Сведения о RED ISAKMP и Oakley

Содержание

Введение

Этот документ предоставляет сведения о Протоколе ISAKMP и Протоколе определения ключа Oakley. Эти протоколы ведут претендентов на пост интернет-управления ключами, рассматриваемого Рабочей группой IPSec инженерной группы по развитию Интернета (IETF).

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Технические сведения

О ISAKMP

ISAKMP служит основой для интернет-управления ключами и предоставляет определенную поддержку протокола для согласования атрибутов безопасности. Один, это не устанавливает ключи сеанса. Однако, это может использоваться с различными протоколами установления ключа сеанса, такими как Oakley, для предоставления полного решения интернет-управления ключами. Спецификация ISAKMP также доступна в постскриптуме.

О Oakley

Протокол Oakley использует гибридный способ Диффи-Хеллмана для установления ключей сеанса на Узлах Интернета и маршрутизаторах. Oakley предоставляет важный параметр безопасности безопасной пересылки (Perfect Forward Secrecy, PFS) и основывается на методах шифрования, которые пережили существенное внимание общественности. Oakley может использоваться отдельно, если никакое согласование атрибута не необходимо, или Oakley может использоваться в сочетании с ISAKMP. Когда ISAKMP используется с Oakley, система депонирования ключей не выполнима.

ISAKMP и протоколы Oakley были объединены в гибридный протокол. Разрешение ISAKMP с Oakley использует платформу ISAKMP для поддержки подмножества режимов обмена ключами Oakley. Этот новый протокол обмена ключами предоставляет дополнительную безопасную пересылку (PFS), полное сопоставление атрибутов ассоциации обеспечения безопасности и методы аутентификации, которые предоставляют и отказ и невозможность отрицать факт отправки. Реализации этого протокола могут использоваться, чтобы установить VPN и также обеспечить пользователей от удаленных узлов (у кого может быть динамично выделенный IP-адрес), доступ к защищенной сети.

О IPSec

Рабочая группа IPSec IETF разрабатывает стандарты для механизмов обеспечения безопасности уровня IP и для IPv4 и для IPv6. Группа также разрабатывает протоколы управления общего ключа для использования в Интернете. Для получения дополнительной информации обратитесь к IP-безопасности и Обзору шифрования.

Программное обеспечение ISAKMP

Реализация Cisco Systems

Демон ISAKMP Cisco Systems доступен бесплатно для любого коммерческого или некоммерческого использования, чтобы помочь совершенствовать ISAKMP как стандартное решение интернет-управлению ключами.

Программное обеспечение ISAKMP Cisco доступно в Соединенных Штатах и Канаде через веб-форму загрузки от Массачусетского технологического института (MIT). Из-за законов экспортного контроля Соединенных Штатов, Cisco неспособна распределить это программное обеспечение за пределами Соединенных Штатов и Канады.

Демон ISAKMP Cisco использует Прикладной программный интерфейс (API) Управления ключами PF_KEY для регистрации в ядре операционной системы (который внедрил этот API), и окружающая инфраструктура управления ключами. Сопоставления безопасности, о

которых выполнил согласование демон ISAKMP, введены в ключевой механизм ядра. Они тогда доступны для использования механизмами обеспечения безопасности стандартного протокола IPSec системы (Заголовок аутентификации [AH] и Безопасное закрытие полезной нагрузки [ESP]).

Свободно распространяемая Научно-исследовательская лаборатория Naval (NRL) США распространение программного обеспечения IPv6+IPSec для полученных систем с 4.4 BSD (включая Berkeley Software Design, Inc. [BSDI] и NetBSD) включает реализацию IPv6, IPSec для IPv6, IPSec для IPv4 и интерфейса PF_KEY. Программное обеспечение NRL доступно в Соединенных Штатах и Канаде через веб-форму загрузки от MIT. За пределами Соединенных Штатов и Канады, программное обеспечение NRL доступно через FTP от ftp://ftp.ripe.net/ipv6/nrl.

Демон Cisco основывается на версии ISAKMP 5 и использует функции от Версии протокола 1 определения ключа Oakley.

Список рассылки для проблем, исправлений ошибки, портируя изменения и общее обсуждение ISAKMP и Oakley был установлен в isakmp-oakley@cisco.com. Для присоединения к этому списку передайте запрос электронной почты с телом сообщения, **подписывают isakmp-oakley** на: majordomo@cisco.com.

Реализация отдела защиты (DoD) Соединенных Штатов

Офис DoD США Исследования Информационной безопасности сделал свою Реализацию прототипа ISAKMP в свободном доступе для распределения в Соединенных Штатах. Интернетный интерфейс доступен для загружения программного обеспечения. Эта реализация не включает возможностей обмена ключа сеанса, но действительно включает полные функции ISAKMP.

Дополнительные сведения

- Страница поддержки IPSec
- Техническая поддержка - Cisco Systems