

프라이빗 네트워크 간 IPSec 라우터 간, 사전 공유, NAT 오버로드 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[구성](#)

[네트워크 다이어그램](#)

[구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[문제 해결 명령](#)

[관련 정보](#)

소개

이 샘플 컨피그레이션에서는 IPSec을 사용하여 두 프라이빗 네트워크(10.50.50.x 및 10.103.1.x) 간 트래픽을 암호화하는 방법을 보여줍니다.네트워크는 개인 주소를 통해 서로를 알고 있습니다.

[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 12.3.1a
- Cisco 2691 Router

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](#).

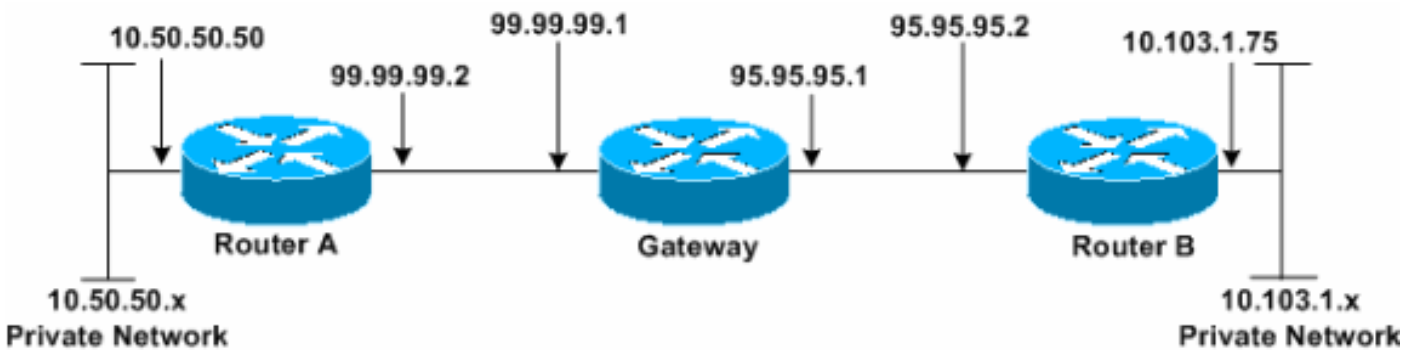
구성

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 이 다이어그램에 표시된 네트워크 설정을 사용합니다.



구성

이 문서에서는 이러한 구성을 사용합니다.

- [라우터 A](#)
- [라우터 B](#)

라우터 A

```
Router_A#write terminal
Building configuration...
Current configuration : 1638 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router_A
!
boot system flash:c2691-ik9o3s-mz.123-1a.bin
!
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
no ftp-server write-enable
!
crypto isakmp policy 1
hash md5
authentication pre-share
```

```

crypto isakmp key cisco123 address 95.95.95.2
!
crypto ipsec transform-set rtpset esp-des esp-md5-hmac
!
crypto map rtp 1 ipsec-isakmp
set peer 95.95.95.2
set transform-set rtpset
!--- Include the private network to private network
traffic !--- in the encryption process. match address
115
!
no voice hpi capture buffer
no voice hpi capture destination
!
interface FastEthernet0/0
ip address 99.99.99.2 255.255.255.0
ip nat outside
duplex auto
speed auto
crypto map rtp
!
interface FastEthernet0/1
ip address 10.50.50.50 255.255.255.0
ip nat inside
duplex auto
speed auto
!
!--- Except the private network traffic from the !---
Network Address Translation (NAT) process. ip nat inside
source route-map nonat interface FastEthernet0/0
overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 99.99.99.1
!
!--- Except the private network traffic from the NAT
process. access-list 110 deny ip 10.50.50.0 0.0.0.255
10.103.1.0 0.0.0.255
access-list 110 permit ip 10.50.50.0 0.0.0.255 any
!--- Include the private network to private network
traffic !--- in the encryption process. access-list 115
permit ip 10.50.50.0 0.0.0.255 10.103.1.0 0.0.0.255
!
!--- Except the private network traffic from the NAT
process. route-map nonat permit 10
match ip address 110
!
dial-peer cor custom
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
login
!
end

Router_A#

```

라우터 B

```
Router_B#write terminal
```

```
Building configuration...
Current configuration : 1394 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router_B
!
boot system flash:c2691-ik9o3s-mz.123-1a.bin
!
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
no ftp-server write-enable
!
crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key cisco123 address 99.99.99.2
!
crypto ipsec transform-set rtpset esp-des esp-md5-hmac
!
crypto map rtp 1 ipsec-isakmp
set peer 99.99.99.2
set transform-set rtpset
!--- Include the private network to private network
traffic !--- in the encryption process. match address
115
!
no voice hpi capture buffer
no voice hpi capture destination
!
interface FastEthernet0/0
ip address 95.95.95.2 255.255.255.0
ip nat outside
duplex auto
speed auto
crypto map rtp
!
interface FastEthernet0/1
ip address 10.103.1.75 255.255.255.0
ip nat inside
duplex auto
speed auto
!
!--- Except the private network traffic from the NAT
process. ip nat inside source route-map nonat interface
FastEthernet0/0 overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 95.95.95.1
!
!--- Except the private network traffic from the NAT
process. access-list 110 deny ip 10.103.1.0 0.0.0.255
10.50.50.0 0.0.0.255
access-list 110 permit ip 10.103.1.0 0.0.0.255 any
!--- Include the private network to private network
traffic !--- in the encryption process. access-list 115
permit ip 10.103.1.0 0.0.0.255 10.50.50.0 0.0.0.255
!
```

```
!--- Except the private network traffic from the NAT
process. route-map nonat permit 10
match ip address 110
!
dial-peer cor custom
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
login
!
end
Router_B#
```

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

문제 해결 명령

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

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

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

관련 정보

- [IP 보안 문제 해결 - 디버그 명령 이해 및 사용](#)
- [IPSec 지원 페이지](#)
- [Technical Support - Cisco Systems](#)