Конфигурирование DN-Based Crypto Maps для VPN Device Access Control

Содержание

Введение

В данном документе описывается порядок конфигурации криптокарт на базе отличительных имен (DN) в целях обеспечения управления доступом и возможности установления туннельного соединения VPN между устройством VPN и маршрутизатором Cisco IOS®. В примере этого документа подпись Rivest, Shamir, и Adelman (RSA) является методом аутентификации IKE. В дополнение к стандартной проверке достоверности сертификата Криптокарты на основе DN пытаются совпасть с ISAKMP - идентичностью узла с определенными полями в его сертификатах, таких как составное имя X.500 или полное доменное имя (FQDN).

Предварительные условия

Требования

Эта функция была сначала представлена в программном обеспечении Cisco IOS версии 12.2(4)T. Вы должны этот выпуск или позже для этой конфигурации.

Cisco IOS Software Release 12.3 (5) был также протестирован. Однако DN базировался, криптокарты отказали из-за идентификатора ошибки Cisco CSCed45783 (только зарегистрированные клиенты).

Используемые компоненты

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

- Маршрутизаторы Cisco 7200
- Cisco IOS Software Release 12.2(4)T1 c7200-ik8o3s-mz.122-4.T1

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.

Общие сведения

Ранее, во время аутентификации IKE с помощью метода простановки подписи RSA, и после проверки достоверности сертификации и дополнительной проверки списка отозванных сертификатов (CRL), Cisco IOS продолжила согласование Быстрого режима IKE. Это не предоставило метод, чтобы препятствовать тому, чтобы удаленные устройства VPN связались с любыми интерфейсами с шифрованием кроме ограничений на IP-адрес однорангового узла шифрования.

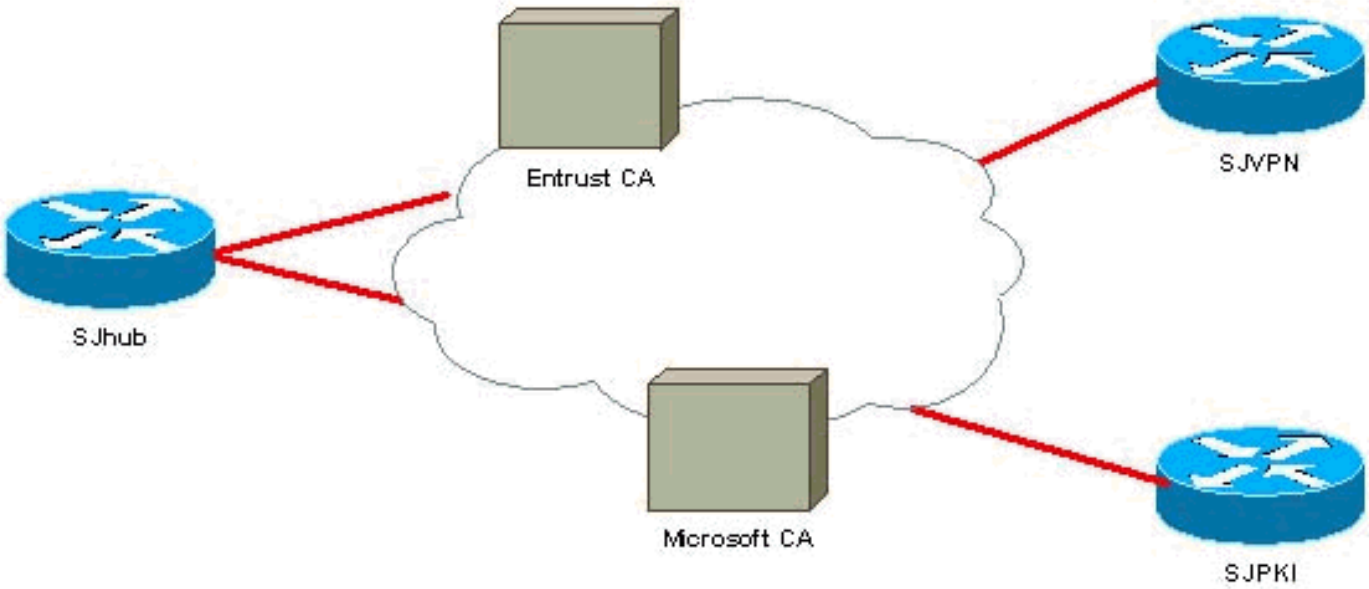
Теперь с Криптокартой на основе DN, Cisco IOS может ограничить удаленные узлы VPN, чтобы только обратиться к выбранным интерфейсам с определенными сертификатами. В частности сертификаты с определенными DN или FQDNs.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Схема сети

В этом документе используются настройки сети, показанные на данной диаграмме.



Конфигурации

В данном документе используется следующая конфигурация.

В данном примере настройка простой сети используется для демонстрации функции. Маршрутизатор SJhub имеет два сертификата: от центра сертификации Entrust и Microsoft. Посмотрите Дополнительные сведения