Содержание

Введение

Протокол IKE является стандартным методом, используемым для расположения безопасной, аутентифицируемой связи. Концентратор Cisco VPN 5000 использует IKE для устанавливания Туннелей IPSec. Эти Туннели IPSec являются магистралью этого продукта.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Концентратор серии VPN 5000

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях в документах см. Cisco Technical Tips Conventions.

Задачи IKE

IKE обрабатывает эти задачи:

- Аутентификация
- Согласование параметров сеанса
- Обмен ключами
- Согласование и конфигурация туннеля IPSec

Аутентификация

Аутентификация является самой важной задачей, которую выполняет IKE, и это является самым сложным. Каждый раз, когда вы выполняете согласование о чем-то, важно знать с тем, о ком вы выполняете согласование. IKE может использовать один из нескольких методов для аутентификации выполняющих согласование сторон друг на друге.

- **Общий ключ** - IKE использует способ хеширования, чтобы гарантировать, что только кто-то, кто обладает тем же ключом, может передать пакеты IKE.
- **Стандарт цифровой подписи (DDS) или Rivest, Shamir, Adelman (RSA) цифровые подписи** - IKE использует криптографию цифровой подписи общего ключа, чтобы проверить, что каждая сторона - то, кем они утверждают, что были.
- **Шифрование RSA** - IKE использует один из двух методов для шифрования достаточного количества согласования, чтобы гарантировать, что только сторона с корректным секретным ключом может продолжить согласование.

Согласование параметров сеанса

Во время согласования в процессе сеанса IKE позволяет сторонам выполнять согласование, как они проведут аутентификацию и как они защитят любые дальнейшие согласования (т.е. Согласование туннеля IPSec). Об этих элементах выполняют согласование:

- **Authentication method-** Это - один из методов, перечисленных в Опознавательном разделе этого документа.
- **Key Exchange Algorithm** - Это - математический метод для того, чтобы надежно обмениваться криптографическими ключами по общедоступному средству (Диффи-Хеллман). Ключи используются в шифровании и алгоритмах подписи пакетов.
- **Алгоритм шифрования** - Стандарт шифрования данных (DES) или Стандарт тройного шифрования данных (3DES).
- **Алгоритм подписи пакетов** - алгоритм представления сообщения в краткой форме 5 (MD5) и Защищенный алгоритм хэширования 1 (SHA-1).

Обмен ключами

IKE использует согласованный метод обмена ключами (см. раздел Согласования в процессе сеанса этого документа) создать достаточно битов материала создания криптографических ключей для обеспечения будущих транзакций. Этот метод гарантирует, что каждый сеанс IKE защищен с новым, безопасным набором ключей.

Аутентификация, согласование в процессе сеанса и обмен ключами составляют фазу 1 Ike согласование. Для Концентратора VPN 5000 эти свойства настроены в **Разделе Политика IKE** через Защитное ключевое слово. Это ключевое слово является меткой, которая имеет три части: алгоритм аутентификации, алгоритм шифрования и Key Exchange Algorithm. Части разделены подчеркиванием. Средства метки MD5_DES_G1 используют MD5 для аутентификации пакета IKE, используют DES для шифрования пакета IKE и используют Группу Диффи-Хеллмана 1 для обмена ключами. Для получения дополнительной информации обратитесь к Настройке Набор правил IKE для Безопасности Туннеля IPSec.

Согласование и конфигурация туннеля IPSec

После того, как IKE закончил выполнять согласование о безопасном способе обмена информацией (фаза 1), IKE используется для согласования о Туннеле IPSec. Это выполнено с помощью фазы IKE два. В этом обмене IKE создает новый ключевой материал для Туннеля IPSec для использования (или использование ключей фазы 1 IKE как ядро или путем выполнения нового обмена ключами). О шифровании и алгоритмах аутентификации для этого туннеля также выполняют согласование.

Туннели IPSec настроены с помощью Группы VPN (раньше Клиент Протокола установления безопасного туннеля (STEP)) раздел для туннелей Клиента VPN и раздел Партнера по туннелю для туннелей между локальными сетями (LAN-to-LAN). Раздел **Пользователей VPN** - то, где сохранен метод аутентификации для каждого пользователя. Эти разделы задокументированы в Настройку Набор правил IKE для Безопасности Туннеля IPSec.

Расширения IKE концентратора VPN 5000

- **RADIUS** - IKE не имеет никакой поддержки Проверки подлинности RADIUS. Проверка подлинности RADIUS выполнена в обмене специальных сведений, который имеет место после первого пакета IKE от Клиента VPN. Если Протокол аутентификации пароля (PAP) требуется, специальная тайна Проверки подлинности RADIUS требуется. Для получения дополнительной информации обратитесь к документации NoCHAP и PAPAuthSecret в Настройке Набор правил IKE для Безопасности Туннеля IPSec. Проверка подлинности RADIUS аутентифицируется и шифруется. Обмен PAP защищен PAPAuthSecret. Однако существует только одна такая тайна для всего IntraPort, таким образом, защита так же слаба как любой совместно используемый пароль.
- **SecurID** - IKE в настоящее время не имеет никакой поддержки Проверки подлинности с помощью secureid. Проверка подлинности с помощью secureid выполнена в специальном информационном обмене промежуточная фаза 1 и фаза два. Этот обмен полностью защищен Сопоставлением безопасности (SA) IKE, о котором выполняют согласование в фазе 1.
- **Протокол управления доступом безопасного туннеля (STAMP)** - Подключения VPN Client обмениваются информацией с IntraPort во время процесса IKE. Информация такой, как будто это в порядке для сохранения тайн, которые IP - сети туннелировать, или туннелировать ли трафик Межсетевого пакетного обмена (IPX), передаются в частных полезных нагрузках во время последних двух пакетов IKE. Эти информационные наполнения только передаются совместимым Клиентам VPN.

ISAKMP и Oakley

Протокол ISAKMP является языком, используемым для проведения согласований через Интернет (например, с помощью Протокола "IP"). Oakley является методом для проведения аутентифицируемого обмена материалом криптографического ключа. IKE соединяет два в один пакет, который позволяет безопасным соединениям быть установленными через небезопасный Интернет.

STEP и STAMP

Протокол установления безопасного туннеля (STEP) является предыдущим названием системы VPN. В дни перед IKE ШТАМП использовался для согласования о IP - безопасных соединениях. Версии Клиента VPN ранее, чем 3.0 ШТАМПА использования для установления соединения с IntraPort.

Дополнительные сведения

- Объявление об окончании продажи концентраторов Cisco серии VPN 5000
- Настройка туннеля между двумя LAN с помощью концентратора, обеспечивающего взаимодействие между маршрутизаторами и VPN 5000
- Страница технической поддержки продукта для концентратора Cisco VPN 5000
- Страница технической поддержки продукта Cisco VPN 5000 Client
- Поддержка технологии Протоколов IPSec Negotiation/IKE
- Cisco Systems – техническая поддержка и документация