VPN 디바이스 액세스 제어를 위한 DN 기반 암호화 맵 구성

목차

소개

이 문서에서는 VPN 디바이스가 Cisco IOS® 라우터를 사용하여 VPN 터널을 설정할 수 있도록 액세스 제어를 제공하도록 DN(Distinguished Name) 기반 암호화 맵을 구성하는 방법에 대해 설명합니다.이 문서의 예에서는 Rivest, Shamir 및 Adelman(RSA) 서명이 IKE 인증 방법입니다.표준 인증서 검증 외에도 DN 기반 암호화 맵은 X.500 고유 이름 또는 FQDN(정규화된 도메인 이름)과 같은 인증서의 특정 필드와 피어의 ISAKMP ID를 일치시키려고 합니다.

사전 요구 사항

요구 사항

이 기능은 Cisco IOS Software 릴리스 12.2(4)T에서 처음 도입되었습니다.이 컨피그레이션에는 이 릴리스 이상이 필요합니다.

Cisco IOS Software 릴리스 12.3(5)도 테스트되었습니다.그러나 Cisco 버그 ID CSCed45783으로 인해 DN 기반 암호화 맵이 실패했습니다(등록된 고객만 해당).

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco 7200 라우터
- Cisco IOS 소프트웨어 릴리스 12.2(4)T1 c7200-ik8o3s-mz.122-4.T1

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

이전에는 RSA 서명 방법을 사용하는 IKE 인증 중에, 인증 검증 및 선택적 CRL(certificate revocation list) 검사 후 Cisco IOS가 IKE 빠른 모드 협상을 계속했습니다.암호화 피어의 IP 주소에 대한 제한 외에 원격 VPN 디바이스가 암호화된 인터페이스와 통신하지 못하도록 하는 방법을 제공하지 않았습니다.

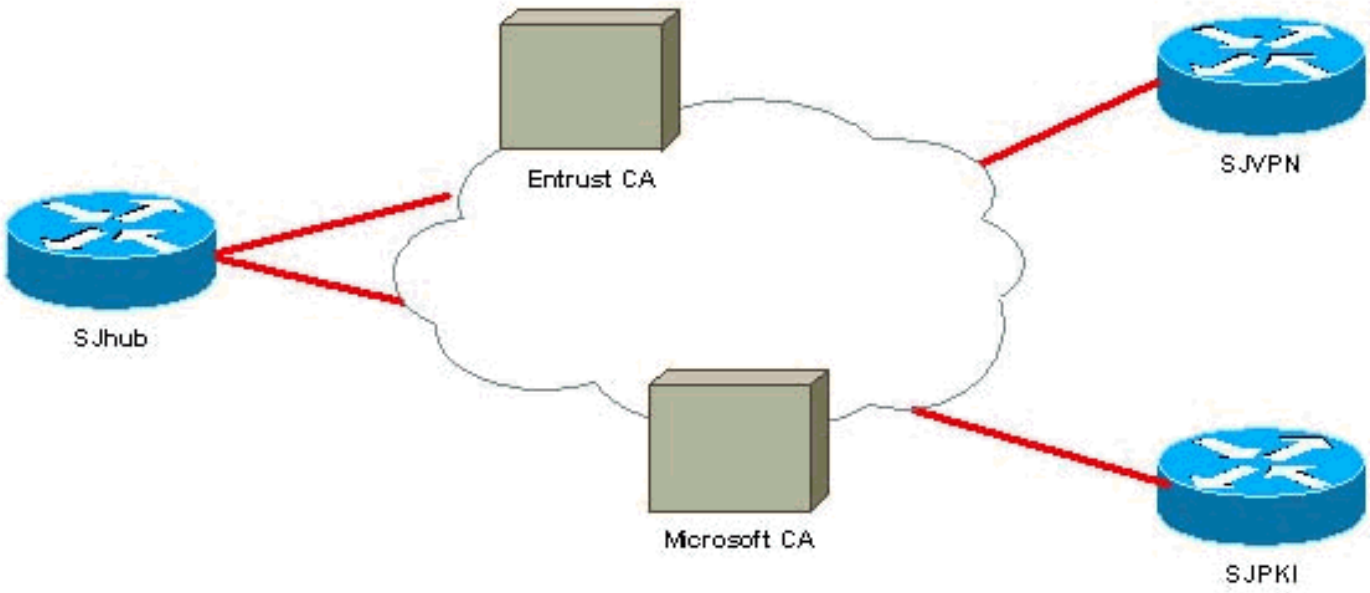
이제 DN 기반 암호화 맵을 통해 Cisco IOS는 원격 VPN 피어를 특정 인증서가 있는 선택한 인터페이스에만 액세스하도록 제한할 수 있습니다.특히 특정 DN 또는 FQDN이 있는 인증서입니다.

구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

네트워크 다이어그램

이 문서에서는 이 다이어그램에 표시된 네트워크 설정을 사용합니다.



구성

이 문서에서는 여기에 표시된 구성을 사용합니다.

이 예에서는 기능을 시연하는 데 간단한 네트워크 설정을 사용합니다.SJhub 라우터에는 두 개의 ID 인증서가 있습니다. 하나는 Entrust CA(Certificate Authority)의 인증서와 다른 하나는 Microsoft CA의 인증서입니다.관련 정보 참조