PIX/ASA 7.X : CAC - проверка подлинности смарт-карт для Cisco VPN Client

Содержание

Введение

Этот документ предоставляет пример конфигурации на устройстве адаптивной защиты Cisco (ASA) для сетевого удаленного доступа с картой общего доступа (CAC) для аутентификации.

Область этого документа покрывает конфигурацию Cisco ASA с Менеджером устройств адаптивной безопасности (ASDM) (ASDM), Cisco VPN Client и Microsoft Active Directory (AD) / Протокол LDAP.

Конфигурация в этом руководстве использует Microsoft AD/LDAP server. Этот документ также покрывает дополнительные характеристики, такие как OCSP и Карты атрибутов LDAP.

Предварительные условия

Требования

Базовые знания о Cisco ASA, Cisco VPN Client, Microsoft AD/LDAP и Инфраструктуре открытых ключей (PKI) выгодны для понимания завершенной настройки. Знакомство с AD составом группы и свойствами пользователя, а также объектами LDAP помогает коррелировать процесс авторизации между атрибутами сертификата и объектами AD/LDAP.

Используемые компоненты

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

- Устройство адаптивной защиты (ASA) серии 5500 Cisco, которое выполняет Версию программного обеспечения 7.2 (2)
- Cisco Adaptive Security Device Manager (ASDM) версия 5.2 (1)
- Cisco VPN Client 4. x

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

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Конфигурация Cisco ASA

Этот раздел покрывает конфигурацию Cisco ASA через ASDM. Это покрывает обязательные действия для развертывания туннеля удаленного доступа VPN посредством IP - безопасного соединения. Сертификат CAC используется для аутентификации, и атрибут главного имени пользователя (UPN) в сертификате заполнен в Active Directory для авторизации.

Вопросы развертывания

- Это руководство НЕ покрывает базовые конфигурации, такие как интерфейсы, DNS, NTP, маршрутизация, доступ к устройству или доступ ASDM, и т.д. Предполагается, что оператор сети знаком с этими конфигурациями.Для получения дополнительной информации обратитесь к Многофункциональным Устройствам безопасности.
- Некоторые разделы являются обязательными конфигурациями, необходимыми для основного доступа VPN. Например, VPN-туннель может быть настройкой с картой CAC без проверок OCSP, проверок сопоставлений LDAP. DoD передает под мандат проверку OCSP, но туннель работает без настроенного OCSP.
- Основной требуемый образ ASA/PIX 7.2 (2) и ASDM 5.2 (1), но это руководство использует промежуточную конструкцию 7.2.2.10 и ASDM 5.2.2.54.
- Никакое изменение схемы LDAP не необходимо.
- Посмотрите Приложение A для LDAP и примеры сопоставления политики динамического доступа для дополнительной принудительной политики.
- См. Приложение D о том, как проверить объекты LDAP в MS.
- Посмотрите дополнительные сведения