Импорт сертификатов SSL в профилировщик NAC

Содержание

Введение

Система Профилировщика находящийся на web UI может использовать цифровые сертификаты так, чтобы подлинность встроенного Web-сервера на Сервере Cisco NAC Profiler могла быть проверена браузером, поскольку это соединяется для доступа к интерфейсу пользователя Профилировщика, подаваемому HTTPS. Система усиливает одно из наиболее распространенных приложений PKI и цифровых сертификатов, где web-браузер проверяет, что Web-сервер SSL подлинен так, чтобы пользователь чувствовал себя безопасным, что их взаимодействию с Web-сервером, фактически, доверяют и их связь с ним безопасный. Это - тот же механизм, который используется сегодня для обеспечения электронной коммерции и другой безопасной связи с веб-сайтами многих типов тот SSL использования.

Система Профилировщика отправляет с "самоподписанным" цифровым сертификатом, который предоставляет доступ к UI, но без проверки встроенного Web-сервера SSL, как доверяется. Пока сертификат по умолчанию не заменен одним созданным со специфичными для среды атрибутами, такими как имя сервера, и подписан Центром сертификации (CA), web-браузеры, которые обращаются к UI Профилировщика, отображают предупреждение, подобное данному примеру, которые указывают, что браузер не распознает CA, который выполнил сертификат и неспособен, проверяют его как надежный узел.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Сервер NAC

Условные обозначения

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

Основная задача: Установите сертификат

Большинство браузеров требует, чтобы пользователь предоставил дополнительный ввод для продолжения соединения, которое может быть надоедливым.

Чтобы полностью использовать повышенный уровень безопасности, предоставленный при помощи цифровых сертификатов для безопасности SSL интерфейса Профилировщика, изменения к конфигурации подсистемы SSL NPS должны быть внесены. Те изменения требуют замены секретного ключа и цифрового сертификата, которые используются системой по умолчанию с выполненными доверенным центром сертификации и которые являются определенными для установки. После этой процедуры браузер инициирует сеанс HTTPS с Сервером и сразу берет пользователя к процессу регистрации в системе UI для обхода предупреждений сертификата.

Две опции

Существует две альтернативы для этого в системах NPS:

1. Используйте резидентный объект инструментария OpenSSL на устройстве для генерации подписанного сертификата, который может быть установлен на Серверной системе NPS, и PC использовали управлять системой через веб-UI.

Эта опция может использоваться в средах, которые в настоящее время не имеют внутреннего CA и выбирают not to rely on the commercial CA providers, которые взимают сбор для обеспечения цифрового сертификата со знаком, который распознан большинством коммерческих браузеров автоматически.

2. Используйте инструментарий OpenSSL для генерации Запроса подписи сертификата для системы NPS, которая отправлена или внутреннему или внешнему коммерческому сервису CA, который возвращает готовый к использованию, цифровой сертификат со знаком для использования в системе.

Это, как правило, - вопрос внутренней политики безопасности организации, в которой система Профилировщика установлена для создания определения который опция использовать в определенной среде. Подробные инструкции для обеих опций предоставлены в оставшейся части этого документа.

Вариант 1: Используйте Инструментарий OpenSSL на Маяке/NPS для Генерации Знака

До начала процедуры выделил, важно проверить, что система Профилировщика должным образом настроена для использования сервиса названия предприятия, и что Запись DNS сделана такой, что система имеет полное доменное имя (FQDN). Чтобы проверить, что дело обстоит так, гарантируйте, что вы в состоянии открыть сеанс UI с системой Профилировщика с FQDN системы (т.е. https://beacon.bspruce.com/beacon) вместо IP-адреса (или VIP в случае систем HA) в URL, когда вы переходите к UI.

Эта процедура используется в случаях, когда она не желаема для отправки CSR CA вне устройства для подписания. Эта процедура обеспечивает создание подписанного сертификата с инструментарием OpenSSL на устройстве исключительно - ничто не должно быть отправлено другой системе или коммерческому CA для генерации подписанного сертификата для системы Профилировщика.

Успех этой процедуры зависит от следующего он, как задано. Синтаксис команды длинен и подвержен ошибкам. Гарантируйте, что вы находитесь в верном каталоге, как задано в инструкциях перед выполнением команд. Информация для DN, генерируемых для Сертификата CA и Запроса подписи сертификата, таких как страна, состояние, город, имя сервера, и т.д., должна быть введена тождественно (чувствительная к регистру), так, несомненно, должна будет сделать примечания, поскольку вы выполняете шаги, чтобы гарантировать, что процесс идет беспрепятственно.

1. Инициируйте SSH или сеанс консоли к устройству NPS и поднимите до доступа к корневому каталогу. Для систем HA гарантируйте, что вы находитесь в Основной системе путем инициирования SSH к VIP.До использования OpenSSL впервые, должна инициализироваться некоторая файловая структура, используемая OpenSSL. Выполните эти шаги для инициализации OpenSSL:
2. Измените каталог на/etc/pki/CA с этой командой: `cd /etc/pki/CA/`Создайте новый каталог, названный **newcerts**, и выполните эти команды:`mkdir newcerts touch index.txt`
3. Используйте vi для создания нового файла, названного **последовательным**; вставьте **01** в файл и передайте изменения. (: wq!)Измените этот каталог:CD/etc/pki/tls/certs
4. Генерируйте новый секретный ключ для системы с этой командой:`openssl genrsa -out profilerFQDN.key 1024`(где 'profilerFQDN' заменен Полным доменным именем устройства NPS, когда развернуто автономного. Для систем HA FQDN VIP должен использоваться).Если система Профилировщика не находится в DNS, IP-адрес сервера (VIP) может использоваться вместо FQDN, но сертификат связан к этому IP-адресу, который требует, чтобы использование IP в URL (т.е. https://10.10.0.1/профилировщик) избежало предупреждений сертификата.
5. Генерируйте сертификат CA для использования для генерации Серверного сертификата с этой командой, которая создает 3-летний сертификат CA и ключ, генерируемый в шаге #4:`openssl req -new -x509 -days 1095 -key profilerFQDN.key -out cacert.pem`Вам предлагают для нескольких атрибутов, которые включены в запрос сертификата и формирование Составного имени (DN) для сертификата CA. Для части этого эти элементы значение по умолчанию предложено (в []). Введите желаемое значение для каждого параметра DN или'.' чтобы пропустить элемент, несомненно, обратить внимание на параметры DN, используемые в этом шаге. Они должны быть идентичны заданным в генерации Запроса подписи сертификата для Серверного сертификата в шаге #7.Переместите сертификат CA, созданный в последний шаг в

требуемый каталог:`mv cacert.pem /etc/pki/CA`Генерируйте Запрос подписи сертификата для системы Профилировщика с новым секретным ключом:`openssl req -new -key profilerFQDN.key -out profilerFQDN.csr`

6. Так же, как в шаге #5, вам предлагают завершить DN для системы для CSR Сервера. Гарантируйте использование тех же значений для CSR Сервера, которые использовались для Сертификата CA в шаге #5. Если существуют какие-либо изменения в параметрах, CSR не создан успешно. Кроме того, вам предлагают создать пароль для сертификата. Обязательно обратите внимание на пароль.
7. Генерируйте Серверный сертификат с CSR и секретным ключом, генерируемым в предыдущих шагах. Выходные данные этого шага являются подписанным сертификатом, который установлен на Сервере Профилировщика (или серверах, в случае пар HA).`openssl ca -in profilerFQDN.csr -out profilerFQDN.crt -keyfile profilerFQDN.key`Вам предлагают подписать и передать сертификат. Введите **y** для подтверждения подписания и фиксации сертификата для завершения генерации серверного сертификата.
8. Переместите файл сертификата в местоположение, заданное внутренней политикой безопасности (если применимо), или используйте расположения по умолчанию:Если никакое местоположение не задано внутренней политикой безопасности, сертификаты должны быть размещены в/etc/pki/tls/certs/.`mv profilerFQDN.crt /etc/pki/tls/certs/profilerFQDN.crt`
9. Переместите файл закрытого ключа в местоположение, заданное внутренней политикой безопасности (если применимо), или используйте расположения по умолчанию:Если никакое местоположение не задано внутренней политикой безопасности, секретный ключ должен быть размещен в/etc/pki/tls/private/. Используйте команду:`mv profilerFQDN.key /etc/pki/tls/private/profilerFQDN.key`
10. Отредактируйте **ssl.conf** файл с редактором, таким как vi для создания необходимых изменений, чтобы вынудить Web-сервер Профилировщика использовать новый секретный ключ, и сертификат (ssl.conf найден в/etc/httpd/conf.d/).В **ssl.conf** часть Серверного сертификата начинается на линии 107. Измените элемент конфигурации SSLCertificateFile от заводской настройки (/etc/pki/tls/certs/localhost.cert) для обращения к новому файлу сертификата, который был создан в системе в шаге #8.В **ssl.conf** часть Секретного ключа Сервера начинается на линии 114. Измените элемент конфигурации Секретного ключа Сервера от заводской настройки (etc/pki/tls/private/localhost.key) для обращения к новому файлу закрытого ключа, размещенному в систему в шаге #9.
11. Перезапустите веб - сервер Apache на устройстве с этой командой: `apachectl -k restart` **Примечание:** Если система развернута автономная, пропустите к шагу #13.
12. Для систем NPS HA только, выполните эти шаги для установки секретного ключа и CRT на другом участнике (текущее Вторичное устройство) пары HA. Это гарантирует, что, независимо от которого устройство является Основным в паре, механизмы обеспечения безопасности SSL для UI работают тождественно.o. Скопируйте секретный ключ, генерируемый на Основном устройстве в шаге #3 во Вторичное устройство. Если никакое местоположение не задано внутренней политикой безопасности, секретный ключ должен быть размещен в/etc/pki/tls/private/. Используйте эту команду (из/etc/pki/tls/private каталога на Основном):`scp profilerFQDN.key root@[secondary IP]:/etc/pki/tls/private/`Скопируйте CRT со знаком, который был возвращен из CA от Основного до Вторичного устройства. Если никакое местоположение не задано внутренней политикой безопасности, сертификаты

должны быть размещены в/etc/pki/tls/certs/.`scp profilerFQDN.crt root@[secondary IP]:/etc/pki/tls/certs` SSH к Вторичному устройству и редактирует свой **ssl.conf** файл с редактором, таким как vi для создания необходимых изменений, чтобы вынудить Web-сервер на Вторичном устройстве использовать новый секретный ключ, и сертификат (ssl.conf найден в/etc/httpd/conf.d/),В **ssl.conf** часть Серверного сертификата начинается на линии 107. Измените элемент конфигурации SSLCertificateFile от заводской настройки (/etc/pki/tls/certs/localhost.cert) для обращения к новому файлу сертификата, размещенному в систему в шаге #11b.В **ssl.conf** часть Секретного ключа Сервера начинается на линии 114. Измените элемент конфигурации Секретного ключа Сервера от заводской настройки (etc/pki/tls/private/localhost.key) для обращения к новому файлу закрытого ключа, размещенному в систему в шаге #11a.Перезапустите веб - сервер Apache на Вторичном устройстве с этой командой:`apachectl -k restart`Поскольку Серверный сертификат, который был создан с этими шагами, использовал частный CA, браузеры, которые обращаются к UI Профилировщика, должны быть настроены для установки сертификата в репозитории полномочий Сертификата доверенного корня на Компьютерах с операционной системой Windows с IE 7.0. Выполните следующие действия:Скопируйте созданный Серверный сертификат к/home/beacon каталогу устройства:`cp profilerFQDN.crt /home/beacon`Используйте WinSCP или сопоставимое программное обеспечение к SCP .crt файл от устройства до ПК.Дважды нажмите **.crt файл**, чтобы запустить менеджера сертификатов Windows и нажать **Install Certificate**, который запускает Мастера Импорта Сертификата.Выберите **Кнопку с зависимой фиксацией**. Разместите все сертификаты в это хранилище для активации **Кнопки обзора**.Выберите **Browse** и нажмите хранилище сертификата **Доверенных корневых центров сертификации**.Нажмите **OK** для принятия этого сертификата.Повторите этот процесс на других PC, которые используются для управления системой Профилировщика.
13. Обратитесь к UI Профилировщика и обратите внимание что session start HTTPS без предупреждений сертификата, генерируемых браузером.

Вариант 2: Генерируйте/Отправляйте CSR к Внутреннему/Внешнему CA

Перед началом процедуры, выделенной затем важно проверить, что система Профилировщика должным образом настроена для использования сервиса названия предприятия, и что Запись DNS сделана такой, что система имеет полное доменное имя (FQDN). Чтобы проверить, что дело обстоит так, гарантируйте, что вы в состоянии открыть сеанс UI с системой Профилировщика с FQDN системы (т.е. https://beacon.bspruce.com/beacon) вместо IP-адреса или VIP в случае систем HA.

Выполните эти шаги, чтобы генерировать новый секретный ключ для системы, генерировать CSR для представления к внутреннему или внешнему CA, и затем разместить допустимый подписанный сертификат в NPS:

1. Инициируйте SSH или сеанс консоли к устройству NPS, и поднимите его до доступа к корневому каталогу. Для систем HA инициируйте SSH к VIP, чтобы гарантировать, что вы находитесь в Основной системе.
2. Перейдите к каталогу PKI по умолчанию для NPS:`cd /etc/pki/tls`
3. Используйте эту команду для генерации нового файла закрытого ключа для системы:`openssl genrsa ?des3 ?out profilerFQDN.key 1024`Где 'profilerFQDN' заменен

полным доменным именем устройства NPS, когда развернуто автономного. Для систем HA FQDN VIP должен использоваться). Вам предлагают ввести и подтвердить пароль для завершения генерации секретного ключа. Этот пароль требуется для будущих операций с помощью секретного ключа. Обязательно сделайте примечание пароля используемым для генерации с закрытым ключом.

4. С секретным ключом, генерируемым в последнем шаге, генерируйте Запрос подписи сертификата (CSR), который передается Центру сертификации (CA) для генерации Сертификата (CRT) для этой системы.Используйте эту команду для генерации CSR`openssl req ?new ?key profilerFQDN.key ?out profilerFQDN.csr`(Замените полным доменным именем системы для 'profilerFQDN'.)Вам предлагают для пароля для секретного ключа при создании CSR для системы; введите его для перехода.Вам тогда предлагают для нескольких атрибутов, которые включены в запрос сертификата и формирование Составного имени (DN). Для части этого эти элементы значение по умолчанию предложено (в []). Введите желаемое значение для каждого параметра DN или'.' пропускать элемент.
5. Проверьте содержание CSR с этой командой:`openssl req -noout -text -in profilerFQDN.csr`(Замените полным доменным именем системы для 'profilerFQDN'.) Это возвращает информацию о CSR и DN, которые были введены в последний шаг. Если информация в CSR должна быть изменена, повторите шаг #4 полностью
6. Отправьте CSR выбранному Центру сертификации (CA) в соответствии с внутренней политикой. Если запрос успешен, CA передает обратно сертификат идентификации, который был снабжен цифровой подписью с секретным ключом CA. Когда этот новый CRT, подписанный вашим выбранным CA, используется для замены CRT заводской настройки в системе Профилировщика, любой браузер, который обращается к UI Профилировщика, в состоянии проверить идентичность узла, и предупреждающие сообщения в браузере, замеченном на соединение с Web-сервером на сервере NPS, больше не отображаются до проверки подлинности пользователя столько, сколько CRT остается допустимым. (Это предполагает, что браузер имел CA, добавил к его полномочиям Сертификата доверенного корня.)
7. Зависящий от CA, который используется, дополнительные сведения возможно должны быть отправлены наряду с CSR, таким как другие учетные данные или доказательства идентичности, требуемой центром сертификации, и центр сертификации может связаться с претендентом на дополнительную информацию.Как только снабженный цифровой подписью CRT возвращается из CA, продолжите следующий шаг заменять секретный ключ фабрики и сертификат с созданными в шагах выше. Для систем HA та же процедура используется для установки секретного ключа и сертификата на Вторичном устройстве в паре, также.
8. Переместите сертификат и файл закрытого ключа к местоположению, заданному внутренней политикой безопасности, если применимо, или используйте расположения по умолчанию:Если никакое местоположение не задано внутренней политикой безопасности, секретный ключ должен быть размещен в/etc/pki/tls/private/. Используйте следующую команду:`mv profilerFQDN.key /etc/pki/tls/private/profilerFQDN.key`Если никакое местоположение не задано внутренней политикой безопасности, сертификаты должны быть размещены в/etc/pki/tls/certs/.`mv profilerFQDN.crt /etc/pki/tls/certs/profilerFQDN.crt`
9. Отредактируйте **ssl.conf** файл с редактором, таким как **vi** для создания необходимых изменений, чтобы вынудить Web-сервер использовать новый секретный ключ, и сертификат (ssl.conf найден в/etc/httpd/conf.d/).В **ssl.conf** часть Серверного сертификата

начинается на линии 107. Измените элемент конфигурации SSLCertificateFile от заводской настройки (/etc/pki/tls/certs/localhost.cert) для обращения к новому файлу сертификата, размещенному в систему в шаге #8.b.В **ssl.conf** часть Секретного ключа Сервера начинается на линии 114. Измените элемент конфигурации Секретного ключа Сервера от заводской настройки (etc/pki/tls/private/localhost.key) для обращения к новому файлу закрытого ключа, размещенному в систему в шаге #8. о.

10. Перезапустите веб - сервер Apache на устройстве с этой командой:`apachectl -k restart` **Примечание:** Если система развернута автономная, пропустите к шагу #12.
11. Для систем NPS HA только, выполните эти шаги для установки секретного ключа и CRT на другом участнике (текущее Вторичное устройство) пары HA. Это гарантирует, что, независимо от которого устройство является Основным в паре, механизмы обеспечения безопасности SSL для UI работают тождественно.Скопируйте секретный ключ, генерируемый на Основном устройстве в шаге #3 во Вторичное устройство. Если никакое местоположение не задано внутренней политикой безопасности, секретный ключ должен быть размещен в/etc/pki/tls/private/. Используйте эту команду (из/etc/pki/tls/private каталога на Основном):`scp profilerFQDN.key root@[secondary IP]:/etc/pki/tls/private/`. Скопируйте CRT со знаком, возвращенный из CA от Основного до Вторичного устройства. Если никакое местоположение не задано внутренней политикой безопасности, сертификаты должны быть размещены в/etc/pki/tls/certs/.`scp profilerFQDN.crt root@[secondary IP]:/etc/pki/tls/certs` SSH к Вторичному устройству и редактирует свой ssl.conf файл с редактором, таким как vi для создания необходимых изменений, чтобы вынудить Web-сервер на Вторичном устройстве использовать новый секретный ключ, и сертификат (ssl.conf найден в/etc/httpd/conf.d/).В **ssl.conf** часть Серверного сертификата начинается на линии 107. Измените элемент конфигурации SSLCertificateFile от заводской настройки (/etc/pki/tls/certs/localhost.cert) для обращения к новому файлу сертификата, размещенному в систему в шаге #11.b.В **ssl.conf** часть Секретного ключа Сервера начинается на линии 114. Измените элемент конфигурации Секретного ключа Сервера от заводской настройки (etc/pki/tls/private/localhost.key) для обращения к новому файлу закрытого ключа, размещенному в систему в шаге #11. о.Перезапустите веб - сервер Apache на Вторичном устройстве с этой командой:`apachectl -k restart`
12. Обратитесь к UI Профилировщика и обратите внимание что session start HTTPS без предупреждений сертификата, генерируемых браузером. Если предупреждение сохраняется, проверьте, что используемый браузер имеет запуск, CA добавленный к его полномочиям Сертификата доверенного корня.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Страница продукта устройства Cisco NAC (Clean Access)
- Cisco Systems – техническая поддержка и документация