Informações ISAKMP e Oakley VERMELHAS

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Conventions](#)
[Informações técnicas](#)
[Sobre o ISAKMP](#)
[Sobre Oakley](#)
[Sobre o IPSec](#)
[Software ISAKMP](#)
[Implementação dos sistemas Cisco](#)
[Implementação do Departamento de Defesa dos Estados Unidos (DoD)](#)
[Informações Relacionadas](#)

Introduction

Este documento fornece informações sobre o ISAKMP (Internet Security Association and Key Management Protocol) e o protocolo de determinação de chave Oakley. Esses protocolos são os principais concorrentes para o gerenciamento de chaves de Internet que estão sendo considerados pelo Grupo de Trabalho de IPSec da IETF (Internet Engineering Task Force).

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Informações técnicas

Sobre o ISAKMP

O ISAKMP fornece uma estrutura para o gerenciamento de chaves da Internet e fornece o suporte de protocolo específico para a negociação de atributos de segurança. Sozinho, não estabelece chaves de sessão. No entanto, ele pode ser usado com vários protocolos de estabelecimento de chaves de sessão, como Oakley, para fornecer uma solução completa para o gerenciamento de chaves de Internet. A especificação ISAKMP também está disponível em postscript.

Sobre Oakley

O protocolo Oakley usa uma técnica Diffie-Hellman híbrida para estabelecer chaves de sessão em hosts e roteadores da Internet. Oakley fornece a importante propriedade de segurança do Perfect Forward Secret (PFS) e é baseado em técnicas criptográficas que sobreviveram a uma ampla análise pública. Oakley pode ser usado sozinho, se não for necessária nenhuma negociação de atributo, ou Oakley pode ser usado em conjunto com ISAKMP. Quando o ISAKMP é usado com Oakley, o depósito de chave não é viável.

Os protocolos ISAKMP e Oakley foram combinados em um protocolo híbrido. A resolução do ISAKMP com Oakley usa a estrutura do ISAKMP para suportar um subconjunto de modos de troca de chaves Oakley. Esse novo protocolo de troca de chaves fornece PFS opcional, negociação de atributos de associação de segurança completa e métodos de autenticação que fornecem tanto reputação quanto não-repúdio. As implementações deste protocolo podem ser usadas para estabelecer VPNs e também permitir que usuários de locais remotos (que podem ter um endereço IP alocado dinamicamente) acessem uma rede segura.

Sobre o IPSec

O Grupo de Trabalho IPSec da IETF desenvolve padrões para mecanismos de segurança da camada IP para IPv4 e IPv6. O grupo também está desenvolvendo protocolos genéricos de gerenciamento para uso na Internet. Para obter mais informações, consulte a Visão geral de segurança e criptografia de IP.

Software ISAKMP

Implementação dos sistemas Cisco

O software daemon ISAKMP da Cisco Systems está disponível gratuitamente para qualquer uso comercial ou não comercial para ajudar a adiantar o ISAKMP como uma solução padrão para o gerenciamento de chaves de Internet.

O software Cisco ISAKMP está disponível nos Estados Unidos e no Canadá através de um formulário de download na Web do Massachusetts Institute of Technology (MIT). Devido às leis de controle de exportação dos Estados Unidos, a Cisco não consegue distribuir esse software para fora dos Estados Unidos e do Canadá.

O daemon ISAKMP da Cisco usa a API (Key Management Application Program Interface, interface do programa de gerenciamento de chaves) PF_KEY para se registrar em um kernel de sistema operacional (que implementou essa API) e na infraestrutura de gerenciamento de chaves que o rodeia. As associações de segurança negociadas pelo daemon ISAKMP são inseridas no

mecanismo chave do kernel. Eles estão disponíveis para uso pelos mecanismos de segurança IPSec padrão do sistema (Cabeçalho de autenticação [AH] e Payload de segurança de encapsulamento [ESP]).

A distribuição gratuita de software IPv6+IPSec para sistemas derivados de 4,4 BSD (incluindo Berkeley Software Design, Inc. [BSDI] e NetBSD) nos EUA inclui a implementação de IPv6, IPSec para IPv6, IPSec para IPv4 e interface PF_KEY. O software NRL está disponível nos Estados Unidos e no Canadá por meio de um formulário de download na Web do MIT. Fora dos Estados Unidos e Canadá, o software NRL está disponível por FTP em ftp://ftp.ripe.net/ipv6/nrl .

O daemon da Cisco é baseado no ISAKMP versão 5 e usa recursos do Oakley Key Identification Protocol versão 1.

Uma lista de endereços para problemas, correções de bugs, alterações de portabilidade e discussão geral sobre ISAKMP e Oakley foi estabelecida em isakmp-oakley@cisco.com. Para aderir a esta lista, envie uma solicitação de correio eletrônico com um corpo de mensagem de **subscribe isakmp-oakley** para: majordomo@cisco.com.

Implementação do Departamento de Defesa dos Estados Unidos (DoD)

O Departamento de Pesquisa de Segurança da Informação dos Estados Unidos disponibilizou sua Implementação de Protótipo ISAKMP gratuitamente para distribuição nos Estados Unidos. Uma interface baseada na Web está disponível para download do software. Essa implementação não inclui nenhum recurso de troca de chave de sessão, mas inclui todos os recursos ISAKMP.

Informações Relacionadas

- Página de suporte do IPSec
- Suporte Técnico - Cisco Systems