Представление высокого уровня сертификатов и полномочий в CUCM

Содержание

Введение

Цель этого документа состоит в том, чтобы понять основы сертификатов и центров сертификации. Этот документ хвалит другие Документы Cisco, которые обращаются к любому шифрованию или характеристикам проверки подлинности в Cisco Unified Communications Manager (CUCM).

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

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 Условные обозначения технических терминов Cisco.

Цель сертификатов

Сертификаты используются между оконечная точками, чтобы построить доверительные отношения и шифрование данных. Это подтверждает, что оконечные точки связываются с намеченным устройством и имеют опцию для шифрования данных между этими двумя оконечными точками.

Определите доверие с точки зрения сертификата

Большая часть важной части сертификатов является определением, которого оконечная точкам может доверять ваша оконечная точка. Этот документ помогает вам знать и определять, как ваши данные зашифрованы и разделены с намеченным веб-сайтом, телефоном, сервером FTP, и так далее.

Когда ваша система доверяет сертификату, это означает, что существует предварительно установленный сертификат (сертификаты) в вашей системе, которая сообщает, что на 100 процентов уверено, что это делится информацией с корректной оконечная точкой. В противном случае это завершает связь между этими оконечная точками.

Нетехническим примером этого являются ваши водительские права. Вы используете эту лицензию (сервер/трудовая книжка), чтобы доказать, что вы - то, кто вы говорите, что вы; вы получили свою лицензию из вашего локального Подразделения ответвления Автомашин (промежуточный сертификат), кому дало разрешения Подразделение Автомашин (DMV) вашего Состояния (Центр сертификации). Когда необходимо показать лицензию (сервер/трудовая книжка) чиновнику, чиновник знает, что они могут доверять ответвлению DMV (промежуточный сертификат) и Подразделение Автомашин (центр сертификации), и они могут проверить, что эта лицензия была выполнена ими (Центр сертификации). Ваша идентичность проверена чиновнику, и теперь они полагают, что вы - то, кто вы говорите, что вы. В противном случае, если вы дадите ложную лицензию (сервер/трудовая книжка), который не был подписан DMV (промежуточный сертификат), то тогда они не будут доверять, кто вы говорите, что вы. Оставшаяся часть этого документа предоставляет всестороннее, техническое пояснение иерархии сертификата.

Как сертификаты использования браузеров

1. Когда вы посетите веб-сайт, введите URL, такой как http://www. cisco . com.
2. DNS находит IP-адрес сервера, который размещает тот узел.

3. Браузер перешел к тому узлу.

Без сертификатов невозможно знать, использовался ли посторонний сервер DNS, или если вы маршрутизировались к другому серверу. Сертификаты гарантируют, что вы должным образом и надежно маршрутизируетесь к намеченному веб-сайту, такому как ваш веб-сайт банка, где персональное или уязвимые данные, которые вы вводите, безопасны.

Все браузеры имеют другие значки, которые они используют, но обычно, вы видите замок в строке адреса как это:

1. Щелкните по замку, и окно отображается:**Рисунок 1: Идентификация веб-сайта**
2. Нажмите **выставленные для обозрения Сертификаты** для наблюдения сертификата узла как показано в данном примере:**Рис. 2: Информация о сертификате, вкладка Общие** Выделенная информация важна.**Выполненный** Компания или Центр сертификации (CA), которому уже доверяет ваша система.**Допустимый от/к** диапазон дат, что этот сертификат применим. (Иногда вы видите сертификат, где вы знаете о доверии CA но вы видите, что сертификат недопустим. Всегда проверяйте дату, таким образом, вы знаете, истекла ли она.)**Совет:** Оптимальный метод должен создать напоминание в вашем календаре для возобновления сертификата, прежде чем это истечет. Это предотвращает будущие проблемы.

Различия между PEM по сравнению с сертификатами DER

PEM является ASCII; DER является двоичными файлами. Рисунок 3 показывает Формат сертификата PEM.

Рис. 3: Пример сертификата PEM

Рисунок 4 показывает Сертификат DER.

Рис. 4: Пример сертификата DER

Большинство CA компании как VeriSign или Thawt используют формат PEM, чтобы передать сертификаты клиентам, потому что это является почтово-дружественным. Клиент должен скопировать всю строку и включать**-----СЕРТИФИКАТ BEGIN-----**и**-----КОНЕЧНЫЙ СЕРТИФИКАТ-----**, вставить его в текстовый файл и сохранить его с дополнительным.PEM или.CER.

Windows может считать DER и форматы CER с его собственным Апплетом Управления сертификатами и показывает сертификат как показано на рисунке 5.

Рис. 5: Информация о сертификате

В некоторых случаях устройство требует определенного формата (ASCII или двоичные файлы). Для изменения этого загрузите сертификат от CA в необходимом формате или используйте программное средство преобразователя SSL, такое как https://www.sslshopper.com/ssl-converter.html.

Иерархия сертификата

Для доверия сертификату от оконечная точки должно быть доверие, уже установленное с CA. третьей стороны, Например, рисунок 6 показывает, что существует иерархия трех сертификатов.

Рис. 6: Иерархия сертификата

- **Verisign** является CA.
- **Класс 3 Verisign Расширенный SSL Проверки CA** является промежуточным звеном или подписанием серверного сертификата (сервер, авторизовавший CA выполнять сертификаты на его название).
- **www.website.com** является сервером или трудовой книжкой.

Ваша оконечная точка должна знать, что может доверять и CA и промежуточным сертификатам сначала, прежде чем она будет знать, что может доверять серверному сертификату, представленному Подтверждением связи SSL (подробные данные ниже). Чтобы лучше понять, как это доверие работает, обратитесь к разделу в этом документе: **Определите "Доверие" с Точки зрения Сертификата**.

Подписанные сертификаты по сравнению со сторонними сертификатами

Основные различия между самоподписанным и сторонними сертификатами - то, кто подписал сертификат, доверяете ли вы им.

Подписанный сертификат является сертификатом, подписанным сервером, который представляет его; поэтому, сервер/трудовая книжка и сертификат CA являются тем же.

Независимый поставщик CA является сервисом, предоставленным любым общественность CA (как Verisign, Поручите, Digicert) или сервер (как Windows 2003, Linux, Unix, IOS), который управляет законностью сервера/трудовой книжки.

Каждый может быть CA., Является ли ваша система тресты, что CA, тем, что имеет значение больше всего.

Общие имена и альтернативные имена субъекта

Общие имена (CN) и альтернативные имена субъекта (SAN) являются ссылками на IP-адрес или Полное доменное имя (FQDN) адреса, который запрашивают. Например, если вы вводите https://www. cisco . com, тогда CN или SAN должны иметь www. cisco . com в заголовке.

В примере, показанном на рисунке 7, сертификат имеет CN как www. cisco . com. URL-запрос на www. cisco . com от браузера проверяет URL FQDN против информации подарки сертификата. В этом случае они совпадают, и это показывает, что подтверждение связи SSL успешно. Этот веб-сайт был проверен, чтобы быть корректным веб-сайтом, и связь теперь зашифрована между рабочим столом и веб-сайтом.

Рисунок 7: Проверка веб-сайта

В том же сертификате существует SAN заголовок для трех адресов FQDN/DNS:

Рис. 8: SAN заголовок

Этот сертификат может аутентифицировать/сверять www. cisco . com (также определенный в CN), cisco.com и образы Cisco. cisco . com. Это означает, что можно также ввести cisco.com, и этот тот же сертификат может использоваться, чтобы аутентифицировать и зашифровать этот веб-сайт.

CUCM может создать SAN заголовки. См. документ Джейсона Берна, CUCM Загрузка веб-

Сертификатов GUI CCMAdmin на Сообществе поддержки для получения дополнительной информации о SAN заголовках.

Сертификаты подстановочного знака

Сертификаты подстановочного знака являются сертификатами, которые используют звездочку (*) для представления любой строки в разделе URL. Например, для имения сертификата для www. cisco . com, ftp. cisco . com, ssh. cisco . com, и так далее, администратор должен был бы только создать сертификат для *.cisco.com. Чтобы экономить деньги, администратор только должен купить одиночный сертификат и не должен покупать несколька серверов сертификатов.

Эта функция в настоящее время не поддерживается Cisco Unified Communications Manager (CUCM). Однако можно отслеживать это усовершенствование: CSCta14114: Запрос о поддержке сертификата подстановочного знака в CUCM и импорте с закрытым ключом.

Определите сертификаты

Когда сертификаты имеют ту же информацию в них, вы видите, является ли это тот же сертификат. Все сертификаты имеют уникальный серийный номер. Если сертификаты являются теми же сертификатами, восстановленными, или подделка, можно использовать это, чтобы выдержать сравнение. Рисунок 9 предоставляет пример:

Рис. 9: Certificate Serial Number

CSR и их цель

CSR обозначает Запрос подписи сертификата. Если вы хотите создать сторонний сертификат для сервера CUCM, вам нужен CSR для представления CA., Этот CSR много походит на PEM (ASCII) сертификат.

Примечание: Это не сертификат и не может использоваться в качестве один.

CUCM создает CSR автоматически через веб-GUI: **Cisco Унифицированный> Certificate Management> Security администрирования Операционной системы> Генерирует CSR>**, выбирает сервис, вы хотите создать сертификат>, тогда **Генерируют CSR**. Каждый раз, когда эта опция используется, новый секретный ключ и CSR генерируются.

Примечание: Секретный ключ является файлом, который уникален для этого сервера и сервиса. Это никогда не должно даваться никому! При обеспечении секретного ключа кому-то он ставит под угрозу безопасность, которую предоставляет сертификат. Кроме того, не восстанавливайте новый CSR для того же сервиса при использовании старого CSR для создания сертификата. CUCM удаляет старый CSR и секретный ключ и заменяет их обоих, который делает старый CSR бесполезным.

См. документацию Джейсона Берна относительно Сообщества поддержки: Загрузка CUCM веб-Сертификатов GUI CCMAdmin для получения информации о том, как создать CSR.

Использование Сертификатов Между Оконечная точкой и Процессом Квитирования SSL/TLS

Протокол подтверждения связи является серией упорядоченных сообщений, которые выполняют согласование о параметрах безопасности сеанса передачи данных. См. SSL/TLS подробно, который документирует последовательность сообщений в протоколе подтверждения связи. Они могут быть замечены в захвате пакета (PCAP). Подробные данные включают начальное, последующее, и заключительные сообщения, передаваемые и полученные между клиентом и сервером.

Как CUCM использует сертификаты

Различие Между tomcat и доверием tomcat

Когда сертификаты загружены к CUCM, существует две опции для каждого сервиса через **Cisco, которую Находит Унифицированный> Certificate Management> Security администрирования Операционной системы>**.

Пять сервисов, которые позволяют вам **управлять** сертификатами в CUCM:

- tomcat
- iPSec
- (диспетчер вызовов Call Manager)
- capf
- ТВ (в Выпуске 8.0 CUCM и позже)

Вот сервисы, которые позволяют вам **загружать** сертификаты к CUCM:

- tomcat
- доверие tomcat
- iPSec
- доверие ipsec
- (диспетчер вызовов Call Manager)
- callmanager-доверие
- capf
- capf-доверие

Это сервисы, доступные в Выпуске 8.0 CUCM и позже:

- ТВ
- телевизионное доверие
- телефонное доверие
- телефонное доверие vpn
- phone-sast-trust
- phone-ctl-trust

См. Руководства по обеспечению безопасности CUCM Выпуском для получения дополнительной информации на этих типах сертификатов. Этот раздел только объясняет различие между трудовой книжкой и трастовым сертификатом.

Например, с **tomcat**, **тресты tomcat** загружают CA и промежуточные сертификаты так, чтобы этот узел CUCM знал, что это может доверять любому сертификату, подписанному CA и промежуточным сервером. Сертификат tomcat является сертификатом, который представлен сервисом tomcat на этом сервере, если оконечная точка делает запрос HTTP к этому серверу. Для разрешения представления сторонних сертификатов tomcat узел CUCM

должен знать, что это может доверять CA и промежуточному серверу. Поэтому это - требование для загрузки CA и промежуточных сертификатов перед tomcat (сервис), сертификат загружен.

См. CUCM Джейсона Берна Загрузка веб-Сертификатов GUI CCMAdmin на Сообществе поддержки для получения информации, которая поможет вам понимать, как загрузить сертификаты к CUCM.

Каждый сервис имеет свою собственную трудовую книжку и трастовые сертификаты. Они не отделываются друг от друга. Другими словами, CA и промежуточный сертификат, загруженный как трастовый tomcat сервис, не могут использоваться сервисом CallManager.

Примечание: Сертификаты в CUCM на основу узла. Поэтому, если вам нужны сертификаты, загруженные к издателю, и вам нужны абоненты для имения тех же сертификатов, необходимо загрузить их к каждому индивидуальному серверу и узлу до Выпуска 8.5 CUCM. В Выпуске 8.5 CUCM и позже, существует сервис, который реплицирует загруженные сертификаты в остаток узлов в кластере.

Примечание: Каждый узел имеет другой CN. Поэтому CSR должен быть создан каждым узлом для сервиса для представления их собственных сертификатов.

Если у вас есть дополнительные конкретные вопросы на какой-либо из характеристик безопасности CUCM, обратитесь к документации безопасности.

Заключение

Этот документ помогает и создает высокий уровень знания о сертификатах. Этот предмет может иметь значение, может стать более всесторонним, но этот документ ознакомляет вас достаточно для работы с сертификатами. При наличии вопросов на каких-либо характеристиках безопасности CUCM, обратитесь к Руководствам по обеспечению безопасности CUCM Выпуском для получения дополнительной информации.

Дополнительные сведения

- Руководства по обслуживанию Cisco Unified Communications Manager (CallManager) и руководства по обеспечению безопасности
- CISCO UNIFIED COMMUNICATIONS MANAGER (CALLMANAGER)
- Cisco Unified Communications Manager Express
- Сообщество поддержки Cisco: CUCM загрузка веб-сертификатов GUI CCMAdmin
- Дефект CSCta14114: Запрос о поддержке сертификата подстановочного знака в CUCM и импорте с закрытым ключом
- Объясненный Cisco Emergency Responder (CER)
- Cisco Systems – техническая поддержка и документация