

중복 LAN 서브넷을 사용하여 라우터 간 IPSec 터널 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[배경 정보](#)

[구성](#)

[네트워크 다이어그램](#)

[구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[문제 해결 명령](#)

[관련 정보](#)

소개

이 문서에서는 동일한 IP 주소 지정 체계를 사용하여 두 개의 병합 회사를 시뮬레이션하는 네트워킹 예제를 제공합니다. 두 라우터는 VPN 터널에 연결되고 각 라우터 뒤의 네트워크는 동일합니다. 한 사이트가 다른 사이트의 호스트에 액세스하기 위해 라우터에서 NAT(Network Address Translation)를 사용하여 소스 주소와 대상 주소를 서로 다른 서브넷으로 변경합니다.

참고: 이 구성은 네트워크 관리 측면에서 혼동될 수 있으므로 영구 설정으로 권장되지 않습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 라우터 A: Cisco IOS® Software 릴리스 12.3(4)T를 실행하는 Cisco 3640 라우터
- 라우터 B: Cisco IOS® 소프트웨어 릴리스 12.3(5)을 실행하는 Cisco 2621 라우터

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 표기 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙을 참조하십시오](#).

[배경 정보](#)

이 예에서는 사이트 A의 호스트 172.16.1.2이 사이트 B의 동일한 IP 주소 호스트를 액세스할 때 실제 172.16.1.2 주소가 아닌 172.19.1.2 주소에 연결됩니다. 사이트 B의 호스트가 사이트 A에 액세스하면 172.18.1.2 주소에 연결됩니다. 라우터 A의 NAT는 모든 172.16.x.x 주소를 일치하는 172.18.x.x 호스트 항목처럼 변환합니다. 라우터 B의 NAT는 172.16.x.x를 172.19.x.x처럼 변경합니다.

각 라우터의 암호화 기능은 시리얼 인터페이스 전체에서 변환된 트래픽을 암호화합니다. NAT는 라우터에서 암호화하기 전에 발생합니다.

참고: 이 컨피그레이션에서는 두 네트워크만 통신할 수 있습니다. 인터넷 연결을 허용하지 않습니다. 두 사이트가 아닌 다른 위치로의 연결을 위해 인터넷에 대한 추가 경로가 필요합니다. 즉, 호스트에 여러 경로가 구성된 경우 각 면에 다른 라우터 또는 방화벽을 추가해야 합니다.

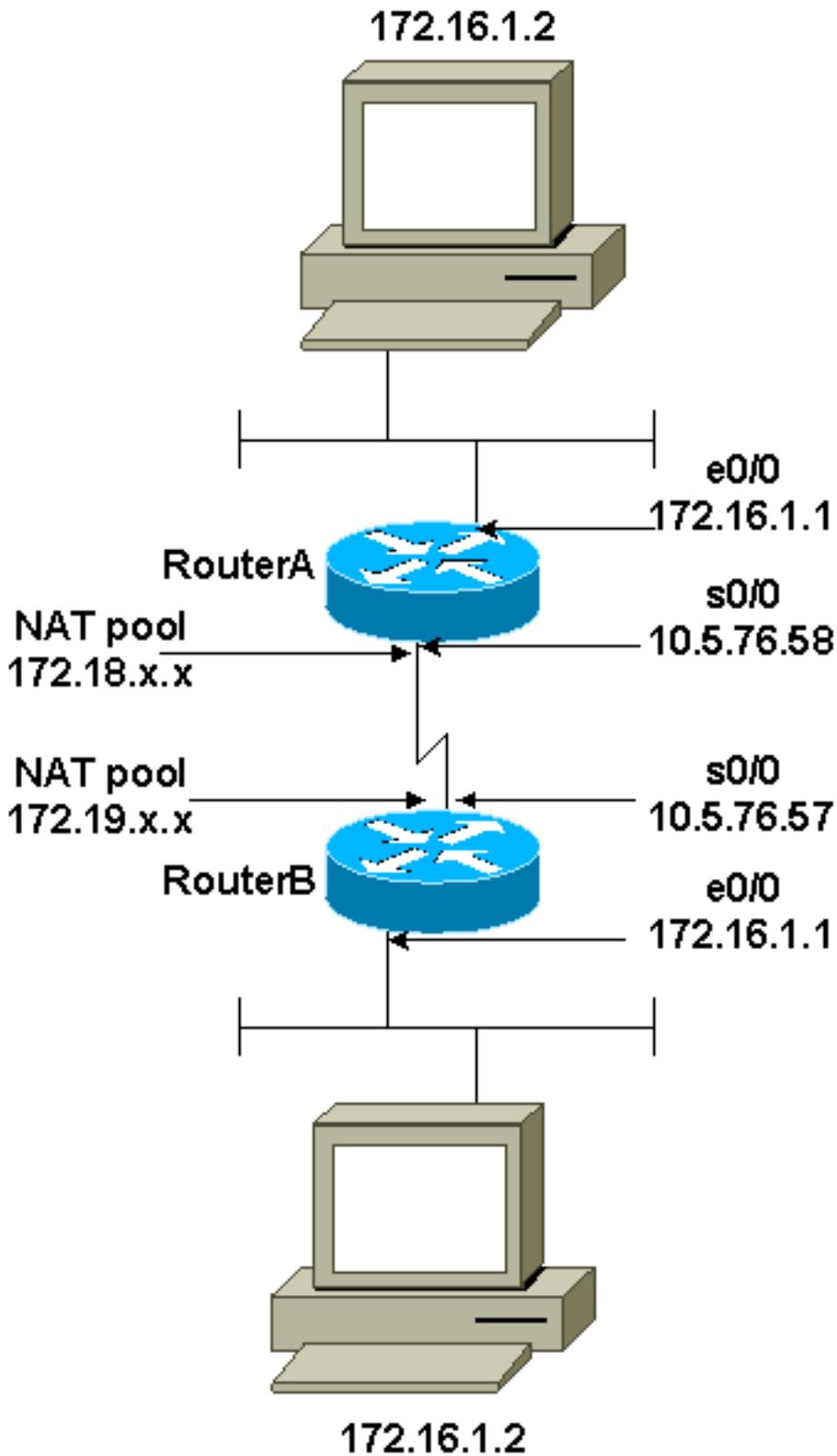
[구성](#)

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 이 문서에 사용된 명령에 대한 추가 정보를 찾으려면 [명령 조회 도구](#)([등록된](#) 고객만 해당)를 사용합니다.

[네트워크 다이어그램](#)

이 문서에서는 다음 네트워크 설정을 사용합니다.



구성

이 문서에서는 다음 구성을 사용합니다.

- [라우터 A](#)
- [라우터 B](#)

라우터 A

```
Current configuration : 1404 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SV3-2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
!
!
!
ip audit notify log
ip audit po max-events 100
ip ssh break-string
no ftp-server write-enable
!
!
!--- These are the Internet Key Exchange (IKE)
parameters. crypto isakmp policy 10
  encr 3des
  hash md5
  authentication pre-share
crypto isakmp key cisco123 address 10.5.76.57
!
!--- These are the IPSec parameters. crypto ipsec
transform-set myset1 esp-3des esp-md5-hmac
!
!
crypto map mymap 10 ipsec-isakmp
  set peer 10.5.76.57
  set transform-set myset1
  !--- Encrypt traffic to the other side. match address
100
!
!
!
interface Serial0/0
  description Interface to Internet
  ip address 10.5.76.58 255.255.0.0
  ip nat outside
  clockrate 128000
  crypto map mymap
!
interface Ethernet0/0
  ip address 172.16.1.1 255.255.255.0
  no ip directed-broadcast
  ip nat inside
  half-duplex
!
!
!--- This is the NAT traffic. ip nat inside source
static network 172.16.0.0 172.18.0.0 /16 no-alias
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0
```

```
!  
!--- Encrypt traffic to the other side. access-list 100  
permit ip 172.18.0.0 0.0.255.255 172.19.0.0 0.0.255.255  
!  
control-plane  
!  
!  
line con 0  
line aux 0  
line vty 0 4  
!  
!  
end
```

라우터 B

```
Current configuration : 1255 bytes  
!  
version 12.3  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname SV3-15  
!  
boot-start-marker  
boot-end-marker  
!  
!  
memory-size iomem 15  
no aaa new-model  
ip subnet-zero  
!  
!  
!  
ip audit notify log  
ip audit po max-events 100  
!  
!--- These are the IKE parameters. crypto isakmp policy  
10  
  encr 3des  
  hash md5  
  authentication pre-share  
crypto isakmp key cisco123 address 10.5.76.58  
!  
!--- These are the IPSec parameters. crypto ipsec  
transform-set myset1 esp-3des esp-md5-hmac  
!  
crypto map mymap 10 ipsec-isakmp  
  set peer 10.5.76.58  
  set transform-set myset1  
!--- Encrypt traffic to the other side. match address  
100  
!  
!  
interface FastEthernet0/0  
  ip address 172.16.1.1 255.255.255.0  
  ip nat inside  
  duplex auto  
  speed auto  
!  
interface Serial0/0  
  description Interface to Internet
```

```
ip address 10.5.76.57 255.255.0.0
ip nat outside
crypto map mymap
!
!--- This is the NAT traffic. ip nat inside source
static network 172.16.0.0 172.19.0.0 /16 no-alias
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0
!
!--- Encrypt traffic to the other side. access-list 100
permit ip 172.19.0.0 0.0.255.255 172.18.0.0 0.0.255.255
!
!
line con 0
line aux 0
line vty 0 4
!
!
!
end
```

다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

일부 **show** 명령은 [출력 인터프리터 툴](#) 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show** 명령 출력의 분석 결과를 볼 수 있습니다.

- **show crypto ipsec sa** - 2단계 보안 연결을 표시합니다.
- **show crypto isakmp sa** - 1단계 보안 연결을 표시합니다.
- **show ip nat translation** - 사용 중인 현재 NAT 변환을 표시합니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

문제 해결 명령

일부 **show** 명령은 [출력 인터프리터 툴](#) 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show** 명령 출력의 분석 결과를 볼 수 있습니다.

참고: debug 명령을 실행하기 전에 [디버그 명령에 대한 중요 정보를 참조하십시오.](#)

- **debug crypto ipsec** - 2단계의 IPSec 협상을 표시합니다.
- **debug crypto isakmp** - 1단계의 ISAKMP(Internet Security Association and Key Management Protocol) 협상을 표시합니다.
- **debug crypto engine** - 암호화된 트래픽을 표시합니다.

관련 정보

- [IPSec 지원 페이지](#)
- [IPSec 네트워크 보안 구성](#)
- [인터넷 키 교환 보안 프로토콜 구성](#)
- [Technical Support - Cisco Systems](#)