IPSec 구성 - Cisco Secure VPN Client 및 No-mode 컨피그레이션으로 와일드카드 사전 공유 키

목차

소개

이 샘플 컨피그레이션에서는 와일드카드 사전 공유 키에 대해 구성된 라우터를 보여 줍니다. 모든 PC 클라이언트는 공통 키를 공유합니다. 원격 사용자가 자신의 IP 주소를 유지하면서 네트워크에 진입합니다. 원격 사용자의 PC와 라우터 간의 데이터가 암호화됩니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 아래 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® 소프트웨어 릴리스 12.2.8.T1
- Cisco Secure VPN Client 버전 1.0 또는 1.1 - 단종
- DES 또는 3DES 이미지가 포함된 Cisco 라우터

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 라이브 네트워크에서 작업하는 경우, 사용하기 전에 모든 명령의 잠재적인 영향을 이해해야 합니다.

표기 규칙

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

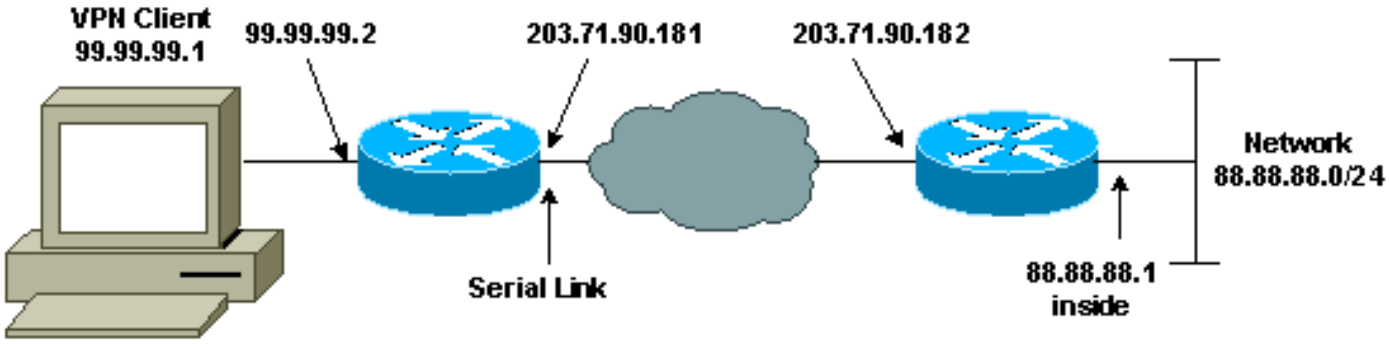
구성

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 아래 다이어그램에 표시된 네트워크 설정을 사용합니다.



구성

이 문서에서는 아래 표시된 구성을 사용합니다.

- 라우터 컨피그레이션
- VPN 클라이언트 컨피그레이션

라우터 컨피그레이션

```
Current configuration:
!
version 12.2

service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RTCisco
!
enable password hjwwkj
!
!
ip subnet-zero
ip domain-name cisco.com
ip name-server 203.71.57.242
!
!
```

```
crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key mysecretkey address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set mypolicy esp-des esp-md5-hmac
!
crypto dynamic-map dyna 10
set transform-set mypolicy
!
crypto map test 10 ipsec-isakmp dynamic dyna
!
!
interface Serial0
ip address 203.71.90.182 255.255.255.252
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
crypto map test
!
interface Ethernet0
ip address 88.88.88.1 255.255.255.0
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 203.71.90.181
!
!
line con 0
transport input none
line aux 0
transport input all
line vty 0 4
password cscscs
login
!
end
```

VPN 클라이언트 컨피그레이션

```
Network Security policy:


1- Myconn
    My Identity
         Connection security: Secure
         Remote Party Identity and addressing
         ID Type: IP subnet
         88.88.88.0
         255.255.255.0
         Port all Protocol all


    Connect using secure tunnel
         ID Type: IP address
         203.71.90.182


    Authentication (Phase 1)
    Proposal 1

        Authentication method: Preshared 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
```

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 isakmp sa** - 1단계 보안 연결을 표시합니다.
- **show crypto ipsec sa** - 1단계 보안 연결 및 프록시, 캡슐화, 암호화, 역캡슐화 및 암호 해독 정보를 표시합니다.
- **show crypto engine connections active** - 현재 연결 및 암호화된 및 해독된 패킷에 대한 정보를 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.

참고: 두 피어에서 보안 연결을 지워야 합니다. 비활성화 모드에서 router 명령을 수행합니다.

참고: 두 IPSec 피어 모두에서 이러한 디버그를 실행해야 합니다.

- **debug crypto isakmp** - 1단계 중 오류를 표시합니다.
- **debug crypto ipsec** - 2단계 중 오류를 표시합니다.
- **debug crypto engine** - 암호화 엔진의 정보를 표시합니다.
- **clear crypto isakmp** - 1단계 보안 연결을 지웁니다.

- **clear crypto sa** - 2단계 보안 연결을 지웁니다.

관련 정보

- IPSec 지원 페이지
- VPN 3000 클라이언트 지원 페이지
- Technical Support - Cisco Systems