Cisco 네트워크 레이어 암호화 구성 및 문제 해결 :IPSec 및 ISAKMP - 2부

목차

소개

이 기술 보고서의 1부는 네트워크 레이어 암호화 배경 정보 및 기본 네트워크 레이어 암호화 컨피그레이션을 다룹니다.이 문서에서는 IPSec(IP Security) 및 ISAKMP(Internet Security Association and Key Management Protocol)를 다룹니다.

IPSec은 Cisco IOS® Software 릴리스 11.3T에 도입되었습니다.ISAKMP/Oakley 및 IPSec으로 구성된 안전한 데이터 전송 메커니즘을 제공합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS Software 릴리스 11.3(T) 이상

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.

네트워크 레이어 암호화 배경 정보 및 구성

정의

이 섹션에서는 이 문서 전체에서 사용되는 관련 용어를 정의합니다.

- **인증:**수신한 데이터가 실제로 클레임된 발신자가 전송됨을 확인하는 속성입니다.
- **기밀성:**의도한 수신자가 전송 내용을 알 수 있도록 하는 통신 속성입니다. 그러나 의도하지 않은 당사자는 전송 대상을 확인할 수 없습니다.
- **데이터 암호화 표준(DES):**DES는 암호 키 방법이라고도 하는 대칭 키 방법을 사용합니다.즉, 데이터 블록이 키로 암호화된 경우 암호화된 블록은 동일한 키로 해독해야 하므로 암호기와 암호 해독기가 동일한 키를 사용해야 합니다.암호화 방법을 잘 알고 널리 알려졌더라도 가장 잘 알려진 공격 방법은 무작위 대입(brute force)입니다.키를 올바르게 확인할 수 있는지 확인하려면 암호화된 블록에 대해 키를 테스트해야 합니다.프로세서가 더욱 강력해짐에 따라 DES의 자연 생명은 곧 끝납니다.예를 들어, 인터넷을 통해 수천 대의 컴퓨터의 예비 처리 능력을 사용하여 조율된 노력으로 21일 이내에 DES로 인코딩된 메시지에 대한 56비트 키를 찾을 수 있습니다 .DES는 미국 정부의 목적을 충족시키기 위해 미국 국가안보국(NSA)에 의해 5년마다 검증된다 .현재의 승인은 1998년에 만료되며 NSA는 그들이 DES를 다시 인증하지 않을 것이라고 암시했다.DES를 넘어서 무작위 대입 공격 외에 알려진 약점도 없는 다른 암호화 알고리즘도 있습니다 .자세한 내용은 NIST(National Institute of Standards and Technology)의 DES FIPS 46-2를 참조하십시오.
- **암호 해독:**암호화 알고리즘을 암호화된 데이터에 역적용함으로써 해당 데이터를 암호화되지 않은 원래 상태로 복원합니다.
- **DSS 및 DSA(디지털 서명 알고리즘):**DSA는 미국 정부의 Capstone 프로젝트의 일부인 DSS(Digital Signature Standard)에서 NIST에 의해 게시되었습니다.DSS는 NIST에 의해 미국 정부의 디지털 인증 표준이 되기 위해 NIST에 의해 선택되었다.이 표준은 1994년 5월 19일 발표되었다.
- **암호화:**데이터를 볼 권한이 없는 사용자에게 이해할 수 없도록 데이터의 모양을 변경하기 위해 특정 알고리즘을 데이터에 적용하는 것입니다.
- **무결성:**탐지되지 않은 변경 없이 데이터가 소스에서 대상으로 전송되도록 하는 속성입니다.
- **거부 없음:**일부 데이터를 보낸 사람이 나중에 해당 데이터를 전송하지 않기를 원할 수도 있지만 실제로 데이터를 전송했다는 것을 증명할 수 있는 수신자의 속성입니다.
- **공개 키 암호화:**기존 암호화는 동일한 비밀 키를 알고 사용하는 메시지의 발신자와 수신자를 기반으로 합니다.발신자는 비밀 키를 사용하여 메시지를 암호화하고 수신자는 동일한 비밀 키를 사용하여 메시지를 해독합니다.이 방법을 "secret-key" 또는 "symmetric cryptography"라고 합니다. 가장 큰 문제는 발신자와 수신자가 비밀 키에 대해 다른 사람이 알아내지 못하게 하는 것입니다.물리적 위치가 서로 다른 경우, 통신 회사, 전화 시스템 또는 기타 전송 매체를 신뢰하여 비밀 키를 전달하는 것을 방지해야 합니다.전송 중인 키를 초과 수신 또는 인터셉트하는 모든

사용자는 나중에 해당 키를 사용하여 암호화되거나 인증된 모든 메시지를 읽고 수정하고 위조할 수 있습니다.키의 생성, 전송 및 저장을 키 관리라고 합니다.모든 cryptosystems는 주요 관리 문제를 처리해야 합니다.비밀 키 암호 시스템의 모든 키는 비밀로 유지되어야 하므로 비밀 키 암호화는 보안 키 관리를 제공하는 데 어려움을 겪는 경우가 많습니다. 특히 많은 사용자가 있는 오픈 시스템에서 그렇습니다.공개 키 암호화의 개념은 키 관리 문제를 해결하기 위해 1976년 Whitfield Diffie와 Martin Hellman에 의해 도입되었습니다.컨셉에서, 각 사람은 공개 키와 개인 키라고 불리는 한 쌍의 열쇠를 갖습니다.개인 키는 비밀로 유지되는 동안 각 사람의 공개 키가 게시됩니다.발신자와 수신자가 비밀 정보를 공유해야 할 필요성이 없어지고 모든 통신에는 공개 키만 포함되며 개인 키는 전송 또는 공유되지 않습니다.더 이상 도청이나 배신을 막을 수 있는 통신 채널을 신뢰할 필요가 없다.유일한 요구 사항은 공개 키가 신뢰할 수 있는(인증된) 방식(예: 신뢰할 수 있는 디렉토리)으로 사용자와 연결된다는 것입니다. 누구나 공용 정보를 사용하여 기밀 메시지를 보낼 수 있지만, 해당 메시지는 개인 키를 통해서만 해독될 수 있으며, 이는 의도한 수신자가 단독으로 소유하고 있습니다.또한 공개 키 암호화는 개인 정보(암호화)뿐만 아니라 인증(디지털 서명)에도 사용할 수 있습니다.

- **공개 키 디지털 서명:** 메시지에 서명하려면 개인 키와 메시지 자체를 모두 포함하는 계산을 수행합니다.출력을 디지털 서명이라고 하며 메시지에 첨부되어 전송됩니다.두 번째 사람은 메시지, 알려진 서명 및 첫 번째 사람의 공개 키를 포함한 계산을 수행하여 서명을 확인합니다.결과가 간단한 수학 관계에 올바르게 저장될 경우 서명은 정품임을 확인합니다.그렇지 않으면 서명이 위조되거나 메시지가 변경되었을 수 있습니다.
- **공개 키 암호화:**한 사람이 다른 사람에게 비밀 메시지를 보내고 싶을 때, 첫 번째 사람은 디렉터리에서 두 번째 사람의 공개 키를 찾고, 그것을 사용하여 메시지를 암호화하여 보냅니다.그런 다음 두 번째 사용자는 개인 키를 사용하여 메시지를 해독하고 읽습니다.수신 대기하는 사람은 메시지를 해독할 수 없습니다.누구든지 암호화된 메시지를 두 번째 사람에게 보낼 수 있지만 두 번째 사람만이 읽을 수 있습니다.분명히, 한 가지 요구 사항은 아무도 해당 공개 키에서 개인 키를 알아낼 수 없다는 것입니다.
- **트래픽 분석:**공격자에게 유용한 정보를 추론하기 위한 네트워크 트래픽 흐름 분석.이러한 정보의 예로는 전송 빈도, 변환자의 ID, 패킷 크기, 사용된 플로우 식별자 등이 있습니다.

IPSec 및 ISAKMP

이 문서에서는 IPSec 및 ISAKMP에 대해 설명합니다.

IPSec은 Cisco IOS Software 릴리스 11.3T에 도입되었습니다.ISAKMP/Oakley 및 IPSec으로 구성된 안전한 데이터 전송 메커니즘을 제공합니다.

IPSec 프로토콜

IPSec 프로토콜(RFC 1825) 은 IP 네트워크 레이어 암호화를 제공하고 IP 데이터그램에 추가할 새로운 헤더 집합을 정의합니다.이러한 새 헤더는 IP 헤더 뒤에, 레이어 4 프로토콜(일반적으로 TCP 또는 UDP) 앞에 배치됩니다. IP 패킷의 페이로드를 보호하기 위한 정보는 아래에 설명된 대로 제공됩니다.

AH(Authentication Header) 및 ESP(Encapsulating Security Payload)는 독립적으로 또는 함께 사용할 수 있지만 대부분의 응용 프로그램에서는 이 중 하나만 사용할 수 있습니다.이러한 두 프로토콜 모두에서 IPSec은 사용할 특정 보안 알고리즘을 정의하지 않고 업계 표준 알고리즘을 구현하기 위한 개방형 프레임워크를 제공합니다.처음에는 대부분의 IPSec 구현이 RSA Data Security 또는 SHA(Secure Hash Algorithm)의 MD5를 지원하는데, 이는 무결성 및 인증을 위해 미국 정부가 정의한 것입니다.DES는 현재 가장 일반적으로 제공되는 대량 암호화 알고리즘입니다. IDEA, Blowfish,

RC4를 비롯한 다른 여러 암호화 시스템의 사용 방법을 정의하는 RFC를 사용할 수 있습니다.

- **AH**(RFC 1826 참조)AH는 IP 데이터그램에 강력한 무결성 및 인증을 제공하는 메커니즘입니다.또한 어떤 암호화 알고리즘이 사용되는지 및 키 지정 방법에 따라 부인 방지 기능을 제공할 수 있습니다.예를 들어, RSA와 같은 비대칭 디지털 서명 알고리즘을 사용하면 거부되지 않을 수 있습니다.AH에서는 기밀성 및 트래픽 분석으로부터의 보호를 제공하지 않습니다.기밀성이 필요한 사용자는 AH를 대신하거나 함께 IP ESP를 사용하는 것을 고려해야 합니다.AH는 각 홉에서 검사되는 다른 헤더 뒤에, 중간 홉에서 검사되지 않은 다른 헤더 앞에 나타날 수 있습니다.AH 바로 앞의 IPv4 또는 IPv6 헤더에 Next Header(또는 프로토콜) 필드에 51이라는 값이 포함됩니다.
- **ESP**(RFC 1827 참조)ESP는 IP 헤더 후와 최종 전송 레이어 프로토콜 앞에 나타날 수 있습니다.Internet Assigned Numbers Authority에서 ESP에 프로토콜 번호 50을 할당했습니다.ESP 헤더 바로 앞의 헤더에는 항상 Next Header(IPv6) 또는 Protocol(IPv4) 필드의 값 50이 포함됩니다.ESP는 암호화되지 않은 헤더와 암호화된 데이터로 구성됩니다.암호화된 데이터에는 전체 IP 데이터그램 또는 상위 계층 프로토콜 프레임(예: TCP 또는 UDP)인 보호된 ESP 헤더 필드와 보호된 사용자 데이터가 모두 포함됩니다.IP ESP는 보호할 데이터를 암호화하고 암호화된 데이터를 IP ESP의 데이터 부분에 배치하여 기밀성과 무결성을 제공하려고 합니다.사용자의 보안 요구 사항에 따라 이 메커니즘을 사용하여 전송 계층 세그먼트(예: TCP, UDP, ICMP, IGMP) 또는 전체 IP 데이터그램을 암호화할 수 있습니다.원래 데이터그램 전체에 기밀을 유지하기 위해서는 보호된 데이터를 캡슐화해야 합니다.이 사양을 사용하면 참여 시스템의 IP 프로토콜 처리 비용이 증가하고 통신 레이턴시도 증가합니다.레이턴시가 증가한 것은 ESP를 포함하는 각 IP 데이터그램에 필요한 암호화 및 암호 해독 때문입니다.터널 모드 ESP에서 원래 IP 데이터그램은 ESP의 암호화된 부분에 배치되며 암호화되지 않은 IP 헤더가 있는 데이터그램 내에 전체 ESP 프레임이 배치됩니다.암호화되지 않은 IP 헤더의 정보는 보안 데이터그램을 원본에서 대상으로 라우팅하는 데 사용됩니다.암호화되지 않은 IP 라우팅 헤더가 IP 헤더와 ESP 사이에 포함될 수 있습니다.이 모드에서는 라우터와 같은 네트워크 디바이스가 IPSec 프록시 역할을 할 수 있습니다.즉, 라우터가 호스트를 대신하여 암호화를 수행합니다.소스의 라우터는 패킷을 암호화하고 IPSec 터널을 따라 전달합니다.목적지의 라우터는 원래 IP 데이터그램을 해독하고 목적지 시스템에 전달합니다.터널 모드의 주요 장점은 IP 보안의 이점을 활용하기 위해 최종 시스템을 수정할 필요가 없다는 점입니다.터널 모드는 트래픽 분석에서도 보호합니다.터널 모드에서는 공격자가 터널 엔드포인트만 확인할 수 있으며 터널 엔드포인트와 동일한 경우에도 터널링된 패킷의 실제 소스 및 대상은 확인할 수 없습니다.IETF에서 정의한 대로 소스 및 대상 시스템이 모두 IPSec을 이해하는 경우에만 IPSec 전송 모드를 사용할 수 있습니다.대부분의 경우 터널 모드로 IPSec을 구축합니다.이렇게 하면 운영 체제나 PC, 서버 및 호스트의 애플리케이션을 수정하지 않고도 네트워크 아키텍처에 IPSec을 구현할 수 있습니다.전송 모드 ESP에서 ESP 헤더는 전송 계층 프로토콜 헤더(예: TCP, UDP 또는 ICMP) 바로 앞에 IP 데이터그램에 삽입됩니다. 이 모드에서는 암호화된 IP 헤더 또는 IP 옵션이 없으므로 대역폭이 유지됩니다.IP 페이로드만 암호화되며 원래 IP 헤더는 그대로 유지됩니다.이 모드에서는 각 패킷에 몇 바이트만 추가할 수 있습니다.또한 공용 네트워크의 디바이스에서 패킷의 최종 소스 및 대상을 볼 수 있습니다.이 기능을 사용하면 IP 헤더의 정보를 기반으로 중간 네트워크에서 특수 처리(예: QoS)를 활성화할 수 있습니다.그러나 레이어 4 헤더는 암호화되어 패킷 검사를 제한합니다.안타깝게도 IP 헤더를 일반 전송 모드로 전달하면 공격자가 일부 트래픽 분석을 수행할 수 있습니다.예를 들어, 공격자는 한 CEO가 다른 CEO에게 많은 패킷을 전송한 경우를 볼 수 있었습니다.그러나 공격자는 IP 패킷이 전송되었음을 알 뿐입니다.공격자는 전자 메일이나 다른 응용 프로그램인지 확인할 수 없습니다.

ISAKMP/오크리

IPSec은 IP 데이터그램을 보호하는 실제 프로토콜이지만 ISAKMP는 정책을 협상하는 프로토콜이며 IPSec 피어가 공유하는 키를 생성하기 위한 공통 프레임워크를 제공합니다.키 관리 또는 키 교환에 대한 세부 정보를 지정하지 않으며 키 생성 기법에 바인딩되지 않습니다.ISAKMP 내부에서는 Cisco가 키 교환 프로토콜에 Oakley를 사용합니다.오클리는 5개의 잘 알려진 그룹 중에서 선택할 수 있다.Cisco IOS는 그룹 1(768비트 키) 및 그룹 2(1024비트 키)를 지원합니다. Cisco IOS Software 릴리스 12.1(3)T에서 그룹 5(1536비트 키)에 대한 지원이 도입되었습니다.

ISAKMP/Oakley는 두 엔티티 간에 인증되고 안전한 터널을 생성한 다음 IPSec에 대한 보안 연결을 협상합니다.이 프로세스에서는 두 엔티티가 서로 인증하고 공유 키를 설정해야 합니다.

양 당사자는 서로 인증되어야 합니다.ISAKMP/Oakley는 여러 인증 방법을 지원합니다.두 엔티티는 RSA 서명, RSA 암호화 nonces 또는 사전 공유 키를 사용하는 협상 프로세스를 통해 공통 인증 프로토콜에 동의해야 합니다.

ISAKMP/Oakley 터널을 암호화하려면 양 당사자 모두 공유 세션 키를 가져야 합니다.Diffie-Hellman 프로토콜은 공통 세션 키에 동의하는 데 사용됩니다.Exchange는 위에서 설명한 대로 인증되어 "중간자(man-in-the-middle)" 공격을 차단합니다.

인증 및 키 교환이라는 두 단계는 두 디바이스 간의 안전한 터널인 ISAKMP/Oakley SA(Session Association)를 생성합니다.터널의 한 쪽은 일련의 알고리즘을 제공합니다.그러면 상대방은 제안 중 하나를 수락하거나 전체 연결을 거부해야 합니다.양측이 사용할 알고리즘에 동의한 경우, AH, ESP 또는 둘 모두와 함께 IPSec에 사용할 주요 자료를 도출해야 합니다.

IPSec은 ISAKMP/Oakley와 다른 공유 키를 사용합니다.IPSec 공유 키는 Diffie-Hellman을 다시 사용하여 완벽한 전달 보안을 보장하거나, ISAKMP/Oakley SA를 의사 난수(nonces)로 해싱하여 생성한 원래 Diffie-Hellman 교환에서 파생된 공유 암호를 새로 고치는 방법으로 파생될 수 있습니다. 첫 번째 방법은 더 강력한 보안을 제공하지만 속도가 느립니다.대부분의 구현에서는 두 가지 방법의 조합이 사용됩니다.즉, Diffie-Hellman은 첫 번째 키 교환에 사용되며, 로컬 정책은 Diffie-Hellman을 사용하거나 단순히 키 리프레쉬를 사용할 시기를 결정합니다.이 작업이 완료되면 IPSec SA가 설정됩니다.

RSA 서명 및 RSA 암호화 논문은 모두 원격 피어의 공개 키를 필요로 하며, 원격 피어가 로컬 공개 키를 보유해야 합니다.공개 키는 ISAKMP에서 인증서 형식으로 교환됩니다.이러한 인증서는 CA(Certificate Authority)에 등록하여 얻습니다. 현재 라우터에 인증서가 없는 경우 ISAKMP는 보호 제품군 RSA 서명을 협상하지 않습니다.

Cisco 라우터는 인증서를 생성하지 않습니다.라우터가 키를 만들고 해당 키에 대한 인증서를 요청합니다.라우터의 키를 ID에 바인딩하는 인증서는 인증 기관에서 생성하고 서명합니다.이는 관리 기능이며, 인증 기관은 항상 사용자가 자신이 누구인지를 확인하기 위해 일종의 검증을 요구합니다.즉, 즉시 새 인증서를 만들 수 없습니다.

통신 시스템은 인증 기관에서 얻은 기존 인증서를 교환합니다.인증서 자체는 공개 정보이지만 인증서를 사용하여 ID를 증명하려는 모든 사용자가 해당 개인 키를 사용할 수 있어야 합니다.그러나 그들은 또한 그 신분을 사용할 수 없어야 하는 어떤 사람에게서도 비밀로 유지되어야 합니다.

인증서는 사용자 또는 시스템을 식별할 수 있습니다.구현에 따라 다릅니다.대부분의 초기 시스템에서는 인증서를 사용하여 시스템을 식별할 수 있습니다.인증서가 사용자를 식별하는 경우 해당 인증서에 해당하는 개인 키는 동일한 시스템의 다른 사용자가 사용할 수 없는 방식으로 저장해야 합니다.일반적으로 키는 암호화되거나 스마트 카드에 보관됩니다.암호화 키 사례는 초기 구현에서 더 일반적일 수 있습니다.어떤 경우든 사용자는 일반적으로 키가 활성화될 때마다 암호문을 입력해야 합니다.

참고: ISAKMP/Oakley는 협상에 UDP 포트 500을 사용합니다.AH는 Protocol(프로토콜) 필드에

51을 포함하고 ESP는 Protocol(프로토콜) 필드에 50을 포함합니다.이러한 항목을 필터링하지 않는지 확인합니다.

이 기술 보고서에 사용된 용어에 대한 자세한 내용은 정의 섹션을 참조하십시오.

IPSec 및 ISAKMP용 Cisco IOS 네트워크 레이어 암호화 구성

이 문서의 작업 샘플 Cisco IOS 구성은 실습 라우터에서 직접 가져왔습니다.단, 이는 관련되지 않은 인터페이스 컨피그레이션을 제거하는 것뿐입니다.이 문서의 모든 자료는 인터넷이나 이 문서 끝에 있는 관련 정보 섹션에서 무료로 사용할 수 있는 리소스에서 제공됩니다.

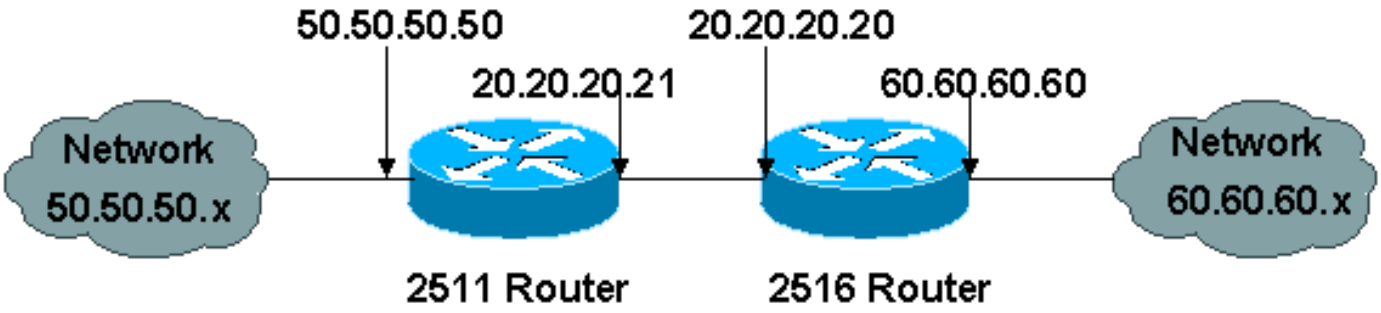
샘플 1:ISAKMP 사전 공유 키

사전 공유 키를 통한 인증은 비공개 키 대안입니다.이 방법을 사용하여 각 피어는 대역 외 교환되어 라우터로 구성된 비밀 키를 공유합니다.이 비밀을 명시적으로 언급하지 않고 각 당사자가 이를 증명할 수 있는 기능이 교환을 인증합니다.이 방법은 소규모 설치에 적합하지만 확장 문제가 있습니다."sharedkey"의 사전 공유 키가 아래에 사용됩니다.호스트가 주소 기반 사전 공유 키를 공유하는 경우 Cisco IOS Software의 기본값인 주소 ID를 사용해야 컨피그레이션에 표시되지 않습니다.

```
crypto isakmp identity address
```

참고: ISAKMP에서 IPSec에 대한 정책 및 키를 설정할 수 없는 경우가 있습니다.라우터에 정의된 인증서가 없고 ISAKMP 정책에 공개 키 기반 인증 방법만 있거나, 피어에 대한 인증서 및 사전 공유 키가 없는 경우(주소를 통해 직접 공유하거나 해당 주소로 구성된 호스트 이름으로 공유됨), ISAKMP가 피어와 협상할 수 없으며 IPSec이 작동하지 않습니다.

다음 그림은 이 구성에 대한 네트워크 다이어그램을 나타냅니다.



다음은 사전 공유 키를 기반으로 IPSec 및 ISAKMP 인증을 수행하는 두 라우터(Cisco 2511 및 Cisco 2516)에 대한 컨피그레이션입니다.코멘트 줄은 첫 번째 문자로 느낌표로 표시되고 라우터에 입력하면 무시됩니다.아래 컨피그레이션에서는 설명을 위해 특정 컨피그레이션 라인 앞에 주석이 있습니다.

Cisco 2511 구성

```
cl-2513-2A#write terminal
Building configuration...

Current configuration:
!
```

```
version 11.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname cl-2513-2A
!
!--- Override the default policy and use !--- preshared
keys for authentication. crypto isakmp policy 1
authentication pre-share group 2 ! !--- Define our
secret shared key so !--- you do not have to use RSA
keys. crypto isakmp key sharedkey address 20.20.20.20 !
!--- These are the authentication and encryption !---
settings defined for "auth2", !--- which is later
applied to the crypto map. crypto ipsec transform-set
auth2 esp-des esp-sha-hmac ! !--- The crypto map where
you define your peer, !--- transform auth2, and your
access list. crypto map test 10 ipsec-isakmp set peer
20.20.20.20 set transform-set auth2 match address 133 !
interface Ethernet0 ip address 50.50.50.50 255.255.255.0
! interface Serial0 ip address 20.20.20.21 255.255.255.0
no ip route-cache no ip mroute-cache !--- Nothing
happens unless you apply !--- the crypto map to an
interface. crypto map test ! ip route 0.0.0.0 0.0.0.0
20.20.20.20 ! !--- This is the access list referenced !-
-- in the crypto map; never use "any". !--- You are
encrypting traffic between !--- the remote Ethernet
LANs. access-list 133 permit ip 50.50.50.0 0.0.0.255
60.60.60.0 0.0.0.255 ! line con 0 line aux 0 line vty 0
4 login ! end
```

Cisco 2516 컨피그레이션

```
cl-2513-2B#show run
Building configuration...

Current configuration:
!
version 11.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname cl-2513-2B
!
ip subnet-zero
!
!--- Override the default policy and use !--- preshared
keys for authentication. crypto isakmp policy 1
authentication pre-share group 2 !--- Define the secret
shared key so you !--- do not have to use RSA keys.
crypto isakmp key sharedkey address 20.20.20.21 !---
These are the authentication and encryption !---
settings defined for "auth2," !--- which is later
applied to the crypto map. crypto ipsec transform-set
auth2 esp-des esp-sha-hmac !--- The crypto map where you
define the peer, !--- transform auth2, and the access
list. crypto map test 10 ipsec-isakmp set peer
20.20.20.21 set transform-set auth2 match address 144 !
interface Ethernet0 ip address 60.60.60.60 255.255.255.0
no ip directed-broadcast ! !--- Nothing happens unless
you apply !--- the crypto map to an interface. interface
Serial0 ip address 20.20.20.20 255.255.255.0 no ip
```

```
directed-broadcast no ip route-cache no ip mroute-cache
clockrate 800000 crypto map test ! ip classless ip route
0.0.0.0 0.0.0.0 20.20.20.21 ! !--- This is the access
list referenced !--- in the crypto map; never use "any".
!--- You are encrypting traffic between !--- the remote
Ethernet LANs. access-list 144 permit ip 60.60.60.0
0.0.0.255 50.50.50.0 0.0.0.255 ! line con 0 transport
input none line aux 0 line vty 0 4 login ! end
```

다음은 **debug** 명령 출력입니다.

```
--------------- Preshare with RSA key defined
(need to remove RSA keys) -----

*Mar  1 00:14:48.579: ISAKMP (10): incorrect policy settings.
 Unable to initiate.
*Mar  1 00:14:48.587: ISAKMP (11): incorrect policy settings.
 Unable to initiate......

--------------- Preshare, wrong hostname ---------------

ISAKMP: no pre-shared key based on hostname wan-2511.cisco.com!
%CRYPTO-6-IKMP_MODE_FAILURE: Processing of Aggressive mode
 failed with peer at
20.20.20.21
--------------- Preshare, incompatable policy --------------
wan2511#
*Mar  1 00:33:34.839: ISAKMP (17): processing SA payload. message ID = 0
*Mar  1 00:33:34.843: ISAKMP (17): Checking ISAKMP transform 1
 against priority 1 policy
*Mar  1 00:33:34.843: ISAKMP:      encryption DES-CBC
*Mar  1 00:33:34.843: ISAKMP:      hash SHA
*Mar  1 00:33:34.847: ISAKMP:      default group 2
*Mar  1 00:33:34.847: ISAKMP:      auth pre-share
*Mar  1 00:33:34.847: ISAKMP:      life type in seconds
*Mar  1 00:33:34.851: ISAKMP:      life duration (basic) of 240
*Mar  1 00:33:34.851: ISAKMP (17): atts are acceptable.
 Next payload is 0
*Mar  1 00:33:43.735: ISAKMP (17): processing KE payload.
 message ID = 0
*Mar  1 00:33:54.307: ISAKMP (17): processing NONCE payload.
 message ID = 0
*Mar  1 00:33:54.311: ISAKMP (17): processing ID payload.
 message ID = 0
*Mar  1 00:33:54.331: ISAKMP (17): SKEYID state generated
*Mar  1 00:34:04.867: ISAKMP (17): processing HASH payload.
 message ID = 0
*Mar  1 00:34:04.879: ISAKMP (17): SA has been authenticated
*Mar  1 00:34:06.151: ISAKMP (17): processing SA payload.
 message ID = -1357683133
*Mar  1 00:34:06.155: ISAKMP (17): Checking IPSec proposal 1
*Mar  1 00:34:06.155: ISAKMP: transform 1, AH_MD5_HMAC
*Mar  1 00:34:06.159: ISAKMP:   attributes in transform:
*Mar  1 00:34:06.159: ISAKMP:      encaps is 1
*Mar  1 00:34:06.159: ISAKMP:      SA life type in seconds
*Mar  1 00:34:06.163: ISAKMP:      SA life duration (basic) of 3600
*Mar  1 00:34:06.163: ISAKMP:      SA life type in kilobytes
*Mar  1 00:34:06.163: ISAKMP:      SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar  1 00:34:06.167: ISAKMP (17): atts not acceptable.
 Next payload is 0
*Mar  1 00:34:06.171: ISAKMP (17): Checking IPSec proposal 1
```

```
*Mar  1 00:34:06.171: ISAKMP: transform 1, ESP_DES
*Mar  1 00:34:06.171: ISAKMP:   attributes in transform:
*Mar  1 00:34:06.175: ISAKMP:      encaps is 1
*Mar  1 00:34:06.175: ISAKMP:      SA life type in seconds
*Mar  1 00:34:06.175: ISAKMP:      SA life duration (basic) of 3600
*Mar  1 00:34:06.179: ISAKMP:      SA life type in kilobytes
*Mar  1 00:34:06.179: ISAKMP:      SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar  1 00:34:06.183: ISAKMP:      HMAC algorithm is SHA
*Mar  1 00:34:06.183: ISAKMP (17): atts are acceptable.
*Mar  1 00:34:06.187: ISAKMP (17): SA not acceptable!
%CRYPTO-6-IKMP_MODE_FAILURE: Processing of Quick mode failed
with peer at 20.20.20.20
wan2511#

----------------- preshare, debug isakmp -------------------

wan2511#
*Mar  1 00:06:54.179: ISAKMP (1): processing SA payload.
 message ID = 0
*Mar  1 00:06:54.179: ISAKMP (1): Checking ISAKMP transform 1
 against priority 1 policy
*Mar  1 00:06:54.183: ISAKMP:      encryption DES-CBC
*Mar  1 00:06:54.183: ISAKMP:      hash SHA
*Mar  1 00:06:54.183: ISAKMP:      default group 2
*Mar  1 00:06:54.187: ISAKMP:      auth pre-share
*Mar  1 00:06:54.187: ISAKMP:      life type in seconds
*Mar  1 00:06:54.187: ISAKMP:      life duration (basic) of 240
*Mar  1 00:06:54.191: ISAKMP (1): atts are acceptable.
 Next payload is 0
*Mar  1 00:07:02.955: ISAKMP (1): processing KE payload.
 message ID = 0
*Mar  1 00:07:13.411: ISAKMP (1): processing NONCE payload.
 message ID = 0
*Mar  1 00:07:13.415: ISAKMP (1): processing ID payload.
 message ID = 0
*Mar  1 00:07:13.435: ISAKMP (1): SKEYID state generated
*Mar  1 00:07:23.903: ISAKMP (1): processing HASH payload.
 message ID = 0
*Mar  1 00:07:23.915: ISAKMP (1): SA has been authenticated
*Mar  1 00:07:25.187: ISAKMP (1): processing SA payload.
 message ID = 1435594195
*Mar  1 00:07:25.187: ISAKMP (1): Checking IPSec proposal 1
*Mar  1 00:07:25.191: ISAKMP: transform 1, AH_SHA_HMAC
*Mar  1 00:07:25.191: ISAKMP:   attributes in transform:
*Mar  1 00:07:25.191: ISAKMP:      encaps is 1
*Mar  1 00:07:25.195: ISAKMP:      SA life type in seconds
*Mar  1 00:07:25.195: ISAKMP:      SA life duration (basic) of 3600
*Mar  1 00:07:25.195: ISAKMP:      SA life type in kilobytes
*Mar  1 00:07:25.199: ISAKMP:      SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar  1 00:07:25.203: ISAKMP (1): atts are acceptable.
*Mar  1 00:07:25.203: ISAKMP (1): Checking IPSec proposal 1
*Mar  1 00:07:25.207: ISAKMP: transform 1, ESP_DES
*Mar  1 00:07:25.207: ISAKMP:   attributes in transform:
*Mar  1 00:07:25.207: ISAKMP:      encaps is 1
*Mar  1 00:07:25.211: ISAKMP:      SA life type in seconds
*Mar  1 00:07:25.211: ISAKMP:      SA life duration (basic) of 3600
*Mar  1 00:07:25.211: ISAKMP:      SA life type in kilobytes
*Mar  1 00:07:25.215: ISAKMP:      SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar  1 00:07:25.215: ISAKMP:      HMAC algorithm is SHA
*Mar  1 00:07:25.219: ISAKMP (1): atts are acceptable.
*Mar  1 00:07:25.223: ISAKMP (1): processing NONCE payload.
```

```
 message ID = 1435594195
*Mar  1 00:07:25.227: ISAKMP (1): processing ID payload.
 message ID = 1435594195
*Mar  1 00:07:25.227: ISAKMP (1): processing ID payload.
 message ID = 1435594195
*Mar  1 00:07:25.639: ISAKMP (1): Creating IPSec SAs
*Mar  1 00:07:25.643:         inbound SA from 20.20.20.20
     to 20.20.20.21
        (proxy 60.60.60.0      to 50.50.50.0     )
*Mar  1 00:07:25.647:         has spi 85067251 and
 conn_id 3 and flags 4
*Mar  1 00:07:25.647:         lifetime of 3600 seconds
*Mar  1 00:07:25.647:         lifetime of 4608000 kilobytes
*Mar  1 00:07:25.651:         outbound SA from 20.20.20.21
     to 20.20.20.20
        (proxy 50.50.50.0      to 60.60.60.0     )
*Mar  1 00:07:25.655:         has spi 57872298 and
 conn_id 4 and flags 4
*Mar  1 00:07:25.655:         lifetime of 3600 seconds
*Mar  1 00:07:25.655:         lifetime of 4608000 kilobytes
*Mar  1 00:07:25.659: ISAKMP (1): Creating IPSec SAs
*Mar  1 00:07:25.659:         inbound SA from 20.20.20.20
   to 20.20.20.21
        (proxy 60.60.60.0      to 50.50.50.0     )
*Mar  1 00:07:25.663:         has spi 538316566 and
 conn_id 5 and flags 4
*Mar  1 00:07:25.663:         lifetime of 3600 seconds
*Mar  1 00:07:25.667:         lifetime of 4608000 kilobytes
*Mar  1 00:07:25.667:         outbound SA from 20.20.20.21
 to 20.20.20.20
        (proxy 50.50.50.0      to 60.60.60.0     )
*Mar  1 00:07:25.671:         has spi 356000275 and
 conn_id 6 and flags 4
*Mar  1 00:07:25.671:         lifetime of 3600 seconds
*Mar  1 00:07:25.675:         lifetime of 4608000 kilobytes
wan2511#

----------------- preshare debug ipsec -------------------
wan2511#
*Mar  1 00:05:26.947: IPSEC(validate_proposal_request):
proposal part #1,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/0.0.0.0/0/0,
    src_proxy= 60.60.60.0/0.0.0.16/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar  1 00:05:26.955: IPSEC(validate_proposal_request):
proposal part #2,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/0.0.0.0/0/0,
    src_proxy= 60.60.60.0/0.0.0.16/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar  1 00:05:26.967: IPSEC(key_engine): got a queue event...
*Mar  1 00:05:26.971: IPSEC(spi_response): getting
 spi 203563166 for SA
        from 20.20.20.20     to 20.20.20.21     for prot 2
*Mar  1 00:05:26.975: IPSEC(spi_response): getting
 spi 194838793 for SA
        from 20.20.20.20     to 20.20.20.21     for prot 3
*Mar  1 00:05:27.379: IPSEC(key_engine): got a queue event...
*Mar  1 00:05:27.379: IPSEC(initialize_sas): ,
```

```
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/255.255.255.0/0/0,
    src_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xC22209E(203563166), conn_id= 3, keysize= 0, flags= 0x4
*Mar  1 00:05:27.387: IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 20.20.20.21, dest= 20.20.20.20,
    src_proxy= 50.50.50.0/255.255.255.0/0/0,
    dest_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x15E010D(22937869), conn_id= 4, keysize= 0, flags= 0x4
*Mar  1 00:05:27.395: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/255.255.255.0/0/0,
    src_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xB9D0109(194838793), conn_id= 5, keysize= 0, flags= 0x4
*Mar  1 00:05:27.403: IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 20.20.20.21, dest= 20.20.20.20,
    src_proxy= 50.50.50.0/255.255.255.0/0/0,
    dest_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xDED0AB4(233638580), conn_id= 6, keysize= 0, flags= 0x4
*Mar  1 00:05:27.415: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.21, sa_prot= 51,
    sa_spi= 0xC22209E(203563166),
    sa_trans= ah-sha-hmac , sa_conn_id= 3
*Mar  1 00:05:27.419: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.20, sa_prot= 51,
    sa_spi= 0x15E010D(22937869),
    sa_trans= ah-sha-hmac , sa_conn_id= 4
*Mar  1 00:05:27.423: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.21, sa_prot= 50,
    sa_spi= 0xB9D0109(194838793),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
*Mar  1 00:05:27.427: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.20, sa_prot= 50,
    sa_spi= 0xDED0AB4(233638580),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
wan2511#

--------------- Preshare, good connection ------
wan2511#
*Mar  1 00:09:45.095: ISAKMP (1): processing SA payload.
 message ID = 0
*Mar  1 00:09:45.099: ISAKMP (1): Checking ISAKMP transform
 1 against priority 1 policy
*Mar  1 00:09:45.099: ISAKMP:      encryption DES-CBC
*Mar  1 00:09:45.103: ISAKMP:      hash SHA
*Mar  1 00:09:45.103: ISAKMP:      default group 2
*Mar  1 00:09:45.103: ISAKMP:      auth pre-share
*Mar  1 00:09:45.107: ISAKMP:      life type in seconds
*Mar  1 00:09:45.107: ISAKMP:      life duration (basic) of 240
*Mar  1 00:09:45.107: ISAKMP (1): atts are acceptable.
Next payload is 0
*Mar  1 00:09:53.867: ISAKMP (1): processing KE payload.
 message ID = 0
*Mar  1 00:10:04.323: ISAKMP (1): processing NONCE payload.
 message ID = 0
*Mar  1 00:10:04.327: ISAKMP (1): processing ID payload.
```

```
 message ID = 0
*Mar  1 00:10:04.347: ISAKMP (1): SKEYID state generated
*Mar  1 00:10:15.103: ISAKMP (1): processing HASH payload.
 message ID = 0
*Mar  1 00:10:15.115: ISAKMP (1): SA has been authenticated
*Mar  1 00:10:16.391: ISAKMP (1): processing SA payload.
 message ID = 800032287
*Mar  1 00:10:16.391: ISAKMP (1): Checking IPSec proposal 1
*Mar  1 00:10:16.395: ISAKMP: transform 1, AH_SHA_HMAC
*Mar  1 00:10:16.395: ISAKMP:   attributes in transform:
*Mar  1 00:10:16.395: ISAKMP:      encaps is 1
*Mar  1 00:10:16.399: ISAKMP:      SA life type in seconds
*Mar  1 00:10:16.399: ISAKMP:      SA life duration (basic) of 3600
*Mar  1 00:10:16.399: ISAKMP:      SA life type in kilobytes
*Mar  1 00:10:16.403: ISAKMP:      SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar  1 00:10:16.407: ISAKMP (1): atts are acceptable.
*Mar  1 00:10:16.407: ISAKMP (1): Checking IPSec proposal 1
*Mar  1 00:10:16.411: ISAKMP: transform 1, ESP_DES
*Mar  1 00:10:16.411: ISAKMP:   attributes in transform:
*Mar  1 00:10:16.411: ISAKMP:      encaps is 1
*Mar  1 00:10:16.415: ISAKMP:      SA life type in seconds
*Mar  1 00:10:16.415: ISAKMP:      SA life duration (basic) of 3600
*Mar  1 00:10:16.415: ISAKMP:      SA life type in kilobytes
*Mar  1 00:10:16.419: ISAKMP:      SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar  1 00:10:16.419: ISAKMP:      HMAC algorithm is SHA
*Mar  1 00:10:16.423: ISAKMP (1): atts are acceptable.
*Mar  1 00:10:16.427: IPSEC(validate_proposal_request):
 proposal part #1,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/0.0.0.0/0/0,
    src_proxy= 60.60.60.0/0.0.0.16/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar  1 00:10:16.435: IPSEC(validate_proposal_request):
 proposal part #2,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/0.0.0.0/0/0,
    src_proxy= 60.60.60.0/0.0.0.16/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar  1 00:10:16.443: ISAKMP (1): processing NONCE payload.
 message ID = 800032287
*Mar  1 00:10:16.443: ISAKMP (1): processing ID payload.
 message ID = 800032287
*Mar  1 00:10:16.447: ISAKMP (1): processing ID payload.
 message ID = 800032287
*Mar  1 00:10:16.451: IPSEC(key_engine): got a queue event...
*Mar  1 00:10:16.455: IPSEC(spi_response): getting
spi 16457800 for SA
        from 20.20.20.20     to 20.20.20.21     for prot 2
*Mar  1 00:10:16.459: IPSEC(spi_response): getting
spi 305534655 for SA
        from 20.20.20.20     to 20.20.20.21     for prot 3
*Mar  1 00:10:17.095: ISAKMP (1): Creating IPSec SAs
*Mar  1 00:10:17.095:         inbound SA from 20.20.20.20
     to 20.20.20.21
        (proxy 60.60.60.0      to 50.50.50.0     )
*Mar  1 00:10:17.099:         has spi 16457800 and conn_id 3
 and flags 4
*Mar  1 00:10:17.103:         lifetime of 3600 seconds
```

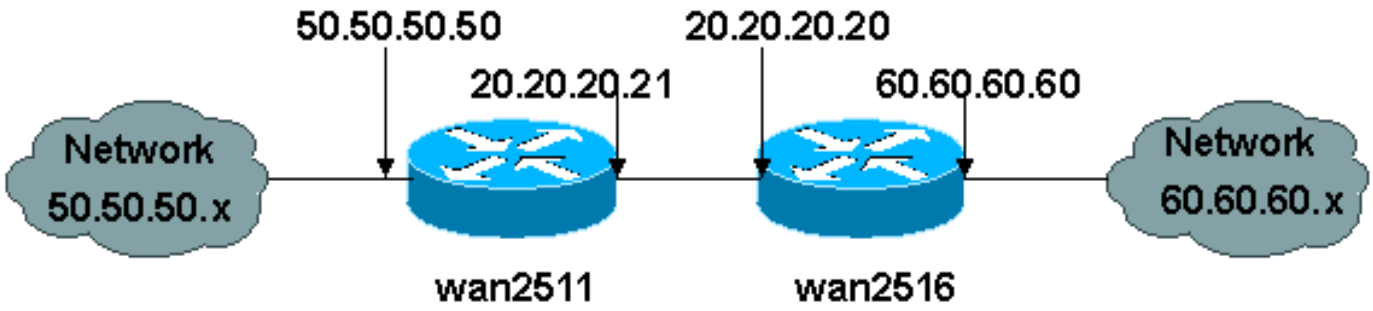
```
*Mar  1 00:10:17.103:         lifetime of 4608000 kilobytes
*Mar  1 00:10:17.103:         outbound SA from 20.20.20.21
     to 20.20.20.20
        (proxy 50.50.50.0      to 60.60.60.0     )
*Mar  1 00:10:17.107:         has spi 507120385 and conn_id 4
 and flags 4
*Mar  1 00:10:17.111:         lifetime of 3600 seconds
*Mar  1 00:10:17.111:         lifetime of 4608000 kilobytes
*Mar  1 00:10:17.115: ISAKMP (1): Creating IPSec SAs
*Mar  1 00:10:17.115:         inbound SA from 20.20.20.20
to 20.20.20.21
        (proxy 60.60.60.0      to 50.50.50.0     )
*Mar  1 00:10:17.119:         has spi 305534655 and
conn_id 5 and flags 4
*Mar  1 00:10:17.119:         lifetime of 3600 seconds
*Mar  1 00:10:17.123:         lifetime of 4608000 kilobytes
*Mar  1 00:10:17.123:         outbound SA from 20.20.20.21
     to 20.20.20.20
        (proxy 50.50.50.0      to 60.60.60.0     )
*Mar  1 00:10:17.127:         has spi 554175376 and
conn_id 6 and flags 4
*Mar  1 00:10:17.127:         lifetime of 3600 seconds
*Mar  1 00:10:17.131:         lifetime of 4608000 kilobytes
*Mar  1 00:10:17.139: IPSEC(key_engine): got a queue event...
*Mar  1 00:10:17.143: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/255.255.255.0/0/0,
    src_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xFB2048(16457800), conn_id= 3, keysize= 0,
 flags= 0x4
*Mar  1 00:10:17.151: IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 20.20.20.21, dest= 20.20.20.20,
    src_proxy= 50.50.50.0/255.255.255.0/0/0,
    dest_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x1E3A0B01(507120385), conn_id= 4, keysize= 0,
 flags= 0x4
*Mar  1 00:10:17.159: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/255.255.255.0/0/0,
    src_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x123616BF(305534655), conn_id= 5, keysize= 0,
 flags= 0x4
*Mar  1 00:10:17.167: IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 20.20.20.21, dest= 20.20.20.20,
    src_proxy= 50.50.50.0/255.255.255.0/0/0,
    dest_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x21080B90(554175376), conn_id= 6, keysize= 0,
 flags= 0x4
*Mar  1 00:10:17.175: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.21, sa_prot= 51,
    sa_spi= 0xFB2048(16457800),
    sa_trans= ah-sha-hmac , sa_conn_id= 3
*Mar  1 00:10:17.179: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.20, sa_prot= 51,
    sa_spi= 0x1E3A0B01(507120385),
    sa_trans= ah-sha-hmac , sa_conn_id= 4
```

```
*Mar  1 00:10:17.183: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.21, sa_prot= 50,
    sa_spi= 0x123616BF(305534655),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
*Mar  1 00:10:17.187: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.20, sa_prot= 50,
    sa_spi= 0x21080B90(554175376),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
*Mar  1 00:10:36.583: ISADB: reaper checking SA, conn_id = 1
wan2511#
```

샘플 2:ISAKMP:RSA 암호화 인증

이 시나리오에서는 공유 비밀 키가 생성되지 않습니다.각 라우터는 자체 RSA 키를 생성합니다.그런 다음 각 라우터가 피어의 RSA 공개 키를 구성해야 합니다.이는 수동 프로세스이며 확장 제한이 명확합니다.즉, 라우터는 보안 연결을 원하는 각 피어에 대해 공용 RSA 키를 가져야 합니다.

다음 문서는 이 샘플 구성에 대한 네트워크 다이어그램을 나타냅니다.



이 예에서는 각 라우터가 RSA 키 쌍을 생성하고(사용자가 생성한 RSA 개인 키는 표시되지 않음) 원격 피어의 공용 RSA 키를 구성합니다.

```
wan2511(config)#crypto key generate rsa
The name for the keys will be: wan2511.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
Generating RSA keys ...
[OK]

wan2511(config)#^Z
wan2511#
wan2511#show crypto key mypubkey rsa
% Key pair was generated at: 00:09:04 UTC Mar 1 1993
Key name: wan2511.cisco.com
Usage:    General Purpose Key
Key Data:
 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00E9007B E5CD7DC8
 6E1C0423 92044254 92C972AD 0CCE9796 86797EAA B6C4EFF0 0F0A5378 6AFAE43B
 3A2BD92F 98039DAC 08741E82 5D9053C4 D9CFABC1 AB54E0E2 BB020301 0001
wan2511#

wan2511(config)#crypto key pubkey-chain rsa
wan2511(config-pubkey-chain)#named-key wan2516.cisco.com
wan2511(config-pubkey-key)#key-string
Enter a public key as a hexidecimal number ....
```

```
wan2511(config-pubkey)#$86F70D 01010105 00034B00 30480241 00DC3DDC 59885F14
wan2511(config-pubkey)#$D918DE FC7ADB76 B0B9DD1A ABAF4884 009E758C 4064C699
wan2511(config-pubkey)#$220CB9 31E267F8 0259C640 F8DE4169 1F020301 0001
wan2511(config-pubkey)#quit
wan2511(config-pubkey-key)#^Z
wan2511#
wan2511#show crypto key pubkey-chain rsa
Key name: wan2516.cisco.com
Key usage: general purpose
Key source: manually entered
Key data:
 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00DC3DDC 59885F14
 1AB30DCB 794AB5C7 82D918DE FC7ADB76 B0B9DD1A ABAF4884 009E758C 4064C699
 3BC9D17E C47581DC 50220CB9 31E267F8 0259C640 F8DE4169 1F020301 0001


wan2511#
wan2511#write terminal
Building configuration...

Current configuration:
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname wan2511
!
enable password ww
!
no ip domain-lookup
ip host wan2516.cisco.com 20.20.20.20
ip domain-name cisco.com
!
crypto isakmp policy 1
 authentication rsa-encr
 group 2
 lifetime 240
crypto isakmp identity hostname
!
crypto ipsec transform-set auth2 ah-sha-hmac esp-des esp-sha-hmac
!
crypto map test 10 ipsec-isakmp
 set peer 20.20.20.20
 set transform-set auth2
 match address 133
!
crypto key pubkey-chain rsa
 named-key wan2516.cisco.com
  key-string
   305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00DC3DDC 59885F14
   1AB30DCB 794AB5C7 82D918DE FC7ADB76 B0B9DD1A ABAF4884 009E758C 4064C699
   3BC9D17E C47581DC 50220CB9 31E267F8 0259C640 F8DE4169 1F020301 0001
  quit
!
interface Ethernet0
 ip address 50.50.50.50 255.255.255.0
!
interface Serial0
 ip address 20.20.20.21 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 crypto map test
```

```
!
interface Serial1
 no ip address
 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.11.19.254
ip route 60.0.0.0 255.0.0.0 20.20.20.20
access-list 133 permit ip 50.50.50.0 0.0.0.255 60.60.60.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
 password ww
 login
line 1 6
 modem InOut
 transport input all
 speed 115200
 flowcontrol hardware
line 7 16
 autoselect ppp
 modem InOut
 transport input all
 speed 115200
 flowcontrol hardware
line aux 0
 login local
 modem InOut
 transport input all
 flowcontrol hardware
line vty 0 4
 password ww
 login
!
end



wan2511#
-----------------

wan2516(config)#crypto key generate rsa
The name for the keys will be: wan2516.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
Generating RSA keys ...
[OK]

wan2516#show crypto key mypubkey rsa
% Key pair was generated at: 00:06:35 UTC Mar 1 1993
Key name: wan2516.cisco.com
Usage:    General Purpose Key
Key Data:
 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00DC3DDC 59885F14
 1AB30DCB 794AB5C7 82D918DE FC7ADB76 B0B9DD1A ABAF4884 009E758C 4064C699
 3BC9D17E C47581DC 50220CB9 31E267F8 0259C640 F8DE4169 1F020301 0001
wan2516#

-------
wan2516(config)#crypto key exchange ?
  dss  Exchange DSS keys
```

```
-------

wan2516(config)#crypto key pubkey-chain rsa
wan2516(config-pubkey-chain)#named-key wan2511.cisco.com
wan2516(config-pubkey-key)#key-string
Enter a public key as a hexidecimal number ....

wan2516(config-pubkey)#$86F70D 01010105 00034B00 30480241 00E9007B E5CD7DC8
wan2516(config-pubkey)#$C972AD 0CCE9796 86797EAA B6C4EFF0 0F0A5378 6AFAE43B
wan2516(config-pubkey)#$741E82 5D9053C4 D9CFABC1 AB54E0E2 BB020301 0001
wan2516(config-pubkey)#quit
wan2516(config-pubkey-key)#^Z

wan2516#show crypto key pubkey rsa
Key name: wan2511.cisco.com
Key usage: general purpose
Key source: manually entered
Key data:
 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00E9007B E5CD7DC8
 6E1C0423 92044254 92C972AD 0CCE9796 86797EAA B6C4EFF0 0F0A5378 6AFAE43B
 3A2BD92F 98039DAC 08741E82 5D9053C4 D9CFABC1 AB54E0E2 BB020301 0001



wan2516#
------------------------
wan2516#write terminal
Building configuration...

Current configuration:
!
version 11.3
no service pad
service timestamps debug datetime msec
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname wan2516
!
enable password ww
!
no ip domain-lookup
ip host wan2511.cisco.com 20.20.20.21
ip domain-name cisco.com
!
crypto isakmp policy 1
 authentication rsa-encr
 group 2
 lifetime 240
crypto isakmp identity hostname
!
crypto ipsec transform-set auth2 ah-sha-hmac esp-des esp-sha-hmac
!
crypto map test 10 ipsec-isakmp
 set peer 20.20.20.21
 set transform-set auth2
 match address 144
!
crypto key pubkey-chain rsa
 named-key wan2511.cisco.com
  key-string
   305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00E9007B E5CD7DC8
   6E1C0423 92044254 92C972AD 0CCE9796 86797EAA B6C4EFF0 0F0A5378 6AFAE43B
```

```
   3A2BD92F 98039DAC 08741E82 5D9053C4 D9CFABC1 AB54E0E2 BB020301 0001
  quit
!
hub ether 0 1
 link-test
 auto-polarity
!
interface Loopback0
 ip address 70.70.70.1 255.255.255.0
 no ip route-cache
 no ip mroute-cache
!
interface Ethernet0
 ip address 60.60.60.60 255.255.255.0
!
interface Serial0
 ip address 20.20.20.20 255.255.255.0
 encapsulation ppp
 clockrate 2000000
 crypto map test
!
interface Serial1
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
!
interface BRI0
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
!
ip default-gateway 20.20.20.21
ip classless
ip route 0.0.0.0 0.0.0.0 20.20.20.21
access-list 144 permit ip 60.60.60.0 0.0.0.255 50.50.50.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
 password ww
 login
line aux 0
 password ww
 login
 modem InOut
 transport input all
 flowcontrol hardware
line vty 0 4
 password ww
 login
!
end

wan2516#

--------------- RSA-enc missing RSA Keys ---------

*Mar  1 00:02:51.147: ISAKMP: No cert, and no keys (public or pre-shared)
        with remote peer 20.20.20.21
*Mar  1 00:02:51.151: ISAKMP: No cert, and no keys (public or pre-shared)
        with remote peer 20.20.20.21

--------------- RSA-enc good connection -----------------
```

```
wan2511#
*Mar  1 00:21:46.375: ISAKMP (1): processing SA payload.
message ID = 0
*Mar  1 00:21:46.379: ISAKMP (1): Checking ISAKMP
transform 1 against
      priority 1 policy
*Mar  1 00:21:46.379: ISAKMP:      encryption DES-CBC
*Mar  1 00:21:46.379: ISAKMP:      hash SHA
*Mar  1 00:21:46.383: ISAKMP:      default group 2
*Mar  1 00:21:46.383: ISAKMP:      auth RSA encr
*Mar  1 00:21:46.383: ISAKMP:      life type in seconds
*Mar  1 00:21:46.387: ISAKMP:      life duration (basic)
of 240
*Mar  1 00:21:46.387: ISAKMP (1): atts are acceptable.
Next payload is 0
*Mar  1 00:21:46.391: Crypto engine 0: generate alg param

*Mar  1 00:21:55.159: CRYPTO_ENGINE: Dh phase 1 status: 0
*Mar  1 00:21:55.163: CRYPTO: DH gen phase 1 status for
conn_id 1 slot 0:OK
*Mar  1 00:21:55.167: ISAKMP (1): Unable to get router
cert to find DN!
*Mar  1 00:21:55.171: ISAKMP (1): SA is doing RSA
encryption authentication
*Mar  1 00:22:04.351: ISAKMP (1): processing KE payload.
message ID = 0
*Mar  1 00:22:04.351: Crypto engine 0: generate alg param

*Mar  1 00:22:14.767: CRYPTO: DH gen phase 2 status for
conn_id 1 slot 0:OK
*Mar  1 00:22:14.771: ISAKMP (1): processing ID payload.
message ID = 0
*Mar  1 00:22:14.775: Crypto engine 0: RSA decrypt
with private key
*Mar  1 00:22:15.967: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:16.167: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:16.367: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:16.579: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:16.787: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:16.987: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:17.215: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:17.431: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:17.539: CRYPTO: RSA private decrypt
finished with status=OK
*Mar  1 00:22:17.543: ISAKMP (1): processing NONCE
payload. message ID = 0
*Mar  1 00:22:17.543: Crypto engine 0: RSA decrypt
with private key
*Mar  1 00:22:18.735: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:18.947: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:19.155: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:19.359: CRYPTO_ENGINE: key process
suspended and continued
```

```
*Mar  1 00:22:19.567: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:19.767: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:19.975: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:20.223: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:20.335: CRYPTO: RSA private decrypt
finished with status=OK
*Mar  1 00:22:20.347: Crypto engine 0: create ISAKMP
SKEYID for conn id 1
*Mar  1 00:22:20.363: ISAKMP (1): SKEYID state generated
*Mar  1 00:22:20.367: Crypto engine 0: RSA encrypt
with public key
*Mar  1 00:22:20.567: CRYPTO: RSA public encrypt
finished with status=OK
*Mar  1 00:22:20.571: Crypto engine 0: RSA encrypt
with public key
*Mar  1 00:22:20.767: CRYPTO: RSA public encrypt
finished with status=OK
*Mar  1 00:22:20.775: ISAKMP (1): processing KE
payload. message ID = 0
*Mar  1 00:22:20.775: ISAKMP (1): processing ID
payload. message ID = 0
*Mar  1 00:22:20.779: Crypto engine 0: RSA decrypt
with private key
*Mar  1 00:22:21.959: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:22.187: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:22.399: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:22.599: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:22.811: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:23.019: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:23.223: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:23.471: CRYPTO_ENGINE: key process
suspended and continued
*Mar  1 00:22:23.583: CRYPTO: RSA private decrypt
finished with status=OK
*Mar  1 00:22:23.583: ISAKMP (1): processing NONCE
payload. message ID = 0
%CRYPTO-6-IKMP_AUTH_FAIL: Authentication method 4
failed with host 20.20.20.20
%CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main
mode failed with peer
  at 20.20.20.20
*Mar  1 00:22:36.955: ISAKMP (1): processing HASH
payload. message ID = 0
*Mar  1 00:22:36.959: generate hmac context for conn id 1
*Mar  1 00:22:36.971: ISAKMP (1): SA has been authenticated
*Mar  1 00:22:36.975: generate hmac context for conn id 1
*Mar  1 00:22:37.311: generate hmac context for conn id 1
*Mar  1 00:22:37.319: ISAKMP (1): processing SA payload.
message ID = -114148384
*Mar  1 00:22:37.319: ISAKMP (1): Checking IPSec proposal 1
*Mar  1 00:22:37.323: ISAKMP: transform 1, AH_SHA_HMAC
*Mar  1 00:22:37.323: ISAKMP: attributes in transform:
*Mar  1 00:22:37.327: ISAKMP: encaps is 1
```

```
*Mar  1 00:22:37.327: ISAKMP: SA life type in seconds
*Mar  1 00:22:37.327: ISAKMP: SA life duration (basic) of 3600
*Mar  1 00:22:37.331: ISAKMP: SA life type in kilobytes
*Mar  1 00:22:37.331: ISAKMP: SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar  1 00:22:37.335: ISAKMP (1): atts are acceptable.
*Mar  1 00:22:37.335: ISAKMP (1): Checking IPSec proposal 1
*Mar  1 00:22:37.339: ISAKMP: transform 1, ESP_DES
*Mar  1 00:22:37.339: ISAKMP: attributes in transform:
*Mar  1 00:22:37.339: ISAKMP: encaps is 1
*Mar  1 00:22:37.343: ISAKMP: SA life type in seconds
*Mar  1 00:22:37.343: ISAKMP: SA life duration (basic) of 3600
*Mar  1 00:22:37.347: ISAKMP: SA life type in kilobytes
*Mar  1 00:22:37.347: ISAKMP: SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar  1 00:22:37.351: ISAKMP: HMAC algorithm is SHA
*Mar  1 00:22:37.351: ISAKMP (1): atts are acceptable.
*Mar  1 00:22:37.355: IPSEC(validate_proposal_request):
proposal part #1,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/0.0.0.0/0/0,
    src_proxy= 60.60.60.0/0.0.0.16/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar  1 00:22:37.363: IPSEC(validate_proposal_request):
proposal part #2,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/0.0.0.0/0/0,
    src_proxy= 60.60.60.0/0.0.0.16/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar  1 00:22:37.371: ISAKMP (1): processing NONCE payload.
      message ID = -114148384
*Mar  1 00:22:37.375: ISAKMP (1): processing ID payload.
message ID = -114148384
*Mar  1 00:22:37.375: ISAKMP (1): processing ID payload.
 message ID = -114148384
*Mar  1 00:22:37.379: IPSEC(key_engine): got a queue event...
*Mar  1 00:22:37.383: IPSEC(spi_response): getting spi
531040311 for SA
        from 20.20.20.20     to 20.20.20.21 for prot 2
*Mar  1 00:22:37.387: IPSEC(spi_response): getting spi
220210147 for SA
        from 20.20.20.20     to 20.20.20.21     for prot 3
*Mar  1 00:22:37.639: generate hmac context for conn id 1
*Mar  1 00:22:37.931: generate hmac context for conn id 1
*Mar  1 00:22:37.975: ISAKMP (1): Creating IPSec SAs
*Mar  1 00:22:37.975: inbound SA from 20.20.20.20
   to 20.20.20.21
        (proxy 60.60.60.0      to 50.50.50.0     )
*Mar  1 00:22:37.979:  has spi 531040311 and conn_id 2 and flags 4
*Mar  1 00:22:37.979:   lifetime of 3600 seconds
*Mar  1 00:22:37.983:    lifetime of 4608000 kilobytes
*Mar  1 00:22:37.983:  outbound SA from 20.20.20.21
 to 20.20.20.20
        (proxy 50.50.50.0 to 60.60.60.0     )
*Mar  1 00:22:37.987: has spi 125043658 and
conn_id 3 and flags 4
*Mar  1 00:22:37.987: lifetime of 3600 seconds
*Mar  1 00:22:37.991: lifetime of 4608000 kilobytes
*Mar  1 00:22:37.991: ISAKMP (1): Creating IPSec SAs
*Mar  1 00:22:37.991: inbound SA from 20.20.20.20 to 20.20.20.21
```

```
        (proxy 60.60.60.0 to 50.50.50.0     )
*Mar  1 00:22:37.995: has spi 220210147 and conn_id 4 and flags 4
*Mar  1 00:22:37.999: lifetime of 3600 seconds
*Mar  1 00:22:37.999: lifetime of 4608000 kilobytes
*Mar  1 00:22:38.003: outbound SA from 20.20.20.21 to 20.20.20.20
        (proxy 50.50.50.0      to 60.60.60.0     )
*Mar  1 00:22:38.003: has spi 299247102 and
conn_id 5 and flags 4
*Mar  1 00:22:38.007: lifetime of 3600 seconds
*Mar  1 00:22:38.007: lifetime of 4608000 kilobytes
*Mar  1 00:22:38.011: IPSEC(key_engine): got a queue event...
*Mar  1 00:22:38.015: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/255.255.255.0/0/0,
    src_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x1FA70837(531040311), conn_id= 2, keysize= 0, flags= 0x4
*Mar  1 00:22:38.023: IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 20.20.20.21, dest= 20.20.20.20,
    src_proxy= 50.50.50.0/255.255.255.0/0/0,
    dest_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x77403CA(125043658), conn_id= 3, keysize= 0, flags= 0x4
*Mar  1 00:22:38.031: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/255.255.255.0/0/0,
    src_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xD2023E3(220210147), conn_id= 4, keysize= 0, flags= 0x4
*Mar  1 00:22:38.039: IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 20.20.20.21, dest= 20.20.20.20,
    src_proxy= 50.50.50.0/255.255.255.0/0/0,
    dest_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x11D625FE(299247102), conn_id= 5, keysize= 0, flags= 0x4
*Mar  1 00:22:38.047: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.21, sa_prot= 51,
    sa_spi= 0x1FA70837(531040311),
    sa_trans= ah-sha-hmac , sa_conn_id= 2
*Mar  1 00:22:38.051: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.20, sa_prot= 51,
    sa_spi= 0x77403CA(125043658),
    sa_trans= ah-sha-hmac , sa_conn_id= 3
*Mar  1 00:22:38.055: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.21, sa_prot= 50,
    sa_spi= 0xD2023E3(220210147),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 4
*Mar  1 00:22:38.063: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.20, sa_prot= 50,
    sa_spi= 0x11D625FE(299247102),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
wan2511#

----------- RSA-ENC ISAKMP debugs good connection ---
wan2511#
*Mar  1 00:27:23.279: ISAKMP (6): processing SA payload.
 message ID = 0
*Mar  1 00:27:23.279: ISAKMP (6): Checking ISAKMP
 transform 1 against
      priority 1 policy
```

```
*Mar  1 00:27:23.283: ISAKMP: encryption DES-CBC
*Mar  1 00:27:23.283: ISAKMP: hash SHA
*Mar  1 00:27:23.283: ISAKMP: default group 2
*Mar  1 00:27:23.287: ISAKMP: auth RSA encr
*Mar  1 00:27:23.287: ISAKMP: life type in seconds
*Mar  1 00:27:23.287: ISAKMP: life duration (basic) of 240
*Mar  1 00:27:23.291: ISAKMP (6): atts are acceptable.
Next payload is 0
*Mar  1 00:27:32.055: ISAKMP (6): Unable to get
router cert to find DN!
*Mar  1 00:27:32.055: ISAKMP (6): SA is doing RSA
encryption authentication
*Mar  1 00:27:41.183: ISAKMP (6): processing KE payload.
message ID = 0
*Mar  1 00:27:51.779: ISAKMP (6): processing ID payload.
 message ID = 0
*Mar  1 00:27:54.507: ISAKMP (6): processing NONCE payload.
 message ID = 0
*Mar  1 00:27:57.239: ISAKMP (6): SKEYID state generated
*Mar  1 00:27:57.627: ISAKMP (6): processing KE payload.
 message ID = 0
*Mar  1 00:27:57.631: ISAKMP (6): processing ID payload.
 message ID = 0
*Mar  1 00:28:00.371: ISAKMP (6): processing NONCE payload.

 message ID = 0
%CRYPTO-6-IKMP_AUTH_FAIL: Authentication method 4 failed
with host 20.20.20.20
%CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main mode failed
 with peer at 20.20.20.20
*Mar  1 00:28:13.587: ISAKMP (6): processing HASH payload.
 message ID = 0
*Mar  1 00:28:13.599: ISAKMP (6): SA has been authenticated
*Mar  1 00:28:13.939: ISAKMP (6): processing SA payload.
 message ID = -161552401
*Mar  1 00:28:13.943: ISAKMP (6): Checking IPSec proposal 1
*Mar  1 00:28:13.943: ISAKMP: transform 1, AH_SHA_HMAC
*Mar  1 00:28:13.943: ISAKMP:   attributes in transform:
*Mar  1 00:28:13.947: ISAKMP: encaps is 1
*Mar  1 00:28:13.947: ISAKMP: SA life type in seconds
*Mar  1 00:28:13.947: ISAKMP: SA life duration (basic) of 3600
*Mar  1 00:28:13.951: ISAKMP: SA life type in kilobytes
*Mar  1 00:28:13.951: ISAKMP: SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar  1 00:28:13.955: ISAKMP (6): atts are acceptable.
*Mar  1 00:28:13.959: ISAKMP (6): Checking IPSec proposal 1
*Mar  1 00:28:13.959: ISAKMP: transform 1, ESP_DES
*Mar  1 00:28:13.959: ISAKMP: attributes in transform:
*Mar  1 00:28:13.963: ISAKMP: encaps is 1
*Mar  1 00:28:13.963: ISAKMP: SA life type in seconds
*Mar  1 00:28:13.963: ISAKMP: SA life duration (basic) of 3600
*Mar  1 00:28:13.967: ISAKMP: SA life type in kilobytes
*Mar  1 00:28:13.967: ISAKMP: SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar  1 00:28:13.971: ISAKMP:      HMAC algorithm is SHA
*Mar  1 00:28:13.971: ISAKMP (6): atts are acceptable.
*Mar  1 00:28:13.975: ISAKMP (6): processing NONCE payload.
 message ID = -161552401
*Mar  1 00:28:13.979: ISAKMP (6): processing ID payload.
 message ID = -161552401
*Mar  1 00:28:13.979: ISAKMP (6): processing ID payload.
 message ID = -161552401
*Mar  1 00:28:14.391: ISAKMP (6): Creating IPSec SAs
*Mar  1 00:28:14.391: inbound SA from 20.20.20.20 to 20.20.20.21
```

```
        (proxy 60.60.60.0 to 50.50.50.0     )
*Mar  1 00:28:14.395: has spi 437593758 and conn_id 7 and flags 4
*Mar  1 00:28:14.399: lifetime of 3600 seconds
*Mar  1 00:28:14.399: lifetime of 4608000 kilobytes
*Mar  1 00:28:14.403: outbound SA from 20.20.20.21 to 20.20.20.20
        (proxy 50.50.50.0 to 60.60.60.0     )
*Mar  1 00:28:14.403: has spi 411835612 and conn_id 8 and flags 4
*Mar  1 00:28:14.407: lifetime of 3600 seconds
*Mar  1 00:28:14.407: lifetime of 4608000 kilobytes
*Mar  1 00:28:14.411: ISAKMP (6): Creating IPSec SAs
*Mar  1 00:28:14.411: inbound SA from 20.20.20.20 to 20.20.20.21
        (proxy 60.60.60.0 to 50.50.50.0     )
*Mar  1 00:28:14.415: has spi 216990519 and conn_id 9 and flags 4
*Mar  1 00:28:14.415: lifetime of 3600 seconds
*Mar  1 00:28:14.419: lifetime of 4608000 kilobytes
*Mar  1 00:28:14.419: outbound SA from 20.20.20.21 to 20.20.20.20
        (proxy 50.50.50.0 to 60.60.60.0     )
*Mar  1 00:28:14.423: has spi 108733569 and conn_id 10 and flags 4
*Mar  1 00:28:14.423: lifetime of 3600 seconds
*Mar  1 00:28:14.427: lifetime of 4608000 kilobytes
wan2511#

-------------------------- RSA-enc IPSEC debug -------
wan2511#
*Mar  1 00:30:32.155: ISAKMP (11): Unable to get
router cert to find DN!
wan2511#show debug
Cryptographic Subsystem:
  Crypto IPSEC debugging is on
wan2511#
wan2511#
wan2511#
wan2511#
%CRYPTO-6-IKMP_AUTH_FAIL: Authentication method
4 failed with host 20.20.20.20
%CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main
mode failed with peer at
20.20.20.20
*Mar  1 00:31:13.931: IPSEC(validate_proposal_request):
 proposal part #1,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/0.0.0.0/0/0,
    src_proxy= 60.60.60.0/0.0.0.16/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar  1 00:31:13.935: IPSEC(validate_proposal_request):
 proposal part #2,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/0.0.0.0/0/0,
    src_proxy= 60.60.60.0/0.0.0.16/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar  1 00:31:13.947: IPSEC(key_engine): got a queue event...
*Mar  1 00:31:13.951: IPSEC(spi_response): getting
spi 436869446 for SA
        from 20.20.20.20     to 20.20.20.21 for prot 2
*Mar  1 00:31:13.955: IPSEC(spi_response): getting
 spi 285609740 for SA
        from 20.20.20.20     to 20.20.20.21 for prot 3
*Mar  1 00:31:14.367: IPSEC(key_engine): got a queue event...
*Mar  1 00:31:14.367: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
```

```
    dest_proxy= 50.50.50.0/255.255.255.0/0/0,
    src_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x1A0A1946(436869446), conn_id= 12, keysize= 0,
flags= 0x4
*Mar  1 00:31:14.375: IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 20.20.20.21, dest= 20.20.20.20,
    src_proxy= 50.50.50.0/255.255.255.0/0/0,
    dest_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x2C40706(46401286), conn_id= 13, keysize= 0,
flags= 0x4
*Mar  1 00:31:14.383: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/255.255.255.0/0/0,
    src_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x11060F0C(285609740), conn_id= 14, keysize= 0,
flags= 0x4
*Mar  1 00:31:14.391: IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 20.20.20.21, dest= 20.20.20.20,
    src_proxy= 50.50.50.0/255.255.255.0/0/0,
    dest_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x12881335(310907701), conn_id= 15, keysize= 0,
 flags= 0x4
*Mar  1 00:31:14.399: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.21, sa_prot= 51,
    sa_spi= 0x1A0A1946(436869446),
    sa_trans= ah-sha-hmac , sa_conn_id= 12
*Mar  1 00:31:14.407: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.20, sa_prot= 51,
    sa_spi= 0x2C40706(46401286),
    sa_trans= ah-sha-hmac , sa_conn_id= 13
*Mar  1 00:31:14.411: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.21, sa_prot= 50,
    sa_spi= 0x11060F0C(285609740),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 14
*Mar  1 00:31:14.415: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.20, sa_prot= 50,
    sa_spi= 0x12881335(310907701),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 15
wan2511#
```

샘플 3:ISAKMP:RSA-SIG 인증/CA

이 예에서는 CA 서버를 사용해야 하는 RSA 서명을 사용합니다.각 피어는 CA 서버에서 인증서를 가져옵니다(일반적으로 인증서를 발급하도록 구성된 워크스테이션). 두 피어에 유효한 CA 인증서가 있으면 ISAKMP 협상의 일부로 RSA 공개 키를 자동으로 교환합니다.이 시나리오에서 필요한 모든 것은 각 피어가 CA에 등록하고 인증서를 획득하기 위한 것입니다.피어는 더 이상 네트워크에 있는 모든 피어의 공용 RSA 키를 유지할 필요가 없습니다.

또한 ISAKMP 정책은 다음과 같은 기본 정책을 사용하고 있으므로 지정되지 않습니다.

```
lab-isdn1#show crypto isakmp policy
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
```

```
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
```

먼저 CA 서버의 호스트 이름을 정의하고 RSA 키를 생성합니다.

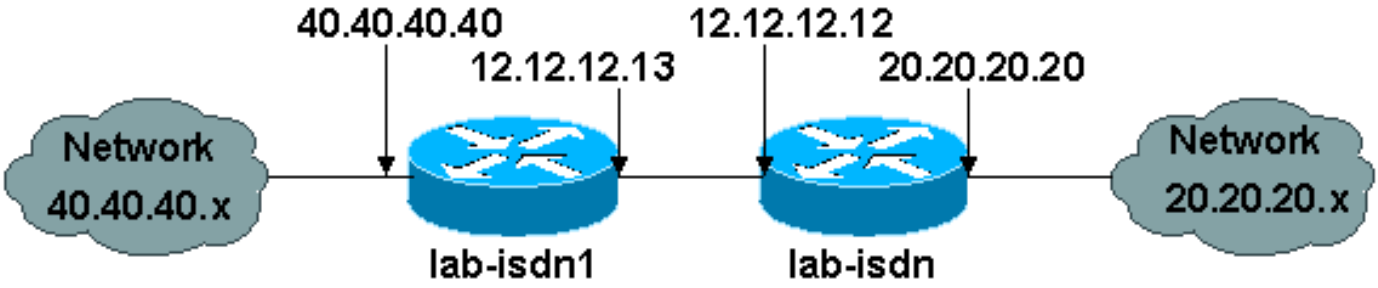
```
test1-isdn(config)#ip host cert-author 10.19.54.46
test1-isdn(config)#crypto key gen rsa usage
The name for the keys will be: test1-isdn.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  Signature Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
Generating RSA keys ...
[OK]
Choose the size of the key modulus in the range of 360 to 2048 for your
  Encryption Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
Generating RSA keys ...
[OK]
```

다음으로, CA 컨피그레이션은 "test1-isdn-ultra"라는 태그로 정의되고 CA 이름 URL을 정의합니다.그런 다음 CA 서버로 인증하고 인증서를 가져옵니다.마지막으로, 사용할 수 있는 "사용 가능한" 인증서를 받았는지 확인합니다.

```
test1-isdn(config)#crypto ca identity test1-isdn-ultra
test1-isdn(ca-identity)#enrollment url http://cert-author
test1-isdn(ca-identity)#crl optional
test1-isdn(ca-identity)#exit

---------------------------------
test1-isdn(config)#crypto ca authenticate test1-isdn-ultra
Certificate has the following attributes:
Fingerprint: 71CA5A98 78828EF8 4987BA95 57830E5F
% Do you accept this certificate? [yes/no]: yes
Apr  3 14:08:56.329: CRYPTO_PKI: http connection opened
Apr  3 14:08:56.595: CRYPTO__PKI: All enrollment requests completed.
Apr  3 14:08:56.599: CRYPTO_PKI: transaction GetCACert completed
Apr  3 14:08:56.599: CRYPTO_PKI: CA certificate received
test1-isdn(config)#

---------------------------------
test1-isdn(config)#crypto ca enroll test1-isdn-ultra
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will be: test1-isdn.cisco.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: 04922418
% Include an IP address in the subject name? [yes/no]: yes
Interface: bri0
Request certificate from CA? [yes/no]: yes
```

```
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.

----------------- status: pending ---------------

test1-isdn#show crypto ca certificate
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7169BEE31B821DFE4B3A338E5F
  Key Usage: Not Set

Certificate
  Subject Name
    Name: test1-isdn.cisco.com
    IP Address: 10.18.117.189
    Serial Number: 04922418
  Status: Pending
  Key Usage: Signature
    Fingerprint:  B1566229 472B1DDB 01A072C0 8202A985 00000000

Certificate
  Subject Name
    Name: test1-isdn.cisco.com
    IP Address: 10.18.117.189
    Serial Number: 04922418
  Status: Pending
  Key Usage: Encryption
    Fingerprint:  1EA39C07 D1B26FC7 7AD08BF4 ACA3AABD 00000000


----------------- status: available ---------------
test1-isdn#show crypto ca certificate
Certificate
  Subject Name
    Name: test1-isdn.cisco.com
    Serial Number: 04922418
  Status: Available
  Certificate Serial Number: 1BAFCBCA71F0434B59D192FAFB37D376
  Key Usage: Encryption

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7169BEE31B821DFE4B3A338E5F
  Key Usage: Not Set

Certificate
  Subject Name
    Name: test1-isdn.cisco.com
    Serial Number: 04922418
  Status: Available
  Certificate Serial Number: 4B39EE2866814279CBA7534496DE1D99
  Key Usage: Signature

test1-isdn#
```

다음 그림은 이 샘플 컨피그레이션의 네트워크 다이어그램을 나타냅니다.



아래 샘플 컨피그레이션은 이전에 CA 인증서를 취득한 두 Cisco 1600 라우터에서 가져온 것이며 인증 정책으로 "rsa-sig"를 사용하여 ISAKMP를 수행하려는 것입니다.두 원격 이더넷 LAN 간의 트래픽만 암호화됩니다.

```
lab-isdn1#write terminal
Building configuration...

Current configuration:
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname lab-isdn1
!
enable secret 5 $1$VdPY$uA/BIVeEm9UAFEm.PPJFc.
!
username lab-isdn password 0 cisco
ip host ciscoca-ultra 171.69.54.46
ip host lab-isdn 12.12.12.12
ip domain-name cisco.com
ip name-server 171.68.10.70
ip name-server 171.68.122.99
isdn switch-type basic-ni1
!
crypto ipsec transform-set mypolicy ah-sha-hmac esp-des esp-sha-hmac
!
crypto map test 10 ipsec-isakmp
 set peer 12.12.12.12
 set transform-set mypolicy
 match address 144
!
crypto ca identity bubba
 enrollment url http://ciscoca-ultra
 crl optional
crypto ca certificate chain bubba
 certificate 3E1ED472BDA2CE0163FB6B0B004E5EEE
  308201BC 30820166 A0030201 0202103E
 1ED472BD A2CE0163 FB6B0B00 4E5EEE30
  0D06092A 864886F7 0D010104 05003042
  31163014 06035504 0A130D43 6973636F
  20537973 74656D73 3110300E 06035504
  0B130744 65767465 73743116 30140603
  55040313 0D434953 434F4341 2D554C54
  5241301E 170D3938 30343038 30303030
  30305A17 0D393930 34303832 33353935
  395A303B 31273025 06092A86 4886F70D
  01090216 18737461 6E6E6F75 732D6973
  646E312E 63697363 6F2E636F 6D311030
```

```
 0E060355 04051307 35363739 39383730
 5C300D06 092A8648 86F70D01 01010500
 034B0030 48024100 D2D125FF BBFC6E56
 93CB4385 5473C165 BC7CCAF6 45C35BED
 554BAA0B 119AFA6F 0853F574 5E0B8492
 2E39B5FA 84C4DD05 C19AA625 8184395C
 6CBC7FA4 614F6177 02030100 01A33F30
 3D300B06 03551D0F 04040302 05203023
 0603551D 11041C30 1A821873 74616E6E
 6F75732D 6973646E 312E6369 73636F2E
 636F6D30 09060355 1D130402 3000300D
 06092A86 4886F70D 01010405 00034100
 04AF83B8 FE95F5D9 9C07C105 F1E88F1A
 9320CE7D 0FA540CF 44C77829 FC85C94B
 8CB4CA32 85FF9655 8E47AC9A B9D6BF1A
 0C4846DE 5CB07C8E A32038EC 8AFD161A
 quit
certificate ca 3051DF7169BEE31B821DFE4B3A338E5F
 30820182 3082012C A0030201 02021030
 51DF7169 BEE31B82 1DFE4B3A 338E5F30
 0D06092A 864886F7 0D010104 05003042
 31163014 06035504 0A130D43 6973636F
 20537973 74656D73 3110300E 06035504
 0B130744 65767465 73743116 30140603
 55040313 0D434953 434F4341 2D554C54
 5241301E 170D3937 31323032 30313036
 32385A17 0D393831 32303230 31303632
 385A3042 31163014 06035504 0A130D43
 6973636F 20537973 74656D73 3110300E
 06035504 0B130744 65767465 73743116
 30140603 55040313 0D434953 434F4341
 2D554C54 5241305C 300D0609 2A864886
 F70D0101 01050003 4B003048 024100C1
 B69D7BF6 34E4EE28 A84E0DC6 FCA4DEA8
 04D89E50 C5EBE862 39D51890 D0D4B732
 678BDBF2 80801430 E5E56E7C C126E2DD
 DBE9695A DF8E5BA7 E67BAE87 29375302
 03010001 300D0609 2A864886 F70D0101
 04050003 410035AA 82B5A406 32489413
 A7FF9A9A E349E5B4 74615E05 058BA3CE
 7C5F00B4 019552A5 E892D2A3 86763A1F
 2852297F C68EECE1 F41E9A7B 2F38D02A
 B1D2F817 3F7B
 quit
certificate 503968D890F7D409475B7280162754D2
 308201BC 30820166 A0030201 02021050
 3968D890 F7D40947 5B728016 2754D230
 0D06092A 864886F7 0D010104 05003042
 31163014 06035504 0A130D43 6973636F
 20537973 74656D73 3110300E 06035504
 0B130744 65767465 73743116 30140603
 55040313 0D434953 434F4341 2D554C54
 5241301E 170D3938 30343038 30303030
 30305A17 0D393930 34303832 33353935
 395A303B 31273025 06092A86 4886F70D
 01090216 18737461 6E6E6F75 732D6973
 646E312E 63697363 6F2E636F 6D311030
 0E060355 04051307 35363739 39383730
 5C300D06 092A8648 86F70D01 01010500
 034B0030 48024100 BECE2D8C B32E6B09
 0ADE0D46 AF8D4A1F 37850034 35D0C729
 3BF91518 0C9E4CF8 1A6A43AE E4F04687
 B8E2859D 33D5CE04 2E5DDEA6 3DA54A31
 2AD4255A 756014CB 02030100 01A33F30
```

```
  3D300B06 03551D0F 04040302 07803023
  0603551D 11041C30 1A821873 74616E6E
  6F75732D 6973646E 312E6369 73636F2E
  636F6D30 09060355 1D130402 3000300D
  06092A86 4886F70D 01010405 00034100
  B3AF6E71 CBD9AEDD A4711B71 6897F2CE
  D669A23A EE47B92B B2BE942A 422DF4A5
  7ACB9433 BD17EC7A BB3721EC E7D1175F
  5C62BC58 C409F805 19691FBD FD925138
  quit
!
interface Ethernet0
 ip address 40.40.40.40 255.255.255.0
 no ip mroute-cache
!
interface BRI0
 ip address 12.12.12.13 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 dialer idle-timeout 99999
 dialer map ip 12.12.12.12 name lab-isdn 4724171
 dialer hold-queue 40
 dialer-group 1
 isdn spid1 919472411800 4724118
 isdn spid2 919472411901 4724119
 ppp authentication chap
 crypto map test
!
ip classless
ip route 0.0.0.0 0.0.0.0 12.12.12.12
access-list 144 permit ip 40.40.40.0 0.0.0.255 20.20.20.0 0.0.0.255
dialer-list 1 protocol ip permit
!
line con 0
 exec-timeout 0 0
line vty 0 4
 password ww
 login
!
end

lab-isdn1#

------------------

lab-isdn#write terminal
Building configuration...

Current configuration:
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname lab-isdn
!
enable secret 5 $1$oNe1$wDbhBdcN6x9Y5gfuMjqh10
!
username lab-isdn1 password 0 cisco
ip host ciscoca-ultra 171.69.54.46
ip host lab-isdn1 12.12.12.13
ip domain-name cisco.com
```

```
ip name-server 171.68.10.70
ip name-server 171.68.122.99
isdn switch-type basic-ni1
!
crypto ipsec transform-set mypolicy ah-sha-hmac
 esp-des esp-sha-hmac
!
crypto map test 10 ipsec-isakmp
 set peer 12.12.12.13
 set transform-set mypolicy
 match address 133
!
crypto ca identity lab
 enrollment url http://ciscoca-ultra
 crl optional
crypto ca certificate chain lab
 certificate 44FC6C531FC3446927E4EE307A806B20
  308201E0 3082018A A0030201 02021044
  FC6C531F C3446927 E4EE307A 806B2030
  0D06092A 864886F7 0D010104 05003042
  31163014 06035504 0A130D43 6973636F
  20537973 74656D73 3110300E 06035504
  0B130744 65767465 73743116 30140603
  55040313 0D434953 434F4341 2D554C54
  5241301E 170D3938 30343038 30303030
  30305A17 0D393930 34303832 33353935
  395A305A 31263024 06092A86 4886F70D
  01090216 17737461 6E6E6F75 732D6973
  646E2E63 6973636F 2E636F6D 311E301C
  060A2B06 0104012A 020B0201 130E3137
  312E3638 2E313137 2E313839 3110300E
  06035504 05130735 36373939 3139305C
  300D0609 2A864886 F70D0101 01050003
  4B003048 024100B8 F4A17A70 FAB5C2E3
  39186513 486779C7 61EF0AC1 3B6CFF83
  810E6D28 B3E4C034 CD803CFF 5158C270
  28FEBCDE CB6EF2D4 83BDD9B3 EAF915DB
  78266E96 500CD702 03010001 A3443042
  300B0603 551D0F04 04030205 20302806
  03551D11 0421301F 82177374 616E6E6F
  75732D69 73646E2E 63697363 6F2E636F
  6D8704AB 4475BD30 09060355 1D130402
  3000300D 06092A86 4886F70D 01010405
  00034100 BF65B931 0F960195 ABDD41D5
  622743D9 C12B5499 B3A8EB30 5005E6CC
  7FDF7C5B 51D13EB8 D46187E5 A1E7F711
  AEB7B33B AA4C6728 7A4BA692 00A44A05 C5CF973F
  quit
 certificate ca 3051DF7169BEE31B821DFE4B3A338E5F
  30820182 3082012C A0030201 02021030
  51DF7169 BEE31B82 1DFE4B3A 338E5F30
  0D06092A 864886F7 0D010104 05003042
  31163014 06035504 0A130D43 6973636F
  20537973 74656D73 3110300E 06035504
  0B130744 65767465 73743116 30140603
  55040313 0D434953 434F4341 2D554C54
  5241301E 170D3937 31323032 30313036
  32385A17 0D393831 32303230 31303632
  385A3042 31163014 06035504 0A130D43
  6973636F 20537973 74656D73 3110300E
  06035504 0B130744 65767465 73743116
  30140603 55040313 0D434953 434F4341
  2D554C54 5241305C 300D0609 2A864886
  F70D0101 01050003 4B003048 024100C1
```

```
  B69D7BF6 34E4EE28 A84E0DC6 FCA4DEA8
  04D89E50 C5EBE862 39D51890 D0D4B732
  678BDBF2 80801430 E5E56E7C C126E2DD
  DBE9695A DF8E5BA7 E67BAE87 29375302
  03010001 300D0609 2A864886 F70D0101
  04050003 410035AA 82B5A406 32489413
  A7FF9A9A E349E5B4 74615E05 058BA3CE
  7C5F00B4 019552A5 E892D2A3 86763A1F
  2852297F C68EECE1 F41E9A7B 2F38D02A
  B1D2F817 3F7B
  quit
 certificate 52A46D5D10B18A6F51E6BC735A36508C
  308201E0 3082018A A0030201 02021052
  A46D5D10 B18A6F51 E6BC735A 36508C30
  0D06092A 864886F7 0D010104 05003042
  31163014 06035504 0A130D43 6973636F
  20537973 74656D73 3110300E 06035504
  0B130744 65767465 73743116 30140603
  55040313 0D434953 434F4341 2D554C54
  5241301E 170D3938 30343038 30303030
  30305A17 0D393930 34303832 33353935
  395A305A 31263024 06092A86 4886F70D
  01090216 17737461 6E6E6F75 732D6973
  646E2E63 6973636F 2E636F6D 311E301C
  060A2B06 0104012A 020B0201 130E3137
  312E3638 2E313137 2E313839 3110300E
  06035504 05130735 36373939 3139305C
  300D0609 2A864886 F70D0101 01050003
  4B003048 024100D7 71AD5672 B487A019
  5ECD1954 6F919A3A 6270102E 5A9FF4DC
  7A608480 FB27A181 715335F4 399D3E57
  7F72B323 BF0620AB 60C371CF 4389BA4F
  C60EE6EA 21E06302 03010001 A3443042
  300B0603 551D0F04 04030207 80302806
  03551D11 0421301F 82177374 616E6E6F
  75732D69 73646E2E 63697363 6F2E636F
  6D8704AB 4475BD30 09060355 1D130402
  3000300D 06092A86 4886F70D 01010405
  00034100 8AD45375 54803CF3 013829A8
  8DB225A8 25342160 94546F3C 4094BBA3
  F2F5A378 97E2F06F DCFFC509 A07B930A
  FBE6C3CA E1FC7FD9 1E69B872 C402E62A A8814C09
  quit
!
interface Ethernet0
 ip address 20.20.20.20 255.255.255.0
!
interface BRI0
 description bri to rtp
 ip address 12.12.12.12 255.255.255.0
 no ip proxy-arp
 encapsulation ppp
 no ip mroute-cache
 bandwidth 128
 load-interval 30
 dialer idle-timeout 99999
 dialer hold-queue 40
 dialer-group 1
 isdn spid1 919472417100 4724171
 isdn spid2 919472417201 4724172
 ppp authentication chap
 crypto map test
!
ip classless
```

```
ip route 0.0.0.0 0.0.0.0 12.12.12.13
access-list 133 permit ip 20.20.20.0 0.0.0.255
 40.40.40.0 0.0.0.255
dialer-list 1 protocol ip permit
!
line con 0
 exec-timeout 0 0
line vty 0 4
 password ww
 login
!
end

lab-isdn#

------------------ RSA-sig ---------------------------
lab-isdn#show debug
Cryptographic Subsystem:
  Crypto ISAKMP debugging is on
  Crypto Engine debugging is on
  Crypto IPSEC debugging is on
lab-isdn#

lab-isdn#
*Mar 21 20:16:50.871: ISAKMP (4): processing SA payload.
 message ID = 0
*Mar 21 20:16:50.871: ISAKMP (4): Checking ISAKMP transform 1
 against priority 65535
        policy
*Mar 21 20:16:50.875: ISAKMP: encryption DES-CBC
*Mar 21 20:16:50.875: ISAKMP: hash SHA
*Mar 21 20:16:50.875: ISAKMP: default group 1
*Mar 21 20:16:50.875: ISAKMP:  auth RSA sig
*Mar 21 20:16:50.879: ISAKMP (4): atts are acceptable.
 Next payload is 0
*Mar 21 20:16:50.879: Crypto engine 0: generate
 alg param

*Mar 21 20:16:54.070: CRYPTO_ENGINE: Dh phase 1
status: 0
*Mar 21 20:16:54.090: ISAKMP (4): SA is doing RSA
 signature authentication
*Mar 21 20:16:57.343: ISAKMP (4): processing KE
 payload. message ID = 0
*Mar 21 20:16:57.347: Crypto engine 0: generate alg param

*Mar 21 20:17:01.168: ISAKMP (4): processing NONCE
payload. message ID = 0
*Mar 21 20:17:01.176: Crypto engine 0: create ISAKMP
 SKEYID for conn id 4
*Mar 21 20:17:01.188: ISAKMP (4): SKEYID state generated
*Mar 21 20:17:07.331: ISAKMP (4): processing ID
 payload. message ID = 0
*Mar 21 20:17:07.331: ISAKMP (4): processing CERT
 payload. message ID = 0
*Mar 21 20:17:07.497: ISAKMP (4): cert approved
 with warning
*Mar 21 20:17:07.600: ISAKMP (4): processing SIG
 payload. message ID = 0
*Mar 21 20:17:07.608: Crypto engine 0: RSA decrypt
 with public key
*Mar 21 20:17:07.759: generate hmac context for
 conn id 4
*Mar 21 20:17:07.767: ISAKMP (4): SA has been
```

```
 authenticated
*Mar 21 20:17:07.775: generate hmac context for
 conn id 4
*Mar 21 20:17:07.783: Crypto engine 0: RSA encrypt
 with private key
*Mar 21 20:17:08.672: CRYPTO_ENGINE: key process
 suspended and continued
*Mar 21 20:17:08.878: CRYPTO_ENGINE: key process
 suspended and continued
*Mar 21 20:17:09.088: CRYPTO_ENGINE: key process
 suspended and continued
*Mar 21 20:17:09.291: CRYPTO_ENGINE: key process
 suspended and continued
*Mar 21 20:17:09.493: CRYPTO_ENGINE: key process
 suspended and continued
*Mar 21 20:17:09.795: CRYPTO_ENGINE: key process
 suspended and continued
*Mar 21 20:17:10.973: generate hmac context for
 conn id 4
*Mar 21 20:17:10.981: ISAKMP (4): processing SA
 payload. message ID = -538880964
*Mar 21 20:17:10.981: ISAKMP (4): Checking IPSec proposal 1
*Mar 21 20:17:10.981: ISAKMP: transform 1, AH_SHA_HMAC
*Mar 21 20:17:10.985: ISAKMP: attributes in transform:
*Mar 21 20:17:10.985: ISAKMP: encaps is 1
*Mar 21 20:17:10.985: ISAKMP: SA life type in seconds
*Mar 21 20:17:10.985: ISAKMP: SA life duration (basic) of 3600
*Mar 21 20:17:10.989: ISAKMP: SA life type in kilobytes
*Mar 21 20:17:10.989: ISAKMP: SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar 21 20:17:10.993: ISAKMP (4): atts are acceptable.
*Mar 21 20:17:10.993: ISAKMP (4): Checking IPSec proposal 1
*Mar 21 20:17:10.993: ISAKMP: transform 1, ESP_DES
*Mar 21 20:17:10.997: ISAKMP: attributes in transform:
*Mar 21 20:17:10.997: ISAKMP: encaps is 1
*Mar 21 20:17:10.997: ISAKMP: SA life type in seconds
*Mar 21 20:17:10.997: ISAKMP: SA life duration (basic) of 3600
*Mar 21 20:17:11.001: ISAKMP: SA life type in kilobytes
*Mar 21 20:17:11.001: ISAKMP: SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar 21 20:17:11.001: ISAKMP: HMAC algorithm is SHA
*Mar 21 20:17:11.005: ISAKMP (4): atts are acceptable.
*Mar 21 20:17:11.005: IPSEC(validate_proposal_request):
 proposal part #1,
  (key eng. msg.) dest= 12.12.12.12, SRC= 12.12.12.13,
    dest_proxy= 20.20.20.0/0.0.0.0/0/0,
    src_proxy= 40.40.40.0/0.0.0.16/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar 21 20:17:11.013: IPSEC(validate_proposal_request):
 proposal part #2,
  (key eng. msg.) dest= 12.12.12.12, SRC= 12.12.12.13,
    dest_proxy= 20.20.20.0/0.0.0.0/0/0,
    src_proxy= 40.40.40.0/0.0.0.16/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar 21 20:17:11.021: ISAKMP (4): processing NONCE payload.
  message ID = -538880964
*Mar 21 20:17:11.021: ISAKMP (4): processing ID payload.
  message ID = -538880964
*Mar 21 20:17:11.021: ISAKMP (4): processing ID payload.
 message ID = -538880964
```

```
*Mar 21 20:17:11.025: IPSEC(key_engine):
got a queue event...
*Mar 21 20:17:11.029: IPSEC(spi_response):
getting spi 112207019 for SA
        from 12.12.12.13     to 12.12.12.12 for prot 2
*Mar 21 20:17:11.033: IPSEC(spi_response):
getting spi 425268832 for SA
        from 12.12.12.13     to 12.12.12.12 for prot 3
*Mar 21 20:17:11.279: generate hmac context for conn id 4
*Mar 21 20:17:11.612: generate hmac context for conn id 4
*Mar 21 20:17:11.644: ISAKMP (4): Creating IPSec SAs
*Mar 21 20:17:11.644:         inbound SA from
12.12.12.13 to 12.12.12.12
        (proxy 40.40.40.0      to 20.20.20.0     )
*Mar 21 20:17:11.648:         has spi 112207019
and conn_id 5 and flags 4
*Mar 21 20:17:11.648:         lifetime of 3600 seconds
*Mar 21 20:17:11.648:         lifetime of 4608000 kilobytes
*Mar 21 20:17:11.652: outbound SA from 12.12.12.12 to 12.12.12.13
        (proxy 20.20.20.0  to 40.40.40.0     )
*Mar 21 20:17:11.652: has spi 83231845 and conn_id 6 and flags 4
*Mar 21 20:17:11.656: lifetime of 3600 seconds
*Mar 21 20:17:11.656: lifetime of 4608000 kilobytes
*Mar 21 20:17:11.656: ISAKMP (4): Creating IPSec SAs
*Mar 21 20:17:11.656:  inbound SA from 12.12.12.13 to 12.12.12.12
        (proxy 40.40.40.0      to 20.20.20.0     )
*Mar 21 20:17:11.660: has spi 425268832 and conn_id 7 and flags 4
*Mar 21 20:17:11.660: lifetime of 3600 seconds
*Mar 21 20:17:11.664: lifetime of 4608000 kilobytes
*Mar 21 20:17:11.664: outbound SA from 12.12.12.12 to 12.12.12.13
        (proxy 20.20.20.0 to 40.40.40.0     )
*Mar 21 20:17:11.668: has spi 556010247 and conn_id 8 and flags 4
*Mar 21 20:17:11.668: lifetime of 3600 seconds
*Mar 21 20:17:11.668: lifetime of 4608000 kilobytes
*Mar 21 20:17:11.676: IPSEC(key_engine): got a queue event...
*Mar 21 20:17:11.676: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.12.12.12, SRC= 12.12.12.13,
    dest_proxy= 20.20.20.0/255.255.255.0/0/0,
    src_proxy= 40.40.40.0/255.255.255.0/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x6B024AB(112207019), conn_id= 5, keysize= 0, flags= 0x4
*Mar 21 20:17:11.680: IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 12.12.12.12, dest= 12.12.12.13,
    src_proxy= 20.20.20.0/255.255.255.0/0/0,
    dest_proxy= 40.40.40.0/255.255.255.0/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x4F60465(83231845), conn_id= 6, keysize= 0, flags= 0x4
*Mar 21 20:17:11.687: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.12.12.12, SRC= 12.12.12.13,
    dest_proxy= 20.20.20.0/255.255.255.0/0/0,
    src_proxy= 40.40.40.0/255.255.255.0/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x19591660(425268832), conn_id= 7, keysize= 0, flags= 0x4
*Mar 21 20:17:11.691: IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 12.12.12.12, dest= 12.12.12.13,
    src_proxy= 20.20.20.0/255.255.255.0/0/0,
    dest_proxy= 40.40.40.0/255.255.255.0/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x21240B07(556010247), conn_id= 8, keysize= 0, flags= 0x4
*Mar 21 20:17:11.699: IPSEC(create_sa): sa created,
```

```
  (sa) sa_dest= 12.12.12.12, sa_prot= 51,
    sa_spi= 0x6B024AB(112207019),
    sa_trans= ah-sha-hmac , sa_conn_id= 5
*Mar 21 20:17:11.703: IPSEC(create_sa): sa created,
  (sa) sa_dest= 12.12.12.13, sa_prot= 51,
    sa_spi= 0x4F60465(83231845),
    sa_trans= ah-sha-hmac , sa_conn_id= 6
*Mar 21 20:17:11.707: IPSEC(create_sa): sa created,
  (sa) sa_dest= 12.12.12.12, sa_prot= 50,
    sa_spi= 0x19591660(425268832),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 7
*Mar 21 20:17:11.707: IPSEC(create_sa): sa created,
  (sa) sa_dest= 12.12.12.13, sa_prot= 50,
    sa_spi= 0x21240B07(556010247),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 8
*Mar 21 20:18:06.767: ISADB: reaper checking SA, conn_id = 4
lab-isdn#
```

IPSec 및 ISAKMP 문제 해결

일반적으로 다음 명령을 사용하여 정보를 수집하여 각 문제 해결 세션을 시작하는 것이 좋습니다 .별표(*)는 특히 유용한 명령을 나타냅니다.자세한 내용은 IP 보안 문제 해결 - 디버그 명령 이해 및 사용을 참조하십시오.

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.

명령	
디버그 암호화 pki 트랜잭션	* debug crypto ipsec
* 디버그 암호화 isakmp	디버그 암호화 키
디버그 암호화 세션	디버그 암호화 엔진
활성 암호화 엔진 연결 표시	show crypto engine connections dropped-packet 표시
암호화 엔진 구성 표시	* show crypto ca certificates
* show crypto key mypubkey rsa	* show crypto key pubkey-chain rsa
암호화 isakmp 정책 표시	crypto isakmp sa 표시
crypto ipsec sa 표시	show crypto ipsec session key
show crypto ipsec transform-proposal	암호화 맵 인터페이스 bri 0 표시
암호화 맵 태그 테스트 표시	암호화 연결 지우기 <SA의 연결 ID>
* clear crypto isakmp	* 암호화 sa 지우기
crypto sa 카운터 지우기	암호화 sa 맵 지우기
암호화 sa 피어 지우기	암호화 sa spi 지우기
crypto sa 카운터 지우기	

이러한 명령 중 일부의 샘플 출력이 아래에 나와 있습니다.

```
wan2511#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 9    Serial0         20.20.20.21 set    HMAC_SHA        0        240
 10   Serial0         20.20.20.21 set    HMAC_SHA        240      0

wan2511#show crypto engine connections dropped-packet
Interface            IP-Address    Drop Count

wan2511#show crypto engine configuration
slot:               0
engine name:        unknown
engine type:        software
serial number:      01496536
platform:           rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    140
input queue bot:    140
input queue count:  0

wan2511#show crypto key mypubkey rsa
% Key pair was generated at: 00:09:04 UTC Mar 1 1993
Key name: wan2511.cisco.com
Usage:    General Purpose Key
Key Data:
 305C300D 06092A86 4886F70D 01010105
00034B00 30480241 00E9007B E5CD7DC8
 6E1C0423 92044254 92C972AD 0CCE9796
86797EAA B6C4EFF0 0F0A5378 6AFAE43B
 3A2BD92F 98039DAC 08741E82 5D9053C4
D9CFABC1 AB54E0E2 BB020301 0001

wan2511#show crypto key pubkey-chain rsa
wan2511#

wan2511#show crypto isakmp policy
Protection suite of priority 1
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               240 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
wan2511#show crypto isakmp sa
    dst           src          state        conn-id   slot
20.20.20.21    20.20.20.20    QM_IDLE           7       0

wan2511#
wan2511#show crypto ipsec sa

interface: Serial0
    Crypto map tag: test, local addr. 20.20.20.21

   local  ident (addr/mask/prot/port): (50.50.50.0/255.255.255.0/0/0)
```

```
   remote ident (addr/mask/prot/port): (60.60.60.0/255.255.255.0/0/0)
   current_peer: 20.20.20.20
     PERMIT, flags={origin_is_acl,ident_is_ipsec,}
    #pkts encaps: 320, #pkts encrypt: 320, #pkts digest 320
    #pkts decaps: 320, #pkts decrypt: 320, #pkts verify 320
    #send errors 0, #recv errors 0

     local crypto endpt.: 20.20.20.21, remote crypto endpt.: 20.20.20.20
     path mtu 1500, media mtu 1500
     current outbound spi: 6625CD

     inbound esp sas:
      spi: 0x1925112F(421859631)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 11, crypto map: test
        sa timing: remaining key lifetime (k/sec): (4607971/3354)
        IV size: 8 bytes
        replay detection support: Y


     inbound ah sas:
      spi: 0x12050DD2(302321106)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 9, crypto map: test
        sa timing: remaining key lifetime (k/sec): (4607958/3354)
        replay detection support: Y


     outbound esp sas:
      spi: 0x3262313(52830995)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 12, crypto map: test
        sa timing: remaining key lifetime (k/sec): (4607971/3354)
        IV size: 8 bytes
        replay detection support: Y


     outbound ah sas:
      spi: 0x6625CD(6694349)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 10, crypto map: test
        sa timing: remaining key lifetime (k/sec): (4607958/3354)
        replay detection support: Y

wan2511#show crypto ipsec session-key
Session key lifetime: 4608000 kilobytes/3600 seconds

wan2511#show crypto ipsec transform-proposal
Transform proposal auth2: { ah-sha-hmac  }
   supported settings = { Tunnel,  },
   default settings = { Tunnel,  },
   will negotiate = { Tunnel,  },

   { esp-des esp-sha-hmac  }
   supported settings = { Tunnel,  },
   default settings = { Tunnel,  },
   will negotiate = { Tunnel,  },


wan2511#show crypto map interface serial 0
```

```
Crypto Map "test" 10 ipsec-isakmp
        Peer = 20.20.20.20
        Extended IP access list 133
            access-list 133 permit ip
                source: addr = 50.50.50.0/0.0.0.255
                dest:   addr = 60.60.60.0/0.0.0.255
        Current peer: 20.20.20.20
        Session key lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform proposals={ auth2, }

wan2511#show crypto map tag test
Crypto Map "test" 10 ipsec-isakmp
        Peer = 20.20.20.20
        Extended IP access list 133
            access-list 133 permit ip
                source: addr = 50.50.50.0/0.0.0.255
                dest:   addr = 60.60.60.0/0.0.0.255
        Current peer: 20.20.20.20
        Session key lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform proposals={ auth2, }

wan2511#

----------------------
lab-isdn1#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 5    BRI0            12.12.12.13 set    HMAC_SHA        0        89
 6    BRI0            12.12.12.13 set    HMAC_SHA        89       0

lab-isdn1#show crypto engine connections dropped-packet
Interface            IP-Address    Drop Count

BRI0                 12.12.12.13   4
lab-isdn1#show crypto engine configuration
slot:               0
engine name:        unknown
engine type:        software
serial number:      05679987
platform:           rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    243
input queue bot:    243
input queue count:  0

lab-isdn1#show crypto ca cert
Certificate
  Subject Name
    Name: lab-isdn1.cisco.com
    Serial Number: 05679987
  Status: Available
  Certificate Serial Number: 3E1ED472BDA2CE0163FB6B0B004E5EEE
  Key Usage: Encryption

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7169BEE31B821DFE4B3A338E5F
  Key Usage: Not Set

Certificate
  Subject Name
```

```
    Name: lab-isdn1.cisco.com
    Serial Number: 05679987
  Status: Available
  Certificate Serial Number: 503968D890F7D409475B7280162754D2
  Key Usage: Signature


lab-isdn1#show crypto key mypubkey rsa
% Key pair was generated at: 03:10:23 UTC Mar 21 1993
Key name: lab-isdn1.cisco.com
Usage:    Signature Key
Key Data:
 305C300D 06092A86 4886F70D 01010105
00034B00 30480241 00BECE2D 8CB32E6B
 090ADE0D 46AF8D4A 1F378500 3435D0C7
293BF915 180C9E4C F81A6A43 AEE4F046
 87B8E285 9D33D5CE 042E5DDE A63DA54A
312AD425 5A756014 CB020301 0001
% Key pair was generated at: 03:11:17 UTC Mar 21 1993
Key name: lab-isdn1.cisco.com
Usage:    Encryption Key
Key Data:
 305C300D 06092A86 4886F70D 01010105
00034B00 30480241 00D2D125 FFBBFC6E
 5693CB43 855473C1 65BC7CCA F645C35B
ED554BAA 0B119AFA 6F0853F5 745E0B84
 922E39B5 FA84C4DD 05C19AA6 25818439
5C6CBC7F A4614F61 77020301 0001

lab-isdn1#show crypto key pubkey-chain rsa
Key name: Cisco SystemsDevtestCISCOCA-ULTRA
Key serial number: C7040262
Key usage: signatures only
Key source: certificate
Key data:
 305C300D 06092A86 4886F70D 01010105
 00034B00 30480241 00C1B69D 7BF634E4
 EE28A84E 0DC6FCA4 DEA804D8 9E50C5EB
 E86239D5 1890D0D4 B732678B DBF28080
 1430E5E5 6E7CC126 E2DDDBE9 695ADF8E
 5BA7E67B AE872937 53020301 0001

Key name: lab-isdn.cisco.com
Key address: 171.68.117.189
Key serial number: 05679919
Key usage: general purpose
Key source: certificate
Key data:
 305C300D 06092A86 4886F70D 01010105
00034B00 30480241 00D771AD 5672B487
 A0195ECD 19546F91 9A3A6270 102E5A9F
F4DC7A60 8480FB27 A1817153 35F4399D
 3E577F72 B323BF06 20AB60C3 71CF4389
 BA4FC60E E6EA21E0 63020301 0001


lab-isdn1#show crypto isakmp policy
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
```

```
lab-isdn1#show crypto isakmp sa
    dst           src          state        conn-id   slot
12.12.12.12    12.12.12.13    QM_IDLE           4       0


lab-isdn1#show crypto ipsec sa

interface: BRI0
    Crypto map tag: test, local addr. 12.12.12.13

   local  ident (addr/mask/prot/port): (40.40.40.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (20.20.20.0/255.255.255.0/0/0)
   current_peer: 12.12.12.12
     PERMIT, flags={origin_is_acl,ident_is_ipsec,}
    #pkts encaps: 89, #pkts encrypt: 89, #pkts digest 89
    #pkts decaps: 89, #pkts decrypt: 89, #pkts verify 89
    #send errors 11, #recv errors 0

     local crypto endpt.: 12.12.12.13, remote crypto endpt.: 12.12.12.12
     path mtu 1500, media mtu 1500
     current outbound spi: 6B024AB

     inbound esp sas:
      spi: 0x21240B07(556010247)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 7, crypto map: test
        sa timing: remaining key lifetime (k/sec): (4607989/3062)
        IV size: 8 bytes
        replay detection support: Y


     inbound ah sas:
      spi: 0x4F60465(83231845)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5, crypto map: test
        sa timing: remaining key lifetime (k/sec): (4607984/3062)
        replay detection support: Y


     outbound esp sas:
      spi: 0x19591660(425268832)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 8, crypto map: test
        sa timing: remaining key lifetime (k/sec): (4607989/3062)
        IV size: 8 bytes
        replay detection support: Y


     outbound ah sas:
      spi: 0x6B024AB(112207019)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 6, crypto map: test
        sa timing: remaining key lifetime (k/sec): (4607984/3062)
        replay detection support: Y


lab-isdn1#show crypto ipsec session-key
Session key lifetime: 4608000 kilobytes/3600 seconds
```

```
lab-isdn1#show crypto ipsec transform-proposal
Transform proposal mypolicy: { ah-sha-hmac  }
   supported settings = { Tunnel,  },
   default settings = { Tunnel,  },
   will negotiate = { Tunnel,  },

   { esp-des esp-sha-hmac  }
   supported settings = { Tunnel,  },
   default settings = { Tunnel,  },
   will negotiate = { Tunnel,  },


lab-isdn1#show crypto map interface bri 0
Crypto Map "test" 10 ipsec-isakmp
        Peer = 12.12.12.12
        Extended IP access list 144
            access-list 144 permit ip
                source: addr = 40.40.40.0/0.0.0.255
                dest:   addr = 20.20.20.0/0.0.0.255
        Current peer: 12.12.12.12
        Session key lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform proposals={ mypolicy, }


lab-isdn1#show crypto map tag test
Crypto Map "test" 10 ipsec-isakmp
        Peer = 12.12.12.12
        Extended IP access list 144
            access-list 144 permit ip
                source: addr = 40.40.40.0/0.0.0.255
                dest:   addr = 20.20.20.0/0.0.0.255
        Current peer: 12.12.12.12
        Session key lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform proposals={ mypolicy, }

lab-isdn1#

----------------------------
lab-isdn1#clear crypto isakmp
lab-isdn1#
*Mar 21 20:58:34.503: ISADB: reaper checking SA, conn_id = 4  DELETE IT!
*Mar 21 20:58:34.507: generate hmac context for conn id 4
*Mar 21 20:58:34.519: CRYPTO(epa_release_crypto_conn_entry): released conn 4
lab-isdn1#
lab-isdn1#clear crypto sa
lab-isdn1#
*Mar 21 20:58:42.495: IPSEC(delete_sa): deleting SA,
  (sa) sa_dest= 12.12.12.13, sa_prot= 51,
    sa_spi= 0x4F60465(83231845),
    sa_trans= ah-sha-hmac , sa_conn_id= 5
*Mar 21 20:58:42.499: CRYPTO(epa_release_crypto_conn_entry): released conn 5
*Mar 21 20:58:42.499: IPSEC(delete_sa): deleting SA,
  (sa) sa_dest= 12.12.12.12, sa_prot= 51,
    sa_spi= 0x6B024AB(112207019),
    sa_trans= ah-sha-hmac , sa_conn_id= 6
*Mar 21 20:58:42.503: CRYPTO(epa_release_crypto_conn_entry): released conn 6
*Mar 21 20:58:42.503: IPSEC(delete_sa): deleting SA,
  (sa) sa_dest= 12.12.12.13, sa_prot= 50,
    sa_spi= 0x21240B07(556010247),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 7
*Mar 21 20:58:42.507: CRYPTO(epa_release_crypto_conn_entry): released conn 7
```

```
*Mar 21 20:58:42.507: IPSEC(delete_sa): deleting SA,
  (sa) sa_dest= 12.12.12.12, sa_prot= 50,
    sa_spi= 0x19591660(425268832),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 8
*Mar 21 20:58:42.511: CRYPTO(epa_release_crypto_conn_entry): released conn 8
lab-isdn1#
```

관련 정보

- Cisco 네트워크 레이어 암호화 구성 및 문제 해결:배경 - 1부
- NIST(National Institute of Standards and Technology)에서 DES FIPS 46-2
- NIST(National Institute of Standards and Technology)에서 DSS FIPS 186
- RSA Laboratories의 최신 암호화에 대한 FAQ
- IETF 보안 표준
- 인터넷 키 교환 보안 프로토콜 구성
- IPSec 네트워크 보안 구성
- IPSec 지원 페이지
- Technical Support - Cisco Systems