라우터 모드 구성, 와일드 카드, 사전 공유 키, NAT 없음

목차

소개

이 샘플 컨피그레이션에서는 라우터가 NAT(Network Address Translation)를 사용하지 않고 모드 컨피그레이션(풀에서 IP 주소 가져오기), 와일드카드, 사전 공유 키(모든 PC 클라이언트가 공통 키를 공유)용으로 구성됩니다. 오프 사이트 사용자는 네트워크에 들어갈 수 있으며 풀에서 내부 IP 주소를 할당할 수 있습니다. 사용자에게 네트워크 내부에 있는 것 같습니다. 네트워크 내부의 디바이스는 라우팅 불가능한 10.2.1.x 풀에 대한 경로를 사용하여 설정됩니다.

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® Software 12.0.7T 이상
- 이 소프트웨어 버전을 지원하는 하드웨어
- CiscoSecure VPN Client 1.0/1.0.A 또는 1.1(각각 2.0.7/E 또는 2.1.12으로 표시됨)(**도움말 > 정보**로 이동하여 확인)

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 참조하십시오.

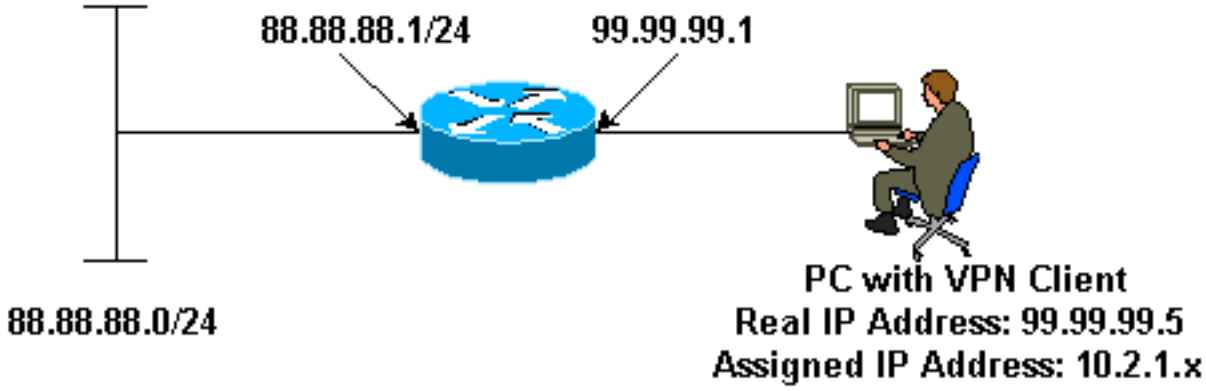
구성

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 다음 네트워크 설정을 사용합니다.



구성

이 문서에서는 다음 구성을 사용합니다.

- VPN 클라이언트
- 라우터

VPN 클라이언트

```
Network Security policy:

1- Myconn
        My Identity = ip address
                Connection security: Secure
                Remote Party Identity and addressing
                        ID Type: IP subnet
                        88.88.88.0
                        Port all Protocol all

                Connect using secure tunnel
                        ID Type: IP address
                        99.99.99.1
                        Pre-shared key = cisco123

        Authentication (Phase 1)
        Proposal 1
                Authentication method: pre-shared key
```

```
                Encryp Alg: DES
                Hash Alg: MD5
                SA life: Unspecified
                Key Group: DH 1

        Key exchange (Phase 2)
        Proposal 1
                Encapsulation ESP
                Encrypt Alg: DES
                Hash Alg: MD5
                Encap: tunnel
                SA life: Unspecified
                no AH

2- Other Connections
            Connection security: Non-secure
            Local Network Interface
                Name: Any
                IP Addr: Any
                Port: All
```

라우터

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname router
!
enable password ww
!
username cisco password 0 cisco
!
clock timezone EST -5
ip subnet-zero
cns event-service server
!

crypto isakmp policy 1
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0
crypto isakmp client configuration address-pool local
ourpool
!
crypto ipsec transform-set trans1 esp-des esp-md5-hmac
!
crypto dynamic-map dynmap 10
 set transform-set trans1
crypto map intmap client configuration address initiate
crypto map intmap client configuration address respond
crypto map intmap 10 ipsec-isakmp dynamic dynmap
!
interface Ethernet0

 ip address 99.99.99.1 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
```

```
 crypto map intmap
!
interface Ethernet1
 ip address 88.88.88.1 255.255.255.0
 no ip directed-broadcast
!

ip local pool ourpool 10.2.1.1 10.2.1.254
ip classless
no ip http server
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 password ww
 login
!
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 engine connections active** —암호화된 패킷과 해독된 패킷을 표시합니다.
- **show crypto ipsec sa** —2단계 보안 연결을 표시합니다.
- **show crypto isakmp sa** —1단계 보안 연결을 표시합니다.

이러한 디버그는 두 IPSec 라우터(피어)에서 모두 실행 중이어야 합니다. 보안 연결을 모두 지우려면 두 피어에서 모두 수행해야 합니다.

- **debug crypto ipsec** —2단계의 IPSec 협상을 표시합니다.
- **debug crypto isakmp** —1단계의 ISAKMP 협상을 표시합니다.
- **debug crypto engine** —암호화된 트래픽을 표시합니다.
- **clear crypto isakmp** —1단계와 관련된 보안 연결을 지웁니다.
- **clear crypto sa** —2단계와 관련된 보안 연결을 지웁니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- VPN 3000 Series Concentrator 제품 지원
- Cisco VPN 3000 클라이언트 제품 지원
- IPSec(IP Security Protocol) 기술 지원
- Technical Support - Cisco Systems