RED ISAKMP 및 Oakley 정보

목차

소개

이 문서에서는 ISAKMP(Internet Security Association and Key Management Protocol) 및 Oakley Key Decision Protocol에 대한 정보를 제공합니다.이러한 프로토콜은 IETF(Internet Engineering Task Force)의 IPSec Working Group 에서 고려하는 인터넷 키 관리의 선두 주자입니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

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

기술 정보

ISAKMP 정보

ISAKMP는 인터넷 키 관리를 위한 프레임워크를 제공하며 보안 특성의 협상을 위한 특정 프로토콜 지원을 제공합니다.세션 키만 설정되지 않습니다.그러나 Oakley와 같은 다양한 세션 키 설정 프로토콜과 함께 사용하여 인터넷 키 관리에 대한 완벽한 솔루션을 제공할 수 있습니다.ISAKMP 사양은 포스트스크립트에서도 사용할 수 있습니다.

오크리 정보

Oakley 프로토콜은 하이브리드 Diffie-Hellman 기술을 사용하여 인터넷 호스트 및 라우터에 세션 키를 설정합니다.Oakley는 PFS(Perfect Forward Secrecy)의 중요한 보안 속성을 제공하며, 상당한 공개 조사를 통과한 암호화 기술을 기반으로 합니다.오클리는 특성 협상이 필요하지 않거나, 오크리가 ISAKMP와 함께 사용될 수 있습니다.ISAKMP가 오클리와 함께 사용될 때 키 에스크로는 가능하지 않습니다.

ISAKMP와 Oakley 프로토콜은 하이브리드 프로토콜로 통합되었습니다.ISAKMP with Oakley의 해결은 ISAKMP 프레임워크를 사용하여 Oakley 키 교환 모드의 하위 집합을 지원합니다.이 새로운 키 교환 프로토콜은 선택 사항인 PFS, 전체 보안 연결 특성 협상, 거부 및 거부 방지 모두를 제공하는 인증 방법을 제공합니다.이 프로토콜의 구현을 사용하여 VPN을 설정하고, 원격 사이트(동적으로 할당된 IP 주소가 있을 수 있음)의 사용자가 보안 네트워크에 액세스할 수 있도록 허용할 수도 있습니다.

IPSec 정보

IETF의 IPSec 작업 그룹은 IPv4 및 IPv6에 대한 IP 레이어 보안 메커니즘에 대한 표준을 개발하며, 또한 인터넷에서 사용할 일반 키 관리 프로토콜을 개발하고 있습니다. 자세한 내용은 IP 보안 및 암호화 개요를 참조하십시오.

ISAKMP 소프트웨어

Cisco Systems 구현

Cisco Systems의 ISAKMP 데몬 소프트웨어는 인터넷 키 관리를 위한 표준 솔루션으로서 ISAKMP를 발전시키는 데 도움이 되는 상용 또는 비상업용 용도로 무료로 사용할 수 있습니다.

Cisco ISAKMP 소프트웨어는 미국 및 캐나다 내에서 MIT(Massachusetts Institute of Technology)의 웹 다운로드 양식 을 통해 사용할 수 있습니다. 미국의 수출 통제 법규로 인해 Cisco는 이 소프트웨어를 미국 및 캐나다 이외의 다른 국가에 배포할 수 없습니다.

Cisco ISAKMP 데몬은 PF_KEY API(Key Management Application Program Interface)를 사용하여 운영 체제 커널(이 API를 구현한) 및 주변 키 관리 인프라에 등록합니다.ISAKMP 데몬에서 협상한 보안 연결은 커널의 키 엔진에 삽입됩니다.그런 다음 시스템의 표준 IPSec 보안 메커니즘(인증 헤더 [AH] 및 보안 페이로드 캡슐화[ESP])에서 사용할 수 있습니다.

4.4BSD 파생 시스템(Berkeley Software Design, Inc. [BSDI] 및 NetBSD 포함)에 대해 자유롭게 배포할 수 있는 NRL(U.S. Naval Research Laboratory) IPv6, IPv6용 IPSec, IPv4용 IPSec 및 PF_KEY 인터페이스 등이 포함됩니다.NRL 소프트웨어는 MIT의 웹 다운로드 양식 을 통해 미국과 캐나다 내에서 사용할 수 있습니다.미국 및 캐나다 이외의 지역에서는 NRL 소프트웨어를 ftp://ftp.ripe.net/ipv6/nrl에서 FTP를 통해 사용할 수 있습니다 .

Cisco 데몬은 ISAKMP 버전 5를 기반으로 하며 Oakley Key Decision Protocol 버전 1의 기능을 사용합니다.

ISAKMP 및 Oakley에 대한 문제, 버그 수정, 이식 변경 사항, 일반적인 논의를 위한 메일 목록은 isakmp-oakley@cisco.com에서 확인되었습니다.이 목록에 참여하려면 **subscribe isakmp-oakley**의 메시지 본문이 포함된 이메일 요청을 다음으로 보냅니다.majordomo@cisco.com

미국 국방부(DoD) 구현

미국 정보 보안 연구소(DoD Office of Information Security Research)는 ISAKMP 프로토타입 구현을 미국 내에서 자유롭게 배포할 수 있도록 했습니다.웹 기반 인터페이스를 사용하여 소프트웨어를 다운로드할 수 있습니다.이 구현에는 세션 키 교환 기능이 포함되지 않지만 전체 ISAKMP 기능이 포함되어 있습니다.

관련 정보

- IPSec 지원 페이지
- Technical Support - Cisco Systems