Содержание

Введение

Все Цифровые сертификаты имеют созданный во времени окончания срока действия в сертификате, который назначен сервером Центра сертификации (CA) запуска во время регистрации. Когда Цифровой сертификат используется для аутентификации VPN IPSec ISAKMP, существует автоматическая проверка времени окончания срока действия сертификата подключающегося устройства и системного времени на устройстве (оконечная точка VPN). Это гарантирует, что используемый сертификат допустим и не истек. Это также, почему *необходимо* установить внутренние часы на каждой оконечной точке VPN (маршрутизатор). Если Протокол NTP (или Простой сетевой протокол синхронизации времени [SNTP]) не возможен на маршрутизаторах криптографии VPN, то используйте ручную **команду set clock**.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на всех маршрутизаторах, которые выполняют cXXXX-advsecurityk9-mz.123-5.9. T отображают для той соответствующей платформы.

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 см. в документе Технические рекомендации Cisco. Условные обозначения.

Когда Цифровой сертификат Считают Истекшим или Не

Истекший?

- Если системное время после времени окончания срока действия сертификата или перед выполненным временем сертификата, сертификат истекается (недопустимый).
- Если системное время в или между выполненным временем сертификата и временем сертификата с истекшим сроком, сертификат не истекается (допустимый).

Цель функции Автоматической регистрации состоит в том, чтобы предоставить администратору CA механизм, чтобы позволить в настоящее время регистрируемому маршрутизатору автоматически повторно регистрироваться с его сервером CA на настроенном проценте срока действия сертификата маршрутизатора. Это - важная функция управляемости / обеспеченность сертификатов как механизм управления. Если вы использовали определенный CA для запуска сертификатов к потенциально тысячам маршрутизаторов с поддержкой VPN ответвления с одной годовой продолжительностью действия (без Автоматической регистрации), то точно за один год выполненного времени, все сертификаты истекают, и все ответвления теряют подключение через IPSec. Также, если функция Автоматической регистрации установлена в "автоматическую регистрацию 70", как в данном примере, то в 70% срока действия выполненного сертификата (1 год), каждый маршрутизатор автоматически выполняет новый запрос регистрации к Cisco сервер IOS® CA, перечисленный в точке доверия.

Примечание: Одно исключение из функции Автоматической регистрации - то, что, если она установлена в *меньше чем или равный 10*, тогда это находится в минутах. Если это *больше, чем 10*, то это - процент от срока действия сертификата.

Существуют некоторые предупреждения Cisco IOS CA, администратор должен знать с Автоматической регистрацией. Администратор должен выполнить эти действия для повторного зачисления, чтобы быть успешным:

1. Вручную предоставьте или отклоните каждый запрос повторного зачисления на Cisco IOS CA сервер (пока "grant auto" не используется на Cisco IOS CA сервер).Cisco IOS CA сервер все еще должен или предоставить или отклонить каждый из этих запросов (учитывая, что Cisco IOS CA не включили "grant auto"). Однако никакое административное действие на маршрутизаторе регистрации не требуется, чтобы запускать процесс повторного зачисления.
2. Сохраните новый повторно зарегистрированный сертификат в маршрутизаторе с поддержкой VPN перерегистрации, в подходящих случаях.Если нет никаких несохраненных изменений конфигурации, ожидающих в маршрутизаторе, то новый сертификат автоматически сохранен к Энергонезависимой памяти (NVRAM). Новый сертификат записан в NVRAM, и предыдущий сертификат удален.Если существует несохраненное ожидание изменений конфигурации, то необходимо выполнить **команду copy run start** на маршрутизаторе регистрации для сохранения изменений конфигурации и нового повторно зарегистрированного сертификата в NVRAM. Как только **команда copy run start** завершена, тогда новый сертификат записан в NVRAM, и предыдущий сертификат удален.**Примечание:** Когда новое повторное зачисление успешно, который *не* отзывает предыдущий сертификат для того зарегистрированного устройства на сервере CA. Когда устройства VPN связываются, они передают друг другу Серийный номер сертификата (уникальный номер).**Примечание:** Например, если вы в 70% срока действия сертификата, и ответвление VPN должно было повторно зарегистрироваться с CA, тот CA имеет два сертификата для того имени хоста. Однако

маршрутизатор регистрации только имеет один (более новый). Если вы принимаете решение, можно административно отозвать старый сертификат или позволить ему обычно истекать.**Примечание:** Более новые версии кода функции Автоматической регистрации имеют опцию для "восстанавливания" пар согласованных ключей, используемых для регистрации.Эта опция является "не по умолчанию" для регенерации пар согласованных ключей.Если эта опция была выбрана, знают об идентификаторе ошибки Cisco CSCea90136. Это исправление ошибки обеспечивает новую пару согласованных ключей, которая будет помещена во временные файлы, в то время как новое хранилище сертификатов имеет место по существующему Туннелю IPSec (который использует старую пару согласованных ключей).Автоматическая регистрация имеет опцию для генерации новых ключей во время обновления сертификации. В настоящее время это вызывает прерывание обслуживания в течение времени, которое требуется для получения нового сертификата. Это вызвано тем, что существует новый ключ, но никакой сертификат, который совпадает с ним.Этот короткометражный ролик сохраняет старый ключ и сертификат, пока новый сертификат не доступен.Автоматическая генерация ключа также внедрена для ручной регистрации. Ключи генерируются (по мере необходимости) для автоматического или ручной регистрации.Найденная версия - 12.3PIH03Версия, которая будет исправлена в - 12.3TВерсия применилась к - 12.3PI03Интегрированный в - ни одинДля дополнительных сведений обратиться в техническую поддержку Cisco.

Дополнительные сведения

- Страница поддержки IPSec
- Техническая поддержка - Cisco Systems