Настройте поддержку HTTPS интеграции SCEP ISE

Содержание

Введение

Этот документ описывает шаги, требуемые настраивать Протокол передачи гипертекстовых файлов, Безопасный (HTTPS) поддержка интеграции Безопасного протокола регистрации сертификата (SCEP) с платформой Identity Services Engine (ISE).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Базовые знания о Web-сервере информационных сервисов интернета (IIS) Microsoft
- Опыт в конфигурации SCEP и сертификатов на ISE

Используемые компоненты

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

- Выпуск 1.1 ISE. x

- Предприятие R2 Windows Server 2008 года с заплатами для KB2483564 и KB2633200 установлено

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.

Информация, отнесенная к сервисам сертификации Microsoft, предоставлена как руководство в частности для BYOD Cisco. Именуйте TechNet Microsoft как категорический источник истины для центра сертификации Microsoft, службы Network Device Enrollment Service (NDES), и SCEP отнесся конфигурации сервера.

Общие сведения

В развертываниях BYOD одним из основных компонентов является Microsoft 2008 R2 Enterprise server, которой установили роль NDES. Этот сервер является участником леса Active Directory (AD). Во время начальной установки NDES Web-сервер IIS Microsoft автоматически установлен и настроен для поддержки завершения HTTP SCEP. В некоторых развертываниях BYOD клиенты могли бы хотеть далее защитить связь между ISE и NDES использование HTTPS. Эта процедура детализирует шаги, требуемые запрашивать и устанавливать сертификат Протокола SSL для веб-сайта SCEP.

Настройка

Конфигурация серверного сертификата NDES

> **Примечание:** Необходимо настроить новый сертификат для IIS (только потребовал, когда IIS интегрирован с PKI третьей стороны, таким как Verisign или когда Центр сертификации (CA) и роли сервера NDES разделены на отдельные серверы). В установке, если роль NDES находится на текущем Microsoft CA server, IIS использует сертификат идентификации сервера, созданный во время настройки CA. Для автономных конфигураций, таких как это, пропустите непосредственно к **Серверу NDES IIS, Связывающий Раздел конфигурации** в этом документе.

1. Соединитесь с сервером NDES через консоль или RDP.
2. Нажмите **Start-> Administrative Tools-> Internet Information Services (IIS) Manager**.
3. Выделите название сервера IIS и нажмите значок **Серверных сертификатов**.
4. Щелкните **по Create Certificate Request** и завершите поля.
5. Откройте .cer файл, созданный в предыдущем шаге с текстовым редактором, и скопируйте содержание к буферу обмена.
6. Обратитесь к веб-сайту Microsoft CA Web Enrollment и нажмите **Request a Certificate**.URL в качестве примера: http://yourCAIP/certsrv
7. Нажмите **Submit запрос сертификата при помощи....** Вставка в содержании сертификата от буфера обмена, и выбирает **Шаблон веб-сервера**.

8. Нажмите **Submit** и затем сохраните файл сертификата к рабочему столу.
9. Возвратитесь к серверу NDES и откройте утилиту IIS Manager. Щелкните по имени сервера и затем нажмите **Complete Certificate Request** для импорта недавно созданного серверного сертификата.

Сервер NDES IIS, связывающий конфигурацию

1. Разверните **имя сервера**, разверните **Узлы**, нажмите **Default Web Site**.
2. Нажмите **Bindings** в верхнем правом угле.
3. **Нажмите Add**, измените HTTPS **Typeto** и выберите сертификат из выпадающего списка.
4. **Нажмите кнопку OK.**

Конфигурация сервера ISE

1. Соединитесь с веб-интерфейсом Регистрации сервера CA и загрузите цепочку сертификата CA.
2. От GUI ISE перейдите к **администрированию-> Сертификаты-> Хранилище Сертификата** и импортируйте цепочку сертификата CA в хранилище ISE.
3. Перейдите к **администрированию-> Сертификаты-> SCEP CA Профили** и настройте URL для HTTPS. Нажмите **Test Connectivity** и затем нажмите **Save**.

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

- Перейдите к **администрированию-> Сертификаты-> Сертификат, Storeand** проверяют, что присутствуют цепочка сертификата CA и полномочия регистрации сервера NDES (RA) сертификат.
- Используйте Wireshark или Дамп TCP для мониторинга начального обмена SSL между узлом admin ISE и сервером NDES.

Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show**. **Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

- Сломайте топологию сети BYOD в логический waypoints, чтобы помочь определять отладку и точки перехвата вдоль пути между этими оконечными точками - ISE, NDES и CA.
- Гарантируйте, что TCP 443 разрешен двунаправленным образом между ISE и сервером NDES.

- Контролируйте CA и журналы серверного приложения NDES для ошибок регистрации и используйте Google или TechNet для исследования тех ошибок.
- Используйте утилиту TCP Dump на PSN ISE и трафике монитора к и от сервера NDES. Это расположено при **Операциях> Инструменты диагностики> Общие средства**.
- Установите Wireshark на сервере NDES или используйте SPAN на посреднических коммутаторах для получения трафика SCEP к и от PSN ISE.

Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show**. **Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**

> **Примечание:** Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

Дополнительные сведения

- Настройте поддержку SCEP BYOD
- Cisco Systems – техническая поддержка и документация