ISAKMP VERMELHO e informação de Oakley

Índice

Introdução

Este documento fornece a informação no Internet Security Association and Key Management Protocol (ISAKMP) e no protocolo da determinação da chave de Oakley. Estes protocolos são concorrentes principais para o gerenciamento de chave de Internet que está sendo considerado pelo grupo em funcionamento do IPsec do Internet Engineering Task Force (IETF).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Informações técnicas

Sobre o ISAKMP

O ISAKMP fornece uma estrutura para o gerenciamento de chave de Internet e fornece o suporte de protocolo específico para a negociação dos atributos de segurança. Apenas, não estabelece chaves de sessão. Porém pode ser usado com vários protocolos de estabelecimento da chave de sessão, tais como Oakley, para fornecer uma solução completa ao gerenciamento de chave de Internet. A especificação ISAKMP igualmente está disponível no p.s.

Sobre Oakley

O protocolo Oakley usa uma técnica híbrida de Diffie-Hellman para estabelecer chaves de sessão em host de Internet e em Roteadores. Oakley fornece a propriedade de segurança importante do discrição perfeita adiante (PFS) e é baseado nas técnicas criptográficas que sobreviveram ao exame público substancial. Oakley pode ser usado por si só, se nenhuma negociação do atributo é precisada, ou Oakley pode ser usado conjuntamente com o ISAKMP. Quando o ISAKMP é usado com Oakley, o principal garantia não é praticável.

O ISAKMP e os protocolos Oakley foram combinados em um protocolo híbrido. A definição do ISAKMP com Oakley usa a estrutura do ISAKMP para apoiar um subconjunto de modos das trocas de chave de Oakley. Este protocolo de intercâmbio chave novo fornece pF opcional, negociação de atributo de associação de segurança completa, e métodos de autenticação que fornecem o repúdio e a não-repudiação. As aplicações deste protocolo podem ser usadas para estabelecer VPN e para permitir igualmente usuários dos locais remotos (quem podem ter um endereço IP de Um ou Mais Servidores Cisco ICM NT dinamicamente atribuído) alcance a uma rede segura.

Sobre o IPsec

O grupo em funcionamento do IPsec do IETF desenvolve padrões para mecanismos de segurança da camada de IP para o IPv4 e o IPv6. O grupo igualmente está desenvolvendo protocolos de gestão da chave genérica para o uso no Internet. Para mais informação, refira a Segurança IP e a Visão Geral sobre Criptografia.

Software isakm

Aplicação do Cisco Systems

O software daemon ISAKMP de Cisco Systems está disponível gratuitamente para que todo o uso comercial ou não comercial ajude o ISAKMP avançado como uma solução padrão ao gerenciamento de chave de Internet.

O software isakm de Cisco está disponível dentro do Estados Unidos e do Canadá através de um formulário da transferência da Web de Massachusetts Institute of Technology (MIT). Devido às leis de controle de exportação do Estados Unidos, Cisco é incapaz de distribuir este software fora do Estados Unidos e do Canadá.

O daemon de ISAKMP de Cisco usa o Application Program Interface do gerenciamento chave PF_KEY (API) para registrar-se com um núcleo do sistema operacional (que executou este API) e a infraestrutura de gerenciamento chave circunvizinha. As associações de segurança que foram negociadas pelo daemon de ISAKMP são introduzidas no motor chave do núcleo. Estão então

disponíveis para o uso dos mecanismos de segurança do IPSec padrão do sistema ([AH] do cabeçalho de autenticação e [ESP] do Encapsulating Security Payload).

A distribuição de software livre-distribuível do laboratório de pesquisa naval E.U. (NRL) IPv6+IPSec para os sistemas derivados 4.4-BSD (que incluem [BSDI] de Berkeley Design de software, Inc. e NetBSD) inclui a aplicação do IPv6, o IPsec para o IPv6, o IPsec para o IPv4, e a relação PF_KEY. O software NRL está disponível dentro do Estados Unidos e do Canadá através de um formulário da transferência da Web do MIT. Fora do Estados Unidos e do Canadá, o software NRL está disponível com o FTP de ftp://ftp.ripe.net/ipv6/nrl .

O demônio de Cisco é baseado na versão ISAKMP 5 e usa características da versão do protocolo 1. da determinação da chave de Oakley.

Uma lista de endereços para problemas, correções de bug, mudanças movendo, e discussão geral do ISAKMP e do Oakley foi estabelecida em isakmp-oakley@cisco.com. Para juntar-se a esta lista, envie uma requisição de e-mail com um corpo da mensagem de **subscrevem o ISAKMP-oakley** a: majordomo@cisco.com.

Aplicação do departamento de defesa do Estados Unidos (DoD)

O escritório DoD E.U. da pesquisa de segurança das informação fez sua implementação de protótipo ISAKMP livremente disponível para a distribuição dentro do Estados Unidos. Uma interface baseada NA Web está disponível para transferir o software. Esta aplicação não inclui nenhuma capacidades de intercâmbio da chave de sessão, mas inclui características completas ISAKMP.

Informações Relacionadas

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