Cisco 네트워크 레이어 암호화 구성 및 문제 해결 :배경 - 1부

목차

소개

이 문서에서는 IPSec 및 ISAKMP(Internet Security Association and Key Management Protocol)를 사용한 Cisco Network-Layer Encryption 구성 및 문제 해결에 대해 설명하고 IPSec 및 ISAKMP와 함께 네트워크 레이어 암호화 배경 정보 및 기본 컨피그레이션을 다룹니다.

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® 소프트웨어 릴리스 11.2 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

네트워크 레이어 암호화 기능은 Cisco IOS® 소프트웨어 릴리스 11.2에서 도입되었습니다. 이 기능은 보안 데이터 전송을 위한 메커니즘을 제공하며 다음 두 가지 구성 요소로 구성됩니다.

- **라우터 인증:**두 라우터는 암호화된 트래픽을 전달하기 전에 DSS(Digital Signature Standard) 공개 키를 사용하여 일회성 양방향 인증을 수행하여 무작위 문제를 서명합니다.
- **네트워크 레이어 암호화:**IP 페이로드 암호화의 경우 라우터는 Diffie-Hellman 키 교환을 사용하여 12.2(13)T에 도입된 DES(40 또는 56비트 세션 키), Triple DES - 3DES(168비트) 또는 최신 Advanced Encryption Standard - AES(128비트(기본값) 또는 192비트 또는 256비트 키)를 안전하게 생성합니다.새 세션 키는 구성 가능한 기반으로 생성됩니다.암호화 정책은 확장 IP 액세스 목록을 사용하여 라우터 간에 암호화할 네트워크, 서브넷, 호스트 또는 프로토콜 쌍을 정의하는 암호화 맵에 의해 설정됩니다.

암호화 배경

암호술 분야는 통신을 비공개로 유지하는 것에 관한 것이다.민감한 통신의 보호는 그 역사의 대부분을 통해 암호화에 중점을 두었다.암호화는 데이터를 읽을 수 없는 형식으로 변환하는 것입니다.이 정보의 목적은 암호화된 데이터를 볼 수 있더라도 의도하지 않은 사용자로부터 정보를 숨겨 놓음으로써 프라이버시를 보장하는 것입니다.암호 해독은 암호화의 반대입니다.이는 암호화된 데이터를 다시 이해할 수 있는 형태로 바꾸는 것입니다.

암호화 및 암호 해독에는 일부 비밀 정보(일반적으로 "키"라고 함)를 사용해야 합니다. 사용된 암호화 메커니즘에 따라 암호화 및 암호 해독에 동일한 키를 사용할 수 있습니다.다른 메커니즘의 경우 암호화 및 해독에 사용되는 키가 다를 수 있습니다.

디지털 서명은 문서를 특정 키의 소유자에 바인딩하는 반면, 디지털 타임스탬프는 문서를 특정 시간에 해당 작성 문서에 바인딩합니다.이러한 암호화 메커니즘을 사용하여 공유 디스크 드라이브, 높은 보안 설치 또는 유료 TV 채널에 대한 액세스를 제어할 수 있습니다.

최신 암호화가 점점 더 다양해지고 있지만, 암호화는 근본적으로 해결하기 어려운 문제를 기반으로 합니다.암호화 메시지의 암호 해독 또는 디지털 문서 서명과 같은 키를 알아야 하므로 문제가 발생할 수 있습니다.특정 해시 값을 생성하는 메시지를 찾는 등 본질적으로 완료하는 것이 어렵기 때문에 문제가 발생할 수도 있습니다.

암호화의 필드가 발전함에 따라 암호화가 무엇이고 무엇으로 암호화하지 않는지 구분선이 모호해

졌습니다.오늘날 암호화는 해결하기 어려운 수학 문제의 존재에 의존하는 기술과 응용 프로그램에 대한 연구로 요약될 수 있습니다.암호화 분석가가 암호화 메커니즘을 손상시키려는 시도이며, 암호화 기술은 암호화 및 암호화 분석을 결합하는 규율입니다.

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 통신

에는 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.

예비 정보

이 섹션에서는 몇 가지 기본적인 네트워크 레이어 암호화 개념에 대해 설명합니다.암호화의 여러 측면을 살펴보아야 합니다.처음에는 이러한 문제가 이해되지 않을 수도 있지만, 몇 달 동안 암호화를 사용한 후 더 잘 이해할 수 있기 때문에 지금 읽어 보고 이해하는 것이 좋습니다.

- 암호화는 인터페이스의 출력에서만 발생하며 암호 해독은 인터페이스에 대한 입력 시에만 발생합니다.정책을 계획할 때 이러한 차이가 중요합니다.암호화 및 암호 해독에 대한 정책은 대칭적입니다.즉, 하나를 정의하면 다른 하나는 자동으로 제공됩니다.암호화 맵 및 연결된 확장 액세스 목록을 사용하면 암호화 정책만 명시적으로 정의됩니다.암호 해독 정책은 동일한 정보를 사용하지만, 패킷과 일치하면 소스 및 목적지 주소와 포트를 취소합니다.이렇게 하면 듀플렉스 연결의 양방향으로 데이터가 보호됩니다.crypto map 명령의 match address x 문은 인터페이스에서 나가는 패킷을 설명하는 데 사용됩니다.즉, 패킷의 암호화를 설명합니다.그러나 패킷은 인터페이스에 들어갈 때 암호 해독을 위해 일치해야 합니다.이는 소스 및 대상 주소와 포트가 반대로 액세스 목록을 트래버스하여 자동으로 수행됩니다.이렇게 하면 연결에 대한 대칭이 제공됩니다.암호화 **맵**에서 가리키는 액세스 목록은 트래픽을 하나의(아웃바운드) 방향으로만 설명해야 합니다.정의한 액세스 목록과 일치하지 않는 IP 패킷은 전송되지만 암호화되지 않습니다.액세스 목록의 "거부"는 해당 호스트가 일치하지 않아야 함을 나타내며, 이는 해당 호스트가 암호화되지 않음을 의미합니다.이 컨텍스트에서 "거부"는 패킷이 삭제되었음을 의미하지는 않습니다.
- 확장 액세스 목록에서 "any"라는 단어를 사용하는 것에 주의하십시오."any"를 사용하면 일치하는 "암호화되지 않은" 인터페이스로 이동하는 경우가 아니면 트래픽이 삭제됩니다.또한 Cisco IOS Software Release 11.3(3)T의 IPSec에서는 "any"가 허용되지 않습니다.
- 소스 또는 목적지 주소를 지정할 때 "any" 키워드를 사용하지 않는 것이 좋습니다."any"를 지정하면 수신 라우터가 이 트래픽을 자동으로 삭제하므로 라우팅 프로토콜, NTP(Network Time Protocol), 에코, 에코 응답 및 멀티캐스트 트래픽에 문제가 발생할 수 있습니다."any"를 사용하려면 "ntp"와 같이 암호화되지 않은 트래픽에 대해 "deny" 문 앞에 와야 합니다.
- 시간을 절약하려면 암호화 **연결**을 시도하려는 피어 라우터에 ping을 수행할 수 있는지 확인합

니다.또한 잘못된 문제를 해결하는 데 너무 많은 시간을 소비하기 전에(트래픽이 암호화되는 것에 의존함) 서로 ping하도록 엔드 디바이스를 지정합니다.즉, **암호화**를 시도하기 전에 라우팅이 제대로 작동하는지 **확인합니다**.원격 피어에 이그레스 인터페이스에 대한 경로가 없을 수 있습니다. 이 경우 해당 피어와 암호화 세션을 가질 수 없습니다(해당 직렬 인터페이스에서 번호가 지정되지 않은 **ip**를 사용할 수 있을 수 있습니다).

- 많은 WAN Point-to-Point 링크는 라우팅 불가능한 IP 주소를 사용하며, Cisco IOS Software Release 11.2 Encryption은 ICMP(Internet Control Message Protocol)를 사용합니다(ICMP에 이그레스 직렬 인터페이스의 IP 주소를 사용함). 그러면 WAN 인터페이스에서 **ip unnumbered**를 사용해야 할 수 있습니다.항상 **ping** 및 **traceroute** 명령을 수행하여 두 피어링(암호화/해독) 라우터에 대한 라우팅이 제대로 적용되었는지 확인합니다.
- 두 라우터만 Diffie-Hellman 세션 키를 공유할 수 있습니다.즉, 하나의 라우터가 동일한 세션 키를 사용하여 두 피어로 암호화된 패킷을 교환할 수 없습니다.각 라우터 쌍에는 세션 키가 있어야 합니다. 이는 Diffie-Hellman 교환의 결과입니다.
- 암호화 엔진은 Cisco IOS, VIP2 Cisco IOS에 있거나 VIP2의 ESA(Encryption Services Adapter) 하드웨어에 있습니다. VIP2가 없으면 Cisco IOS 암호화 엔진은 모든 포트에서 암호화 정책을 제어합니다.VIP2를 사용하는 플랫폼에는 여러 암호화 엔진이 있습니다.VIP2의 암호화 엔진은 보드에 있는 포트에서 암호화를 제어합니다.
- 트래픽을 암호화할 준비가 된 인터페이스에 트래픽이 도착하도록 설정되었는지 확인합니다.트래픽이 암호화 **맵**이 적용된 인터페이스 이외의 다른 인터페이스**에** 도달할 수 있는 경우 자동으로 삭제됩니다.
- 키 교환을 수행할 때 두 라우터에 대한 콘솔(또는 대체) 액세스를 가질 수 있습니다.키를 기다리는 동안 패시브 측에서 전화를 걸 수 있습니다.
- cfb-**64**는 CPU 로드 측면에서 cfb-**8**보다 더 효율적으로 처리합니다.
- 라우터는 사용하려는 CFB(cipher-feedback) 모드에서 사용할 알고리즘을 실행해야 합니다.각 이미지의 기본값은 이미지 이름(예: cfb-**64**)입니다.
- key-timeout을 변경하는 것이 좋습니다.기본값인 30분은 매우 짧습니다.하루(1440분)로 늘리십시오.
- 키가 만료될 때마다 키 재협상 중에 IP 트래픽이 삭제됩니다.
- 암호화하려는 트래픽만 선택합니다(이렇게 하면 CPU 주기가 절약됨).
- DDR(Dial-on-Demand Routing)을 사용하면 ICMP를 흥미롭게 만들 수 있습니다. 그렇지 않으면 다이얼아웃이 되지 않습니다.
- IP 이외의 트래픽을 암호화하려면 터널을 사용합니다.터널을 사용하여 물리적 인터페이스와 터널 인터페이스 모두에 암호화 맵을 적용합니다.참조: 샘플 5:자세한 내용은 IP 터널에서 IPX 트래픽 암호화.
- 두 암호화 피어 라우터를 직접 연결할 필요가 없습니다.
- 로우엔드 라우터가 "CPU 과다 사용" 메시지를 제공할 수 있습니다.암호화가 많은 CPU 리소스를 사용한다는 것을 알려주기 때문에 이를 무시할 수 있습니다.
- 암호화 라우터를 중복 배치하지 마십시오. 이렇게 하면 트래픽을 암호화하고 다시 암호화하여 CPU를 낭비할 수 있습니다.두 엔드포인트에서 암호화하면 됩니다.참조: 샘플 3:자세한 내용을 보려면 라우터를 통해 암호화를 수행합니다.
- 현재 브로드캐스트 및 멀티캐스트 패킷의 암호화는 지원되지 않습니다.네트워크 설계에서 "보안" 라우팅 업데이트가 중요한 경우, 업데이트 무결성을 보장하기 위해 EIGRP(Enhanced Interior Gateway Routing Protocol), OSPF(Open Shortest Path First) 또는 RIPv2(Routing Information Protocol Version 2)와 같은 인증 내장 프로토콜을 사용해야 합니다.

주의 사항

참고: 아래 설명된 주의 사항이 모두 해결되었습니다.

- 암호화를 위해 ESA를 사용하는 Cisco 7200 라우터는 하나의 세션 키 아래에서 패킷을 해독하지 못한 다음 다른 세션 키 아래에서 패킷을 다시 암호화할 수 없습니다.Cisco 버그 ID CSCdj82613(등록된 고객만 해당)을 참조하십시오.
- 두 라우터가 암호화된 임대 회선과 ISDN 백업 회선으로 연결되어 있으면 임대 회선이 끊기면 ISDN 링크가 제대로 작동됩니다.그러나 임대 회선이 다시 작동하면 ISDN 통화를 배치한 라우터가 충돌합니다.Cisco 버그 ID CSCdj00310(등록된 고객만 해당)을 참조하십시오.
- 여러 VIP가 있는 Cisco 7500 Series 라우터의 경우 **암호화 맵**이 VIP의 한 인터페이스에도 적용되면 하나 이상의 VIP가 충돌합니다.Cisco 버그 ID CSCdi88459(등록된 고객만 해당)를 참조하십시오.
- VIP2 및 ESA가 있는 Cisco 7500 Series 라우터의 경우 사용자가 콘솔 포트에 있지 않으면 **show crypto card** 명령이 출력을 표시하지 않습니다.Cisco 버그 ID CSCdj89070(등록된 고객만 해당)을 참조하십시오.

Cisco IOS 네트워크 레이어 암호화 컨피그레이션

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.

이 문서의 모든 샘플 컨피그레이션은 Cisco IOS Software Release 11.3에서 가져온 것입니다. Cisco IOS Software Release 11.2 명령에서 다음과 같은 몇 가지 변경 사항이 있었습니다.

- 일부 key configuration 명령의 dss입니다.
- cisco는 일부 **show** 명령 및 **crypto map** 명령(Cisco IOS Software Release 11.2 이상에서 참조)과 Cisco IOS Software Release 11.3(2)T에 있는 IPSec을 구별합니다.

참고: 이러한 컨피그레이션 예에 사용된 IP 주소는 Cisco의 Lab에서 무작위로 선택되었으며 완전히 일반적입니다.

1단계:수동으로 DSS 키 쌍 생성

암호화 세션에 참여하는 각 라우터에서 DSS 키 쌍(공개 및 개인 키)을 수동으로 생성해야 합니다.즉, 모든 라우터에 참여하려면 고유한 DSS 키가 있어야 합니다.암호화 엔진은 고유한 DSS 키를 하나만 가질 수 있습니다.DSS와 RSA 키를 구분하기 위해 Cisco IOS Software Release 11.3에 "dss" 키워드가 추가되었습니다.라우터의 고유 DSS 키에 대한 이름을 지정할 수 있습니다(그러나 라우터 호스트 이름을 사용하는 것이 좋습니다). Cisco 2500 Series와 같은 덜 강력한 CPU에서는 키 쌍을 생성하는 데 약 5초 정도 소요됩니다.

라우터는 키 쌍을 생성합니다.

- 공개 키(나중에 암호화 세션에 참여하는 라우터로 전송).
- 개인 키(다른 사람과 보거나 교환되지 않음)실제로 NVRAM의 별도의 섹션에 저장되며 볼 수 없습니다.)

라우터의 DSS 키 쌍이 생성되면 해당 라우터의 암호화 엔진과 고유하게 연결됩니다.키 쌍 생성이 아래의 명령 출력에 나와 있습니다.

```
dial-5(config)#crypto key generate dss dial5
Generating DSS keys ....
 [OK]
```

```
dial-5#show crypto key mypubkey dss
crypto public-key dial5 05679919
 160AA490 5B9B1824 24769FCD EE5E0F46 1ABBD343 4C0C4A03 4B279D6B 0EE5F65F
 F64665D4 1036875A 8CF93691 BDF81722 064B51C9 58D72E12 3E1894B6 64B1D145
quit


dial-5#show crypto engine configuration
slot:               0
engine name:        dial5
engine type:        software
serial number:      05679919
platform:           rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    43
input queue bot:    43
input queue count:  0

dial-5#
```

라우터를 식별하는 키 쌍을 하나만 생성할 수 있으므로 원래 키를 덮어쓸 수 있으며 암호화 연결의 모든 라우터로 공개 키를 다시 보내야 합니다.다음은 아래의 명령 출력에 나와 있습니다.

```
StHelen(config)#crypto key generate dss barney
% Generating new DSS keys will require re-exchanging
   public keys with peers who already have the public key
   named barney!
Generate new DSS keys? [yes/no]: yes
Generating DSS keys ....
 [OK]


StHelen(config)#
Mar 16 12:13:12.851: Crypto engine 0: create key pairs.
```

2단계:피어와 수동으로 DSS 공개 키 교환(대역 외)

라우터의 자체 DSS 키 쌍을 생성하는 것은 암호화 세션 연결을 설정하는 첫 번째 단계입니다.다음 단계는 공개 키를 다른 모든 라우터와 교환하는 것입니다.먼저 show crypto mypubkey 명령을 입력하여 라우터의 DSS 공개 키를 표시하여 이러한 공개 키를 수동으로 입력할 수 있습니다.그런 다음 이러한 공개 키(예: 이메일)를 교환하고 crypto key pubkey-chain dss 명령을 사용하여 피어 라우터의 공개 키를 잘라내어 라우터에 붙여넣습니다.

또한 crypto **key exchange dss** 명령을 사용하여 라우터가 공개 키를 자동으로 교환하도록 할 수도 있습니다.자동화된 방법을 사용하는 경우 키 교환에 사용되는 인터페이스에 **암호화 맵** 문이 없는지 확인합니다.디버그 **암호화 키**는 여기에서 유용합니다.

참고: 키를 교환하기 전에 피어에 **ping**을 수행하는 것이 좋습니다.

```
Loser#ping 19.19.19.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 19.19.19.20, timeout is 2 seconds:
!!!!!

Loser(config)#crypto key exchange dss passive
Enter escape character to abort if connection does not complete.
```

```
Wait for connection from peer[confirm]
Waiting ....


  StHelen(config)#crypto key exchange dss 19.19.19.19 barney
  Public key for barney:
  Serial Number 05694352
  Fingerprint   309E D1DE B6DA 5145 D034

  Wait for peer to send a key[confirm]


Public key for barney:
   Serial Number 05694352
   Fingerprint   309E D1DE B6DA 5145 D034

Add this public key to the configuration? [yes/no]:yes


         Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes.
         Mar 16 12:16:55.343: CRYPTO-KE: Sent 4 bytes.
         Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes.
         Mar 16 12:16:55.347: CRYPTO-KE: Sent 64 bytes.


Mar 16 12:16:45.099: CRYPTO-KE: Received 4 bytes.
Mar 16 12:16:45.099: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:45.103: CRYPTO-KE: Received 6 bytes.
Mar 16 12:16:45.103: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:45.107: CRYPTO-KE: Received 50 bytes.
Mar 16 12:16:45.111: CRYPTO-KE: Received 14 bytes.

Send peer a key in return[confirm]
Which one?

fred? [yes]:
Public key for fred:
   Serial Number 02802219
   Fingerprint   2963 05F9 ED55 576D CF9D


         Waiting ....
         Public key for fred:
           Serial Number 02802219
         Fingerprint   2963 05F9 ED55 576D CF9D

         Add this public key to the configuration? [yes/no]:

Loser(config)#
Mar 16 12:16:55.339: CRYPTO-KE: Sent 4 bytes.
Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes.
Mar 16 12:16:55.343: CRYPTO-KE: Sent 4 bytes.
Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes.
Mar 16 12:16:55.347: CRYPTO-KE: Sent 64 bytes.
Loser(config)#

Mar 16 12:16:56.083: CRYPTO-KE: Received 4 bytes.
Mar 16 12:16:56.087: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:56.087: CRYPTO-KE: Received 4 bytes.
Mar 16 12:16:56.091: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:56.091: CRYPTO-KE: Received 52 bytes.
Mar 16 12:16:56.095: CRYPTO-KE: Received 12 bytes.
Add this public key to the configuration? [yes/no]: yes
StHelen(config)#^Z
```

```
StHelen#
```

이제 공용 DSS 키가 교환되었으므로 아래 명령 출력에 나와 있는 것처럼 두 라우터가 서로의 공개 키를 가지고 있는지, 그 키가 일치하는지 확인하십시오.

```
Loser#show crypto key mypubkey dss
crypto public-key fred 02802219
 79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810
 C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E
quit

Loser#show crypto key pubkey-chain dss
crypto public-key barney 05694352
 B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED
 732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341
quit

--------

StHelen#show crypto key mypubkey dss
crypto public-key barney 05694352
 B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED
 732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341
quit

StHelen#show crypto key pubkey-chain dss
crypto public-key fred 02802219
 79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810
 C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E
quit
```

샘플 1:전용 링크를 위한 Cisco IOS 컨피그레이션

각 라우터에서 DSS 키가 생성되고 DSS 공개 키가 교환된 후 **crypto map** 명령을 인터페이스에 적용할 수 있습니다.암호화 세션은 암호화 맵에서 사용하는 액세스 목록과 일치하는 트래픽을 생성하는 것으로 시작합니다.

```
Loser#write terminal
Building configuration...

Current configuration:
!
! Last configuration change at 13:01:18 UTC Mon Mar 16 1998
! NVRAM config last updated at 13:03:02 UTC Mon Mar 16 1998
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname Loser
!
enable secret 5 $1$AeuFSMx7O/DhpqjLKc2VQVbeC0
!
ip subnet-zero
no ip domain-lookup
crypto map oldstyle 10
 set peer barney
 match address 133
!
crypto key pubkey-chain dss
 named-key barney
```

```
  serial-number 05694352
  key-string
   B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED
   732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341
  quit
!
interface Ethernet0
 ip address 40.40.40.41 255.255.255.0
 no ip mroute-cache
!
interface Serial0
 ip address 18.18.18.18 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 shutdown
!
interface Serial1
 ip address 19.19.19.19 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 clockrate 2400
 no cdp enable
 crypto map oldstyle
!
ip default-gateway 10.11.19.254
ip classless
ip route 0.0.0.0 0.0.0.0 19.19.19.20
access-list 133 permit ip 40.40.40.0 0.0.0.255 30.30.30.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 no exec
 transport input all
line vty 0 4
 password ww
 login
!
end

Loser#
--------------------------

StHelen#write terminal
Building configuration...

Current configuration:
!
! Last configuration change at 13:03:05 UTC Mon Mar 16 1998
! NVRAM config last updated at 13:03:07 UTC Mon Mar 16 1998
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname StHelen
!
boot system flash c2500-is56-l
enable password ww
!
partition flash 2 8 8
!
no ip domain-lookup
crypto map oldstyle 10
```

```
 set peer fred
 match address 144
!
crypto key pubkey-chain dss
 named-key fred
  serial-number 02802219
  key-string
   79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810
   C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E
  quit
 !
 !
interface Ethernet0
 ip address 30.30.30.31 255.255.255.0
!
interface Ethernet1
 no ip address
 shutdown
!
interface Serial0
 no ip address
 encapsulation x25
 no ip mroute-cache
 shutdown
!
interface Serial1
 ip address 19.19.19.20 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 load-interval 30
 compress stac
 no cdp enable
 crypto map oldstyle
!
ip default-gateway 10.11.19.254
ip classless
ip route 0.0.0.0 0.0.0.0 19.19.19.19
access-list 144 permit ip 30.30.30.0 0.0.0.255 40.40.40.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 transport input all
line vty 0 4
 password ww
 login
!
end

StHelen#
```

샘플 2:멀티포인트 프레임 릴레이를 위한 Cisco IOS 컨피그레이션

다음 샘플 명령 출력은 HUB 라우터에서 가져왔습니다.

```
Loser#write terminal
Building configuration...

Current configuration:
!
! Last configuration change at 10:45:20 UTC Wed Mar 11 1998
! NVRAM config last updated at 18:28:27 UTC Tue Mar 10 1998
```

```
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname Loser
!
enable secret 5 $1$AeuFSMx7O/DhpqjLKc2VQVbeC0
!
ip subnet-zero
no ip domain-lookup
!
crypto map oldstuff 10
 set peer barney
 match address 133
crypto map oldstuff 20
 set peer wilma
 match address 144
!
crypto key pubkey-chain dss
 named-key barney
  serial-number 05694352
  key-string
   1D460DC3 BDC73312 93B7E220 1861D55C E00DA5D8 DB2B04CD FABD297C 899D40E7
   D284F07D 6EEC83B8 E3676EC2 D813F7C8 F532DC7F 0A9913E7 8A6CB7E9 BE18790D
  quit
 named-key wilma
  serial-number 01496536
  key-string
   C26CB3DD 2A56DD50 CC2116C9 2697CE93 6DBFD824 1889F791 9BF36E70 7B29279C
   E343C56F 32266443 989B4528 1CF32C2D 9E3F2447 A5DBE054 879487F6 26A55939
  quit
!
crypto cisco pregen-dh-pairs 5
!
crypto cisco key-timeout 1440
!
interface Ethernet0
 ip address 190.190.190.190 255.255.255.0
 no ip mroute-cache
!
interface Serial1
 ip address 19.19.19.19 255.255.255.0
 encapsulation frame-relay
 no ip mroute-cache
 clockrate 500000
 crypto map oldstuff
!
!
ip default-gateway 10.11.19.254
ip classless
ip route 200.200.200.0 255.255.255.0 19.19.19.20
ip route 210.210.210.0 255.255.255.0 19.19.19.21
access-list 133 permit ip 190.190.190.0 0.0.0.255 200.200.200.0 0.0.0.255
access-list 144 permit ip 190.190.190.0 0.0.0.255 210.210.210.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 no exec
 transport input all
line vty 0 4
 password ww
 login
```

```
!
end

Loser#
```

다음 샘플 명령 출력은 원격 사이트 A에서 가져왔습니다.

```
WAN-2511a#write terminal
Building configuration...

Current configuration:
!
version 11.3
no service password-encryption
!
hostname WAN-2511a
!
enable password ww
!
no ip domain-lookup
!
crypto map mymap 10
 set peer fred
 match address 133
!
crypto key pubkey-chain dss
 named-key fred
  serial-number 02802219
  key-string
   56841777 4F27A574 5005E0F0 CF3C33F5 C6AAD000 5518A8FF 7422C592 021B295D
   D95AAB73 01235FD8 40D70284 3A63A38E 216582E8 EC1F8B0D 0256EFF5 0EE89436
  quit
!
interface Ethernet0
 ip address 210.210.210.210 255.255.255.0
 shutdown
!
interface Serial0
 ip address 19.19.19.21 255.255.255.0
 encapsulation frame-relay
 no fair-queue
 crypto map mymap
!
ip default-gateway 10.11.19.254
ip classless
ip route 190.190.190.0 255.255.255.0 19.19.19.19
access-list 133 permit ip 210.210.210.0 0.0.0.255 190.190.190.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line 1
 no exec
 transport input all
line 2 16
 no exec
line aux 0
line vty 0 4
 password ww
 login
!
end

WAN-2511a#
```

다음 샘플 명령 출력은 원격 사이트 B에서 가져왔습니다.

```
StHelen#write terminal
Building configuration...

Current configuration:
!
! Last configuration change at 19:00:34 UTC Tue Mar 10 1998
! NVRAM config last updated at 18:48:39 UTC Tue Mar 10 1998
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname StHelen
!
boot system flash c2500-is56-l
enable password ww
!
partition flash 2 8 8
!
no ip domain-lookup
!
crypto map wabba 10
 set peer fred
 match address 144
!
crypto key pubkey-chain dss
 named-key fred
  serial-number 02802219
  key-string
   56841777 4F27A574 5005E0F0 CF3C33F5 C6AAD000 5518A8FF 7422C592 021B295D
   D95AAB73 01235FD8 40D70284 3A63A38E 216582E8 EC1F8B0D 0256EFF5 0EE89436
  quit
!
interface Ethernet0
 ip address 200.200.200.200 255.255.255.0
!
interface Serial1
 ip address 19.19.19.20 255.255.255.0
 encapsulation frame-relay
 no ip mroute-cache
 crypto map wabba
!
ip default-gateway 10.11.19.254
ip classless
ip route 190.190.190.0 255.255.255.0 19.19.19.19
access-list 144 permit ip 200.200.200.0 0.0.0.255 190.190.190.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 transport input all
line vty 0 4
 password ww
 login
!
end

StHelen#
```

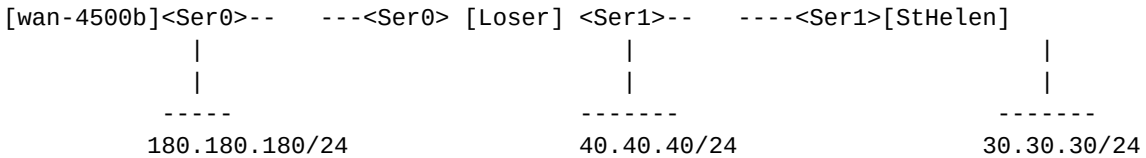
다음 샘플 명령 출력은 Frame Relay 스위치에서 가져왔습니다.

```
Current configuration:
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname wan-4700a
!
enable password ww
!
no ip domain-lookup
frame-relay switching
!
interface Serial0
 no ip address
 encapsulation frame-relay
 clockrate 500000
 frame-relay intf-type dce
 frame-relay route 200 interface Serial1 100
!
interface Serial1
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
 frame-relay route 100 interface Serial0 200
 frame-relay route 300 interface Serial2 200
!
interface Serial2
 no ip address
 encapsulation frame-relay
 clockrate 500000
 frame-relay intf-type dce
 frame-relay route 200 interface Serial1 300
!
```

샘플 3:라우터를 통한 암호화

피어 라우터는 한 홉이 아닐 수 있습니다.원격 라우터로 피어링 세션을 생성할 수 있습니다.다음 예에서 목표는 180.180.180.0/24에서 40.40.40.0/24 사이 및 180.180.180.0/24에서 30.30.30.0/24 사이의 모든 네트워크 트래픽을 암호화하는 것입니다. 40.40.40.0/24에서 30.30.30.0/24 사이의 트래픽은 암호화할 필요가 없습니다.

라우터 wan-4500b는 Loser 및 StHelen과의 암호화 세션 연결을 제공합니다.wan-4500b 이더넷 세그먼트에서 StHelen의 이더넷 세그먼트로 트래픽을 암호화하면 Loser에서 불필요한 암호 해독 단계를 피할 수 있습니다.Loser는 암호화된 트래픽을 StHelen의 직렬 인터페이스에 전달하기만 하면 해독됩니다.이렇게 하면 라우터 Loser의 IP 패킷 및 CPU 사이클에 대한 트래픽 지연이 줄어듭니다.더 중요한 것은, Loser의 엿듣는 사람은 트래픽을 읽을 수 없기 때문에 시스템 보안을 크게 향상시킵니다.Loser가 트래픽의 암호를 해독하는 경우 해독된 데이터가 전환될 가능성이 있습니다.




```
wan-4500b#write terminal
Building configuration...
```

```
Current configuration:
!
version 11.3
no service password-encryption
!
hostname wan-4500b
!
enable password 7 111E0E
!
username cse password 0 ww
no ip domain-lookup
!
crypto map toworld 10
 set peer loser
 match address 133
crypto map toworld 20
 set peer sthelen
 match address 144
!
crypto key pubkey-chain dss
 named-key loser
  serial-number 02802219
  key-string
   F0BE2128 752D1A24 F394B355 3216BA9B 7C4E8677 29C176F9 A047B7D9 7D03BDA4
   6B7AFDC2 2DAEF3AB 393EE7C7 802C1A95 B40031D1 908004F9 8A33A352 FF19BC24
  quit
 named-key sthelen
  serial-number 05694352
  key-string
   5C401002 404DC5A9 EAED2360 D7007E51 4A4BB8F8 6F9B1554 51D8ACBB D3964C10
   A23848CA 46003A94 2FC8C7D6 0B57AE07 9EB5EF3A BD71482B 052CF06B 90C3C618
  quit
 !
interface Ethernet0
 ip address 180.180.180.180 255.255.255.0
!
interface Serial0
 ip address 18.18.18.19 255.255.255.0
 encapsulation ppp
 crypto map toworld
!
router rip
 network 18.0.0.0
 network 180.180.0.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 30.30.30.31
ip route 171.68.118.0 255.255.255.0 10.11.19.254
access-list 133 permit ip 180.180.180.0 0.0.0.255 40.40.40.0 0.0.0.255
access-list 144 permit ip 180.180.180.0 0.0.0.255 30.30.30.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 password 7 044C1C
line vty 0 4
 login local
!
end

wan-4500b#

--------------------
```

```
Loser#write terminal
Building configuration...

Current configuration:
!
! Last configuration change at 11:01:54 UTC Wed Mar 18 1998
! NVRAM config last updated at 11:09:59 UTC Wed Mar 18 1998
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname Loser
!
enable secret 5 $1$AeuFSMx7O/DhpqjLKc2VQVbeC0
!
ip subnet-zero
no ip domain-lookup
ip host StHelen.cisco.com 19.19.19.20
ip domain-name cisco.com
!
crypto map towan 10
 set peer wan
 match address 133
!
crypto key pubkey-chain dss
 named-key wan
  serial-number 07365004
  key-string
   A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
   2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
  quit
!
interface Ethernet0
 ip address 40.40.40.40 255.255.255.0
 no ip mroute-cache
!
interface Serial0
 ip address 18.18.18.18 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 clockrate 64000
 crypto map towan
!
interface Serial1
 ip address 19.19.19.19 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 priority-group 1
 clockrate 64000
!
!
router rip
 network 19.0.0.0
 network 18.0.0.0
 network 40.0.0.0
!
ip default-gateway 10.11.19.254
ip classless
access-list 133 permit ip 40.40.40.0 0.0.0.255 180.180.180.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
```

```
 no exec
 transport input all
line vty 0 4
 password ww
 login
!
end

Loser#

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

StHelen#write terminal
Building configuration...

Current configuration:
!
! Last configuration change at 11:13:18 UTC Wed Mar 18 1998
! NVRAM config last updated at 11:21:30 UTC Wed Mar 18 1998
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname StHelen
!
boot system flash c2500-is56-l
enable password ww
!
partition flash 2 8 8
!
no ip domain-lookup
!
crypto map towan 10
 set peer wan
 match address 144
!
crypto key pubkey-chain dss
 named-key wan
  serial-number 07365004
  key-string
   A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
   2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
  quit
!
interface Ethernet0
 no ip address
!
interface Ethernet1
 ip address 30.30.30.30 255.255.255.0
!
interface Serial1
 ip address 19.19.19.20 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 load-interval 30
 crypto map towan
!
router rip
 network 30.0.0.0
 network 19.0.0.0
!
ip default-gateway 10.11.19.254
ip classless
```

```
access-list 144 permit ip 30.30.30.0 0.0.0.255 180.180.180.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 transport input all
line vty 0 4
 password ww
 login
!
end

StHelen#

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

wan-4500b#show crypto cisco algorithms
  des cfb-64
  40-bit-des cfb-64

wan-4500b#show crypto cisco key-timeout
Session keys will be re-negotiated every 30 minutes

wan-4500b#show crypto cisco pregen-dh-pairs
Number of pregenerated DH pairs: 0

wan-4500b#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 1    Serial0         18.18.18.19 set    DES_56_CFB64    1683     1682
 5    Serial0         18.18.18.19 set    DES_56_CFB64    1693     1693

wan-4500b#show crypto engine connections dropped-packet
Interface            IP-Address    Drop Count

Serial0              18.18.18.19   52
wan-4500b#show crypto engine configuration
slot:               0
engine name:        wan
engine type:        software
serial number:      07365004
platform:           rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    303
input queue bot:    303
input queue count:  0

wan-4500b#show crypto key mypubkey dss
crypto public-key wan 07365004
 A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
quit

wan-4500b#show crypto key pubkey-chain dss
crypto public-key loser 02802219
 F0BE2128 752D1A24 F394B355 3216BA9B 7C4E8677 29C176F9 A047B7D9 7D03BDA4
 6B7AFDC2 2DAEF3AB 393EE7C7 802C1A95 B40031D1 908004F9 8A33A352 FF19BC24
quit
crypto public-key sthelen 05694352
 5C401002 404DC5A9 EAED2360 D7007E51 4A4BB8F8 6F9B1554 51D8ACBB D3964C10
 A23848CA 46003A94 2FC8C7D6 0B57AE07 9EB5EF3A BD71482B 052CF06B 90C3C618
quit
```

```
wan-4500b#show crypto map interface serial 1
No crypto maps found.

wan-4500b#show crypto map
Crypto Map "toworld" 10 cisco
        Connection Id = 1        (1 established,    0 failed)
        Peer = loser
        PE = 180.180.180.0
        UPE = 40.40.40.0
        Extended IP access list 133
            access-list 133 permit ip
                source: addr = 180.180.180.0/0.0.0.255
                dest:   addr = 40.40.40.0/0.0.0.255

Crypto Map "toworld" 20 cisco
        Connection Id = 5        (1 established,    0 failed)
        Peer = sthelen
        PE = 180.180.180.0
        UPE = 30.30.30.0
        Extended IP access list 144
            access-list 144 permit ip
                source: addr = 180.180.180.0/0.0.0.255
                dest:   addr = 30.30.30.0/0.0.0.255

wan-4500b#

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

Loser#show crypto cisco algorithms
  des cfb-64
  des cfb-8
  40-bit-des cfb-64
  40-bit-des cfb-8

Loser#show crypto cisco key-timeout
Session keys will be re-negotiated every 30 minutes

Loser#show crypto cisco pregen-dh-pairs
Number of pregenerated DH pairs: 10

Loser#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 61   Serial0         18.18.18.18 set    DES_56_CFB64    1683     1682

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

Serial0              18.18.18.18   1
Serial1              19.19.19.19   90
Loser#show crypto engine configuration
slot:               0
engine name:        loser
engine type:        software
serial number:      02802219
platform:           rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    235
input queue bot:    235
input queue count:  0

Loser#show crypto key mypubkey dss
crypto public-key loser 02802219
```

```
 F0BE2128 752D1A24 F394B355 3216BA9B 7C4E8677 29C176F9 A047B7D9 7D03BDA4
 6B7AFDC2 2DAEF3AB 393EE7C7 802C1A95 B40031D1 908004F9 8A33A352 FF19BC24
quit

Loser#show crypto key pubkey-chain dss
crypto public-key wan 07365004
 A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
quit

Loser#show crypto map interface serial 1
No crypto maps found.

Loser#show crypto map
Crypto Map "towan" 10 cisco
        Connection Id = 61       (0 established,    0 failed)
        Peer = wan
        PE = 40.40.40.0
        UPE = 180.180.180.0
        Extended IP access list 133
            access-list 133 permit ip
                source: addr = 40.40.40.0/0.0.0.255
                dest:   addr = 180.180.180.0/0.0.0.255

Loser#

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

StHelen#show crypto cisco algorithms
  des cfb-64

StHelen#show crypto cisco key-timeout
Session keys will be re-negotiated every 30 minutes

StHelen#show crypto cisco pregen-dh-pairs
Number of pregenerated DH pairs: 10

StHelen#show crypto engine connections active

ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 58   Serial1         19.19.19.20 set    DES_56_CFB64    1694     1693

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

Ethernet0            0.0.0.0       1
Serial1              19.19.19.20   80
StHelen#show crypto engine configuration
slot:               0
engine name:        sthelen
engine type:        software
serial number:      05694352
platform:           rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    220
input queue bot:    220
input queue count:  0

StHelen#show crypto key mypubkey dss
crypto public-key sthelen 05694352
 5C401002 404DC5A9 EAED2360 D7007E51 4A4BB8F8 6F9B1554 51D8ACBB D3964C10
 A23848CA 46003A94 2FC8C7D6 0B57AE07 9EB5EF3A BD71482B 052CF06B 90C3C618
```

```
quit

StHelen#show crypto key pubkey-chain dss
crypto public-key wan 07365004
 A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
quit

StHelen#show crypto map interface serial 1
Crypto Map "towan" 10 cisco
        Connection Id = 58       (1 established,    0 failed)
        Peer = wan
        PE = 30.30.30.0
        UPE = 180.180.180.0
        Extended IP access list 144
            access-list 144 permit ip
                source: addr = 30.30.30.0/0.0.0.255
                dest:   addr = 180.180.180.0/0.0.0.255

StHelen#show crypto map
Crypto Map "towan" 10 cisco
        Connection Id = 58       (1 established,    0 failed)
        Peer = wan
        PE = 30.30.30.0
        UPE = 180.180.180.0
        Extended IP access list 144
            access-list 144 permit ip
                source: addr = 30.30.30.0/0.0.0.255
                dest:   addr = 180.180.180.0/0.0.0.255

StHelen#
```

샘플 4:DDR을 사용한 암호화

Cisco IOS는 ICMP를 사용하여 암호화 세션을 설정하므로 DDR 링크를 통해 암호화를 수행할 때 다이얼러 목록에서 ICMP 트래픽을 "관심"으로 분류해야 합니다.

참고: 압축은 Cisco IOS Software Release 11.3에서 작동하지만 암호화된 데이터에는 사용률이 높지 않습니다.암호화된 데이터는 상당히 무작위적인 모습이므로 압축으로 인해 속도가 느려질 뿐입니다.그러나 암호화되지 않은 트래픽에 대해서는 이 기능을 켜두면 됩니다.

경우에 따라 동일한 라우터에 다이얼 백업을 수행해야 합니다.예를 들어, 사용자가 WAN 네트워크에서 특정 링크의 장애를 보호하고자 할 때 사용하는 연료입니다.두 인터페이스가 동일한 피어로 이동하는 경우 두 인터페이스에서 동일한 암호화 맵을 사용할 수 있습니다.이 기능이 제대로 작동하려면 백업 인터페이스를 사용해야 합니다.백업 설계에서 라우터가 다른 상자에 다이얼하는 경우 다른 암호화 맵을 만들고 그에 따라 피어를 설정해야 합니다.또한 **backup interface** 명령을 사용해야 합니다.

```
dial-5#write terminal
Building configuration...

Current configuration:
!
version 11.3
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname dial-5
!
```

```
boot system c1600-sy56-l 171.68.118.83
enable secret 5 $1$oNe1wDbhBdcN6x9Y5gfuMjqh10
!
username dial-6 password 0 cisco
isdn switch-type basic-ni1
!
crypto map dial6 10
 set peer dial6
 match address 133
!
crypto key pubkey-chain dss
 named-key dial6
  serial-number 05679987
  key-string
   753F71AB E5305AD4 3FCDFB6D 47AA2BB5 656BFCAA 53DBE37F 07465189 06E91A82
   2BC91236 13DC4AA8 7EC5B48C D276E5FE 0D093014 6D3061C5 03158820 B609CA7C
  quit
!
interface Ethernet0
 ip address 20.20.20.20 255.255.255.0
!
interface BRI0
 ip address 10.10.10.11 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 load-interval 30
 dialer idle-timeout 9000
 dialer map ip 10.10.10.10 name dial-6 4724118
 dialer hold-queue 40
 dialer-group 1
 isdn spid1 919472417100 4724171
 isdn spid2 919472417201 4724172
 compress stac
 ppp authentication chap
 ppp multilink
 crypto map dial6
!
ip classless
ip route 40.40.40.0 255.255.255.0 10.10.10.10
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

dial-5#

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

dial-6#write terminal
Building configuration...

Current configuration:
!
version 11.3
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
```

```
hostname dial-6
!
boot system c1600-sy56-l 171.68.118.83
enable secret 5 $1$VdPYuA/BIVeEm9UAFEm.PPJFc.
!
username dial-5 password 0 cisco
no ip domain-lookup
isdn switch-type basic-ni1
!
 crypto map dial5 10
 set peer dial5
 match address 144
!
crypto key pubkey-chain dss
 named-key dial5
  serial-number 05679919
  key-string
   160AA490 5B9B1824 24769FCD EE5E0F46 1ABBD343 4C0C4A03 4B279D6B 0EE5F65F
   F64665D4 1036875A 8CF93691 BDF81722 064B51C9 58D72E12 3E1894B6 64B1D145
  quit
 !
!
interface Ethernet0
 ip address 40.40.40.40 255.255.255.0
!
interface BRI0
 ip address 10.10.10.10 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 dialer idle-timeout 9000
 dialer map ip 10.10.10.11 name dial-5 4724171
 dialer hold-queue 40
 dialer load-threshold 5 outbound
 dialer-group 1
 isdn spid1 919472411800 4724118
 isdn spid2 919472411901 4724119
 compress stac
 ppp authentication chap
 ppp multilink
 crypto map dial5
!
ip classless
ip route 20.20.20.0 255.255.255.0 10.10.10.11
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

dial-6#
```

샘플 5:IP 터널에서 IPX 트래픽 암호화

이 예에서는 IP 터널의 IPX 트래픽이 암호화됩니다.

참고: 이 터널(IPX)의 트래픽만 암호화됩니다.다른 모든 IP 트래픽은 단독으로 유지됩니다.

```
WAN-2511a#write terminal
Building configuration...

Current configuration:
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname WAN-2511a
!
enable password ww
!
no ip domain-lookup
ipx routing 0000.0c34.aa6a
!
crypto public-key wan2516 01698232
 B1C127B0 78D79CAA 67ECAD80 03D354B1 9012C80E 0C1266BE 25AEDE60 37A192A2
 B066D299 77174D48 7FBAB5FC 2B60893A 37E5CB7B 62F6D902 9495733B 98046962
 quit
!
crypto map wan2516 10
 set peer wan2516
 match address 133
!
!
interface Loopback1
 ip address 50.50.50.50 255.255.255.0
!
interface Tunnel1
 no ip address
 ipx network 100
 tunnel source 50.50.50.50
 tunnel destination 60.60.60.60
 crypto map wan2516
!
interface Ethernet0
 ip address 40.40.40.40 255.255.255.0
 ipx network 600
!
interface Serial0
 ip address 20.20.20.21 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 crypto map wan2516
!
interface Serial1
 no ip address
 shutdown
!
ip default-gateway 10.11.19.254
ip classless
ip route 0.0.0.0 0.0.0.0 20.20.20.20
access-list 133 permit ip host 50.50.50.50 host 60.60.60.60
!
line con 0
 exec-timeout 0 0
 password ww
 login
line 1 16
line aux 0
 password ww
 login
```

```
line vty 0 4
 password ww
 login
!
end

WAN-2511a#

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

WAN-2516a#write terminal
Building configuration...

Current configuration:
!
version 11.2
no service pad
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname WAN-2516a
!
enable password ww
!
no ip domain-lookup
ipx routing 0000.0c3b.cc1e
!
crypto public-key wan2511 01496536
 C8EA7C21 DF3E48F5 C6C069DB 3A5E1B08 8B830AD4 4F1DABCE D62F5F46 ED08C81D
 5646DC78 DDC77EFC 823F302A F112AF97 668E39A1 E2FCDC05 545E0529 9B3C9553
 quit
!
crypto map wan2511 10
 set peer wan2511
 match address 144
!
!
hub ether 0 1
 link-test
 auto-polarity
!
! <other hub interfaces snipped>
!
hub ether 0 14
 link-test
 auto-polarity
!
interface Loopback1
 ip address 60.60.60.60 255.255.255.0
!
interface Tunnel1
 no ip address
 ipx network 100
 tunnel source 60.60.60.60
 tunnel destination 50.50.50.50
 crypto map wan2511
!
interface Ethernet0
 ip address 30.30.30.30 255.255.255.0
 ipx network 400
!
interface Serial0
 ip address 20.20.20.20 255.255.255.0
```

```
 encapsulation ppp
 clockrate 2000000
 crypto map wan2511
!
interface Serial1
 no ip address
 shutdown
!
interface BRI0
 no ip address
 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 host 60.60.60.60 host 50.50.50.50
access-list 188 permit gre any any
!
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

WAN-2516a#
------------------------

WAN-2511a#show ipx route
Codes: C - Connected primary network,    c - Connected secondary network
       S - Static, F - Floating static, L - Local (internal), W - IPXWAN
       R - RIP, E - EIGRP, N - NLSP, X - External, A - Aggregate
       s - seconds, u - uses

3 Total IPX routes. Up to 1 parallel paths and 16 hops allowed.

No default route known.

C        100 (TUNNEL),        Tu1
C        600 (NOVELL-ETHER),  Et0
R        400 [151/01] via      100.0000.0c3b.cc1e,   24s, Tu1


WAN-2511a#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 1    Serial0         20.20.20.21 set    DES_56_CFB64    207      207


WAN-2511a#ping 400.0000.0c3b.cc1e
Translating "400.0000.0c3b.cc1e"

Type escape sequence to abort.
Sending 5, 100-byte IPX cisco Echoes to 400.0000.0c3b.cc1e, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/35/48 ms
```

```
WAN-2511a#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 1    Serial0         20.20.20.21 set    DES_56_CFB64    212      212


WAN-2511a#ping 30.30.30.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.30.30.30, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms


WAN-2511a#show crypto engine connections active

ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 1    Serial0         20.20.20.21 set    DES_56_CFB64    212      212

WAN-2511a#
```

샘플 6:L2F 터널 암호화

이 예에서는 다이얼링하는 사용자의 L2F 트래픽만 암호화하려고 합니다.여기서 "user@cisco.com"은 도시에서 "DEMO2"라는 로컬 NAS(Network Access Server)를 호출하고 홈 게이트웨이 CD로 터널링됩니다.모든 DEMO2 트래픽(다른 L2F 발신자의 트래픽 포함)이 암호화됩니다.L2F는 UDP 포트 1701을 사용하므로, 어떤 트래픽이 암호화되는지 확인하는 액세스 목록이 생성되는 방식입니다.

참고: 암호화 연결이 설정되지 않은 경우 발신자가 L2F 터널을 만든 첫 번째 사람임을 의미하며 암호화 연결 설정 지연으로 인해 발신자가 삭제될 수 있습니다.CPU 전원이 충분한 라우터에서는 이러한 문제가 발생하지 않을 수 있습니다.또한 암호화 설정 및 해제가 피크 시간이 아닐 때만 발생하도록 키 시간 제한을 늘릴 수 있습니다.

다음 샘플 명령 출력은 원격 NAS에서 가져왔습니다.

```
DEMO2#write terminal
Building configuration...

Current configuration:
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname DEMO2
!
enable password ww
!
username NAS1 password 0 SECRET
username HomeGateway password 0 SECRET
no ip domain-lookup
vpdn enable
vpdn outgoing cisco.com NAS1 ip 20.20.20.20
!
crypto public-key wan2516 01698232
 B1C127B0 78D79CAA 67ECAD80 03D354B1 9012C80E 0C1266BE 25AEDE60 37A192A2
 B066D299 77174D48 7FBAB5FC 2B60893A 37E5CB7B 62F6D902 9495733B 98046962
```

```
 quit
!
crypto map vpdn 10
 set peer wan2516
 match address 133
!
crypto key-timeout 1440
!
interface Ethernet0
 ip address 40.40.40.40 255.255.255.0
!
interface Serial0
 ip address 20.20.20.21 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 crypto map vpdn
!
interface Serial1
 no ip address
 shutdown
!
interface Group-Async1
 no ip address
 encapsulation ppp
 async mode dedicated
 no peer default ip address
 no cdp enable
 ppp authentication chap pap
 group-range 1 16
!
ip default-gateway 10.11.19.254
ip classless
ip route 0.0.0.0 0.0.0.0 20.20.20.20
access-list 133 permit udp host 20.20.20.21 eq 1701
 host 20.20.20.20 eq 1701
!
!
line con 0
 exec-timeout 0 0
 password ww
 login
line 1 16
 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

DEMO2#
```

다음 샘플 명령 출력은 홈 게이트웨이에서 가져왔습니다.

```
CD#write terminal
Building configuration...
```

```
Current configuration:
!
version 11.2
no service pad
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname CD
!
enable password ww
!
username NAS1 password 0 SECRET
username HomeGateway password 0 SECRET
username user@cisco.com password 0 cisco
no ip domain-lookup
vpdn enable
vpdn incoming NAS1 HomeGateway virtual-template 1
!
crypto public-key wan2511 01496536
 C8EA7C21 DF3E48F5 C6C069DB 3A5E1B08 8B830AD4 4F1DABCE D62F5F46 ED08C81D
 5646DC78 DDC77EFC 823F302A F112AF97 668E39A1 E2FCDC05 545E0529 9B3C9553
 quit
!
crypto key-timeout 1440
!
crypto map vpdn 10
 set peer wan2511
 match address 144
!
!
hub ether 0 1
 link-test
 auto-polarity
!
interface Loopback0
 ip address 70.70.70.1 255.255.255.0
!
interface Ethernet0
 ip address 30.30.30.30 255.255.255.0
!
interface Virtual-Template1
 ip unnumbered Loopback0
 no ip mroute-cache
 peer default ip address pool default
 ppp authentication chap
!
interface Serial0
 ip address 20.20.20.20 255.255.255.0
 encapsulation ppp
 clockrate 2000000
 crypto map vpdn
!
interface Serial1
 no ip address
 shutdown
!
interface BRI0
 no ip address
 shutdown
!
ip local pool default 70.70.70.2 70.70.70.77
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 udp host 20.20.20.20 eq 1701 host 20.20.20.21 eq 1701
!
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
```

문제 해결

일반적으로 다음 **show** 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	
show crypto cisco 알고리즘	show crypto cisco key-timeout
show crypto cisco pregen dh-pairs	* 활성 암호화 엔진 연결 표시
show crypto engine connections dropped-packet 표시	암호화 엔진 구성 표시
암호화 키 mypubkey dss 표시	* show crypto key pubkey-chain dss
show crypto map interface serial 1	* show crypto map
디버그 암호화 엔진	* 디버그 암호화 세션
디버그 키	암호화 연결 지우기
암호화 제로	crypto 공개 키 없음

- **show crypto cisco 알고리즘**- 다른 피어 암호화 라우터와 통신하는 데 사용되는 모든 DES(Data Encryption Standard) 알고리즘을 활성화해야 합니다.DES 알고리즘을 활성화하지 않으면 나중에 **암호화 맵**에 알고리즘을 할당하려고 해도 해당 알고리즘을 사용할 수 없습니다.라우터가 피어 라우터와의 암호화된 통신 세션을 설정하려고 하는데 두 라우터의 양쪽 끝에서 동일한 DES 알고리즘이 활성화되지 않으면 암호화된 세션이 실패합니다.양쪽 끝에서 하나 이상의 공통 DES 알고리즘이 활성화된 경우 암호화된 세션을 계속할 수 있습니다.**참고:** cisco라는 추가 단어가 Cisco IOS Software Release 11.3에 나타나며 Cisco IOS Software Release 11.2에서 발견된 IPSec과 Cisco 독점 암호화를 구분해야 합니다.

```
Loser#show crypto cisco algorithms
  des cfb-64
  des cfb-8
  40-bit-des cfb-64
  40-bit-des cfb-8
```

- **show crypto cisco key-timeout** - 암호화된 통신 세션이 설정된 후 특정 시간 동안 유효합니다 .이 시간이 지나면 세션이 시간 초과됩니다.새 세션을 협상해야 하며 암호화된 통신을 계속하려면 새 DES(세션) 키를 생성해야 합니다.암호화된 통신 세션이 만료되기 전에 지속되는 시간을 변경하려면 이 명령을 사용합니다(시간 초과).

```
Loser#show crypto cisco key-timeout
Session keys will be re-negotiated every 30 minutes
```

이 명령을 사용하여 DES 키를 재협상하기 전의 기간을 결정합니다.

```
StHelen#show crypto conn
Connection Table
PE              UPE         Conn_id New_id Algorithm    Time
0.0.0.1         0.0.0.1        4    0      DES_56_CFB64 Mar 01 1993 03:16:09
                flags:TIME_KEYS


StHelen#show crypto key
Session keys will be re-negotiated every 30 minutes

StHelen#show clock
*03:21:23.031 UTC Mon Mar 1 1993
```

- **show crypto cisco pregen-dh-pairs** - 암호화된 각 세션은 고유한 DH 번호 쌍을 사용합니다.새 세션이 설정될 때마다 새 DH 번호 쌍을 생성해야 합니다.세션이 완료되면 이 번호는 삭제됩니다.새 DH 번호 쌍을 생성하는 작업은 CPU 사용량이 많은 작업이며, 특히 로우엔드 라우터의 경우 세션 설정 속도가 느려질 수 있습니다.세션 설정을 가속화하기 위해 지정된 양의 DH 번호 쌍을 미리 생성하여 예약하도록 선택할 수 있습니다.그런 다음 암호화된 통신 세션이 설정되면 해당 예약에서 DH 번호 쌍이 제공됩니다.DH 번호 쌍을 사용한 후 예약은 새 DH 번호 쌍으로 자동으로 보충되므로 항상 사용할 준비가 된 DH 번호 쌍이 있습니다.라우터가 1~2개의 DH 번호 쌍의 사전 생성 예약을 너무 빨리 고갈되도록 여러 개의 암호화된 세션을 자주 설정하는 경우가 아니면 일반적으로 1~2개의 DH 번호 쌍을 미리 생성할 필요가 없습니다.

```
Loser#show crypto cisco pregen-dh-pairs
Number of pregenerated DH pairs: 10
```

- **활성 암호화 cisco 연결 표시**다음은 샘플 명령 출력입니다.

```
Loser#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 16   Serial1         19.19.19.19 set    DES_56_CFB64    376      884
```

- **show crypto cisco engine connections dropped-packet 표시**다음은 샘플 명령 출력입니다.

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

Serial1              19.19.19.19   39
```

- **show crypto engine configuration**(Cisco IOS Software Release 11.2에서 **crypto engine brief**를 **표시**)다음은 샘플 명령 출력입니다.

```
Loser#show crypto engine configuration
slot:               0
engine name:        fred
engine type:        software
serial number:      02802219
platform:           rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    465
input queue bot:    465
input queue count:  0
```

- **암호화 키 mypubkey dss 표시**다음은 샘플 명령 출력입니다.

```
Loser#show crypto key mypubkey dss
crypto public-key fred 02802219
 79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810
 C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E
quit
```

- **show crypto key pubkey chain dss**다음은 샘플 명령 출력입니다.

```
Loser#show crypto key pubkey-chain dss
crypto public-key barney 05694352
 B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED
 732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341
quit
```

- **show crypto map interface serial 1**다음은 샘플 명령 출력입니다.

```
Loser#show crypto map interface serial 1
Crypto Map "oldstyle" 10 cisco
        Connection Id = 16       (8 established,    0 failed)
        Peer = barney
        PE = 40.40.40.0
        UPE = 30.30.30.0
        Extended IP access list 133
            access-list 133 permit ip
                source: addr = 40.40.40.0/0.0.0.255
                dest:   addr = 30.30.30.0/0.0.0.255
```

ping 명령을 사용할 때 시간 차이를 확인합니다.

```
wan-5200b#ping 30.30.30.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.30.30.30, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/54/56 ms
wan-5200b#
-----------
wan-5200b#ping 30.30.30.31

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.30.30.31, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/53/56 ms
-----------------

wan-5200b#ping 19.19.19.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 19.19.19.20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/21/24 ms
------------
```

- **show crypto map interface serial 1**다음은 샘플 명령 출력입니다.

```
Loser#show crypto map
Crypto Map "oldstyle" 10 cisco
        Connection Id = 16       (8 established,    0 failed)
        Peer = barney
        PE = 40.40.40.0
        UPE = 30.30.30.0
        Extended IP access list 133
            access-list 133 permit ip
                source: addr = 40.40.40.0/0.0.0.255
                dest:   addr = 30.30.30.0/0.0.0.255
```

- **디버그 암호화 엔진**다음은 샘플 명령 출력입니다.

```
Loser#debug crypto engine
Mar 17 11:49:07.902: Crypto engine 0: generate alg param
```

```
Mar 17 11:49:07.906: CRYPTO_ENGINE: Dh phase 1 status: 0
Mar 17 11:49:07.910: Crypto engine 0: sign message using crypto engine
Mar 17 11:49:09.894: CRYPTO_ENGINE: packets dropped: State = 0
Mar 17 11:49:11.758: Crypto engine 0: generate alg param

Mar 17 11:49:12.246: CRYPTO_ENGINE: packets dropped: State = 0
Mar 17 11:49:13.342: CRYPTO ENGINE 0: get syndrome for conn id 25
Mar 17 11:49:13.346: Crypto engine 0: verify signature
Mar 17 11:49:14.054: CRYPTO_ENGINE: packets dropped: State = 0
Mar 17 11:49:14.402: Crypto engine 0: sign message using crypto engine
Mar 17 11:49:14.934: Crypto engine 0: create session for conn id 25
Mar 17 11:49:14.942: CRYPTO ENGINE 0: clear dh number for conn id 25
Mar 17 11:49:24.946: Crypto engine 0: generate alg param
```

- **디버그 암호화 세션 관리**다음은 샘플 명령 출력입니다.

```
StHelen#debug crypto sessmgmt

Mar 17 11:49:08.918: IP: s=40.40.40.40 (Serial1), d=30.30.30.30, len 328,
             Found an ICMP connection message.

Mar 17 11:49:08.922: CRYPTO: Dequeued a message: CIM
Mar 17 11:49:08.926: CRYPTO-SDU: Key Timeout, Re-exchange Crypto Keys
Mar 17 11:49:09.978: CRYPTO: Verify done. Status=OK
Mar 17 11:49:09.994: CRYPTO: DH gen phase 1 status for conn_id 22 slot 0:OK
Mar 17 11:49:11.594: CRYPTO: DH gen phase 2 status for conn_id 22 slot 0:OK
Mar 17 11:49:11.598: CRYPTO: Syndrome gen status for conn_id 22 slot 0:OK
Mar 17 11:49:12.134: CRYPTO: Sign done. Status=OK
Mar 17 11:49:12.142: CRYPTO: ICMP message sent: s=19.19.19.20, d=19.19.19.19
Mar 17 11:49:12.146: CRYPTO-SDU: act_on_nnc_req: NNC Echo Reply sent
Mar 17 11:49:12.154: CRYPTO: Create encryption key for conn_id 22 slot 0:OK
Mar 17 11:49:15.366: CRYPTO: Dequeued a message: CCM
Mar 17 11:49:15.370: CRYPTO: Syndrome gen status for conn_id 22 slot 0:OK
Mar 17 11:49:16.430: CRYPTO: Verify done. Status=OK
Mar 17 11:49:16.434: CRYPTO: Replacing -23 in crypto maps with 22 (slot 0)
Mar 17 11:49:26.438: CRYPTO: Need to pregenerate 1 pairs for slot 0.
Mar 17 11:49:26.438: CRYPTO: Pregenerating DH for conn_id 32 slot 0
Mar 17 11:49:28.050: CRYPTO: DH phase 1 status for conn_id 32 slot 0:OK
                             ~~ <---------- This is good ----------> ~~
```

암호화 맵에 잘못된 피어가 설정되어 있으면 이 오류 메시지가 표시됩니다.

```
Mar  2 12:19:12.639: CRYPTO-SDU:Far end authentication error:
          Connection message verify failed
```

암호화 알고리즘이 일치하지 않으면 이 오류 메시지가 표시됩니다.

```
Mar  2 12:26:51.091: CRYPTO-SDU: Connection
failed due to incompatible policy
```

DSS 키가 없거나 유효하지 않으면 이 오류 메시지가 표시됩니다.

```
Mar 16 13:33:15.703: CRYPTO-SDU:Far end authentication error:
           Connection message verify failed
```

- **디버그 암호화 키**다음은 샘플 명령 출력입니다.

```
StHelen#debug crypto key
Mar 16 12:16:45.795: CRYPTO-KE: Sent 4 bytes.
Mar 16 12:16:45.795: CRYPTO-KE: Sent 2 bytes.
Mar 16 12:16:45.799: CRYPTO-KE: Sent 6 bytes.
Mar 16 12:16:45.799: CRYPTO-KE: Sent 2 bytes.
Mar 16 12:16:45.803: CRYPTO-KE: Sent 64 bytes.

Mar 16 12:16:56.083: CRYPTO-KE: Received 4 bytes.
Mar 16 12:16:56.087: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:56.087: CRYPTO-KE: Received 4 bytes.
Mar 16 12:16:56.091: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:56.091: CRYPTO-KE: Received 52 bytes.
Mar 16 12:16:56.095: CRYPTO-KE: Received 12 bytes.
```

- **암호화 연결 지우기**다음은 샘플 명령 출력입니다.

```
wan-2511#show crypto engine connections act
```

```
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 9    Serial0         20.20.20.21 set    DES_56_CFB64    29       28

wan-2511#clear crypto connection 9
wan-2511#
*Mar  5 04:58:20.690: CRYPTO: Replacing 9 in crypto maps with 0 (slot 0)
*Mar  5 04:58:20.694: Crypto engine 0: delete connection 9
*Mar  5 04:58:20.694: CRYPTO: Crypto Engine clear conn_id 9 slot 0: OK
wan-2511#
wan-2511#show crypto engine connections act
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt

wan-2511#
```

- **암호화 제로**다음은 샘플 명령 출력입니다.

```
wan-2511#show crypto mypubkey
crypto public-key wan2511 01496536
 11F43C02 70C0ADB7 5DD50600 A0219E04 C867A5AF C40A4FE5 CE99CCAB A8ECA840
 EB95FBEE D727ED5B F0A6F042 BDB5529B DBB0698D DB0B2756 F6CABE8F 05E4B27F
quit

wan-2511#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
wan-2511(config)#crypto zeroize
Warning! Zeroize will remove your DSS signature keys.
Do you want to continue? [yes/no]: yes
% Keys to be removed are named wan2511.
Do you really want to remove these keys? [yes/no]: yes
% Zeroize done.

wan-2511(config)#^Z
wan-2511#
wan-2511#show crypto mypubkey
wan-2511#
```

- **crypto 공개 키 없음**다음은 샘플 명령 출력입니다.

```
wan-2511#show crypto pubkey
crypto public-key wan2516 01698232
 B1C127B0 78D79CAA 67ECAD80 03D354B1 9012C80E 0C1266BE 25AEDE60 37A192A2
 B066D299 77174D48 7FBAB5FC 2B60893A 37E5CB7B 62F6D902 9495733B 98046962
quit

wan-2511#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
wan-2511(config)#crypto public-key ?
  WORD  Peer name

wan-2511(config)#
wan-2511(config)#no crypto public-key wan2516 01698232
wan-2511(config)#^Z
wan-2511#
wan-2511#show crypto pubkey
wan-2511#
```

ESA를 통한 Cisco 7200 트러블슈팅

또한 Cisco는 ESA라고 하는 Cisco 7200 Series 라우터에서 암호화를 수행할 수 있는 하드웨어 지원 옵션을 제공합니다.ESA는 VIP2-40 카드용 포트 어댑터 또는 Cisco 7200용 독립형 포트 어댑터 형식입니다.이러한 배치를 통해 하드웨어 어댑터 또는 VIP2 소프트웨어 엔진을 사용하여 Cisco 7500 VIP2 카드의 인터페이스를 통해 들어오거나 나가는 데이터를 암호화하고 해독할 수 있습니다.Cisco 7200은 하드웨어 지원을 통해 Cisco 7200 섀시의 모든 인터페이스에 대한 트래픽을 암호화할 수 있습니다.암호화를 사용하면 라우팅 또는 기타 Cisco IOS 기능과 같은 다른 용도로 사용할 수

있는 귀중한 CPU 주기가 절약됩니다.

Cisco 7200에서 독립형 포트 어댑터는 Cisco IOS 소프트웨어 암호화 엔진과 정확히 동일하게 구성되지만, 일부 추가 명령은 하드웨어에만 사용되며 암호화를 수행할 엔진(소프트웨어 또는 하드웨어)을 결정하는 데 사용됩니다.

먼저 하드웨어 암호화를 위해 라우터를 준비합니다.

```
wan-7206a(config)#
%OIR-6-REMCARD: Card removed from slot 3, interfaces disabled
*Mar  2 08:17:16.739: ...switching to SW crypto engine

wan-7206a#show crypto card 3

Crypto card in slot: 3

Tampered:        No
Xtracted:        Yes
Password set:    Yes
DSS Key set:     Yes
FW version       0x5049702
wan-7206a#

wan-7206a(config)#

wan-7206a(config)#crypto zeroize 3
Warning! Zeroize will remove your DSS signature keys.
Do you want to continue? [yes/no]: yes
% Keys to be removed are named hard.
Do you really want to remove these keys? [yes/no]: yes
[OK]
```

아래와 같이 하드웨어 암호화를 활성화하거나 비활성화합니다.

```
wan-7206a(config)#crypto esa shutdown 3
...switching to SW crypto engine


wan-7206a(config)#crypto esa enable 3
There are no keys on the ESA in slot 3- ESA not enabled.
```

다음으로, ESA를 활성화하기 전에 키를 생성합니다.

```
wan-7206a(config)#crypto gen-signature-keys hard
% Initialize the crypto card password. You will need
   this password in order to generate new signature
   keys or clear the crypto card extraction latch.

Password:
Re-enter password:
Generating DSS keys ....
 [OK]

wan-7206a(config)#
wan-7206a#show crypto mypubkey
crypto public-key hard 00000052
 EE691A1F BD013874 5BA26DC4 91F17595 C8C06F4E F7F736F1 AD0CACEC 74AB8905
 DF426171 29257F8E B26D49B3 A8E11FB0 A3501B13 D3F19623 DCCE7322 3D97B804
quit
```

```
wan-7206a#
wan-7206a(config)#crypto esa enable 3
...switching to HW crypto engine

wan-7206a#show crypto engine brie
crypto engine name:   hard
crypto engine type:   ESA
serial number:        00000052
crypto engine state:  installed
crypto firmware version:  5049702
crypto engine in slot: 3

wan-7206a#
```

ESA로 VIP2 문제 해결

VIP2 카드의 ESA 하드웨어 포트 어댑터는 VIP2 카드의 인터페이스를 통해 들어오거나 나가는 데이터를 암호화하고 해독하는 데 사용됩니다.Cisco 7200과 마찬가지로 암호화 지원을 사용하면 귀중한 CPU 사이클이 절약됩니다.이 경우 **crypto esa enable** 명령은 ESA가 연결된 경우 ESA 포트 어댑터가 VIP2 카드의 포트에 대한 암호화를 수행하므로 존재하지 않습니다.ESA 포트 어댑터가 처음 설치되었거나 제거된 다음 다시 설치된 경우 암호화 지우기 래치를 해당 슬롯에 적용해야 합니다.

```
Router#show crypto card 11

Crypto card in slot: 11

Tampered:         No
Xtracted:         Yes
Password set:     Yes
DSS Key set:      Yes
FW version        0x5049702
Router#
```

ESA 암호화 모듈이 추출되었으므로 아래와 같이 해당 슬롯에서 crypto clear-**latch** 명령을 수행할 때까지 다음 오류 메시지가 표시됩니다.

```
----
*Jan 24 02:57:09.583: CRYPTO: Sign done. Status= Extraction latch set. Request not allowed.
-----
Router(config)#crypto clear-latch ?
  <0-15>  Chassis slot number

Router(config)#crypto clear-latch 11
% Enter the crypto card password.
Password:
Router(config)#^Z
```

이전에 할당된 비밀번호를 잊어버린 경우 crypto clear-latch 명령 대신 **crypto zeroize** 명령을 사용하여 ESA를 재설정합니다.crypto zeroize 명령을 실행한 후 DSS 키를 재생성하고 재교환해야 합니다.DSS 키를 재생성할 때 새 비밀번호를 생성하라는 메시지가 표시됩니다.다음은 예입니다.

```
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#show crypto card 11
```

```
Crypto card in slot: 11

Tampered:        No
Xtracted:        No
Password set:    Yes
DSS Key set:     Yes
FW version       0x5049702
Router#

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


Router#show crypto engine brief
crypto engine name:   TERT
crypto engine type:   software
serial number:        0459FC8C
crypto engine state:  dss key generated
crypto lib version:   5.0.0
crypto engine in slot: 6

crypto engine name:   WAAA
crypto engine type:   ESA
serial number:        00000078
crypto engine state:  dss key generated
crypto firmware version:  5049702
crypto engine in slot: 11

Router#
-----------
Router(config)#crypto zeroize
Warning! Zeroize will remove your DSS signature keys.
Do you want to continue? [yes/no]: yes
% Keys to be removed are named TERT.
Do you really want to remove these keys? [yes/no]: yes
% Zeroize done.

Router(config)#crypto zeroize  11
Warning! Zeroize will remove your DSS signature keys.
Do you want to continue? [yes/no]: yes
% Keys to be removed are named WAAA.
Do you really want to remove these keys? [yes/no]: yes
[OK]

Router(config)#^Z
Router#show crypto engine brief
crypto engine name:   unknown
crypto engine type:   software
serial number:        0459FC8C
crypto engine state:  installed
crypto lib version:   5.0.0
crypto engine in slot: 6

crypto engine name:   unknown
crypto engine type:   ESA
serial number:        00000078
crypto engine state:  installed
crypto firmware version:  5049702
crypto engine in slot: 11

Router#
--------------
Router(config)#crypto gen-signature-keys VIPESA 11
% Initialize the crypto card password. You will need
   this password in order to generate new signature
```

```
   keys or clear the crypto card extraction latch.

Password:
Re-enter password:
Generating DSS keys ....
 [OK]

Router(config)#
*Jan 24 01:39:52.923: Crypto engine 11: create key pairs.
^Z
Router#
------
Router#show crypto engine brief
crypto engine name:   unknown
crypto engine type:   software
serial number:        0459FC8C
crypto engine state:  installed
crypto lib version:   5.0.0
crypto engine in slot: 6

crypto engine name:   VIPESA
crypto engine type:   ESA
serial number:        00000078
crypto engine state:  dss key generated
crypto firmware version:  5049702
crypto engine in slot: 11

Router#
----------
Router#show crypto engine connections active 11
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 2    Serial11/0/0    20.20.20.21 set    DES_56_CFB64    9996     9996

Router#
Router#clear crypto connection 2 11
Router#
*Jan 24 01:41:04.611: CRYPTO: Replacing 2 in crypto maps with 0 (slot 11)
*Jan 24 01:41:04.611: Crypto engine 11: delete connection 2
*Jan 24 01:41:04.611: CRYPTO: Crypto Engine clear conn_id 2 slot 11: OK
Router#show crypto engine connections active 11
No connections.

Router#
*Jan 24 01:41:29.355: CRYPTO ENGINE:Number of connection entries
received from VIP 0
------------

Router#show crypto mypub
% Key for slot 11:
crypto public-key VIPESA 00000078
 CF33BA60 56FCEE01 2D4E32A2 5D7ADE70 6AF361EE 2964F3ED A7CE08BD A87BF7FE
 90A39F1C DF96143A 9B7B9C78 5F59445C 27860F1E 4CD92B6C FBC4CBCC 32D64508
quit

Router#show crypto pub
crypto public-key wan2516 01698232
 C5DE8C46 8A69932C 70C92A2C 729449B3 FD10AC4D 1773A997 7F6BA37D 61997AC3
 DBEDBEA7 51BF3ADD 2BB35CB5 B9126B4D 13ACF93E 0DF0CD22 CFAAC1A8 9CE82985
quit

Router#
----------
interface Serial11/0/0
 ip address 20.20.20.21 255.255.255.0
```

```
 encapsulation ppp
 ip route-cache distributed
 no fair-queue
 no cdp enable
 crypto map test
!
----------
Router#show crypto eng conn act 11
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 3    Serial11/0/0    20.20.20.21 set    DES_56_CFB64    761      760

Router#
*Jan 24 01:50:43.555: CRYPTO ENGINE:Number of connection
entries received from VIP 1

Router#
```

관련 정보

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