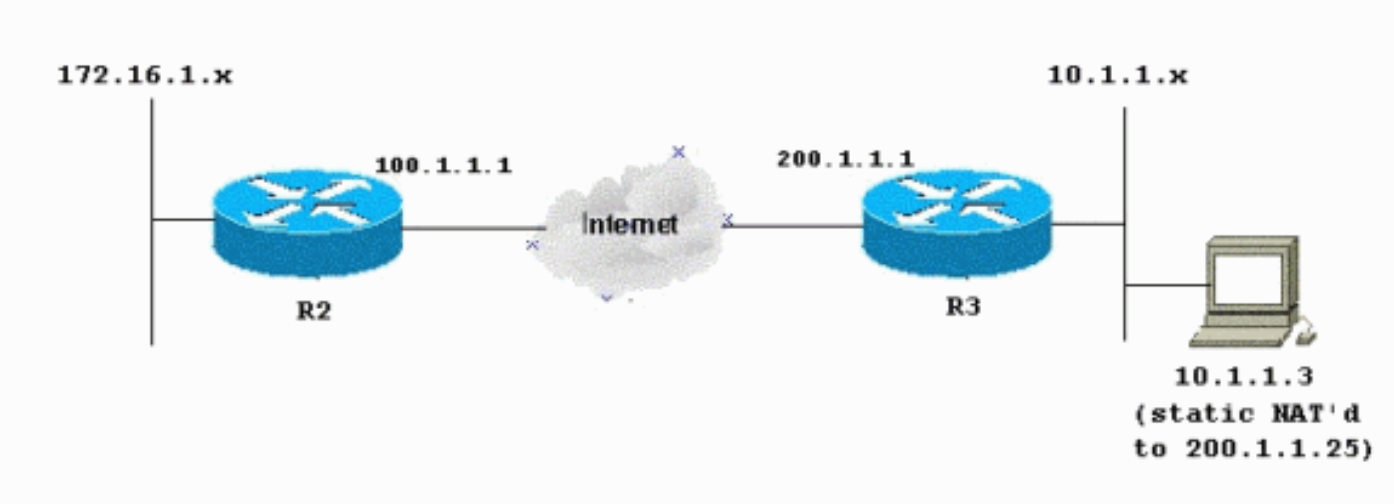
# 구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

**참고:** 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 문서에 사용된 명령에 대한 자세한 내용을 확인하십시오.

## 네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.




## 구성

이 문서에서는 다음 구성을 사용합니다.

- 라우터 2
- 라우터 3

**R2 - 라우터 컨피그레이션**

```
R2#write terminal
Building configuration...
Current configuration : 1412 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
!
!
crypto isakmp policy 10
 authentication pre-share
!
crypto isakmp key ciscokey address 200.1.1.1
!
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
crypto map myvpn 10 ipsec-isakmp
 set peer 200.1.1.1
 set transform-set myset
```

```
!--- Include the private-network-to-private-network
traffic !--- in the encryption process: match address
101
!
!
!
interface Ethernet0/0
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface Ethernet1/0
 ip address 100.1.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 crypto map myvpn
!
ip classless
ip route 0.0.0.0 0.0.0.0 100.1.1.254
!
ip http server
no ip http secure-server
!
!--- Except the private network from the NAT process: ip
nat inside source list 175 interface Ethernet1/0
overload
!
!--- Include the private-network-to-private-network
traffic !--- in the encryption process: access-list 101
permit ip 172.16.1.0 0.0.0.255 10.1.1.0 0.0.0.255
!--- Except the private network from the NAT process:
access-list 175 deny   ip 172.16.1.0 0.0.0.255 10.1.1.0
0.0.0.255
access-list 175 permit ip 172.16.1.0 0.0.0.255 any
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

## R3 - 라우터 컨피그레이션

```
R3#write terminal
Building configuration...
Current configuration : 1630 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
```

```
!
!
no aaa new-model
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
!
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key ciscokey address 100.1.1.1
!
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
crypto map myvpn 10 ipsec-isakmp
 set peer 100.1.1.1
 set transform-set myset
!--- Include the private-network-to-private-network
traffic !--- in the encryption process: match address
101
!
!
!
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface Ethernet1/0
 ip address 200.1.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 crypto map myvpn
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 200.1.1.254
!
no ip http server
no ip http secure-server
!
!--- Except the private network from the NAT process: ip
nat inside source list 122 interface Ethernet1/0
overload
!--- Except the static-NAT traffic from the NAT process
if destined !--- over the encrypted tunnel: ip nat
inside source static 10.1.1.3 200.1.1.25 route-map nonat
!
access-list 101 permit ip 10.1.1.0 0.0.0.255 172.16.1.0
0.0.0.255
!--- Except the private network from the NAT process:
access-list 122 deny   ip 10.1.1.0 0.0.0.255 172.16.1.0
0.0.0.255
access-list 122 permit ip 10.1.1.0 0.0.0.255 any
!--- Except the static-NAT traffic from the NAT process
if destined !--- over the encrypted tunnel: access-list
150 deny   ip host 10.1.1.3 172.16.1.0 0.0.0.255
access-list 150 permit ip host 10.1.1.3 any
!
route-map nonat permit 10
 match ip address 150
```

```
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

# 다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

# 문제 해결

이 섹션에서는 컨피그레이션 문제를 해결할 수 있습니다.

자세한 내용은 IP 보안 문제 해결 - 디버그 명령 이해 및 사용을 참조하십시오.

## 문제 해결 명령

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

**참고:** debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **debug crypto ipsec sa** —2단계의 IPsec 협상을 표시합니다.
- **debug crypto isakmp sa** —1단계의 ISAKMP 협상을 참조하십시오.
- **debug crypto engine** —암호화된 세션을 표시합니다.

# 관련 정보

- **IPsec 협상/IKE 프로토콜 - Cisco Systems**
- **기술 지원 및 문서 – Cisco Systems**