Проблема серверного сертификата Cisco Unified Mobility Advantage с ASA

Содержание

Введение

Этот документ описывает, как обмениваться подписанными сертификатами между Устройством адаптивной защиты (ASA) и сервером Cisco Unified Mobility Advantage (CUMA) и наоборот. Это также объясняет, как устранить неполадки общих проблем, который происходит, в то время как вы импортируете сертификаты.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Серия 5500 Cisco ASA
- Сервер Cisco Unified Mobility Advantage 7

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.

Сценарии развертывания

Существует два сценария развертывания для **прокси TLS**, используемого решением **для Преимущества Мобильности Cisco**.

Примечание: В обоих сценариях клиенты соединяются из Интернета.

1. Устройство адаптивной безопасности функционирует и как межсетевой экран и как прокси TLS.
2. Функции устройства адаптивной безопасности как TLS проксируют только.

В обоих сценариях необходимо экспортировать **Cisco серверный сертификат UMA** и **пара согласованных ключей** в формате **PKCS-12** и импортировать его к устройству адаптивной безопасности. Сертификат используется во время квитирования с Cisco клиенты UMA.

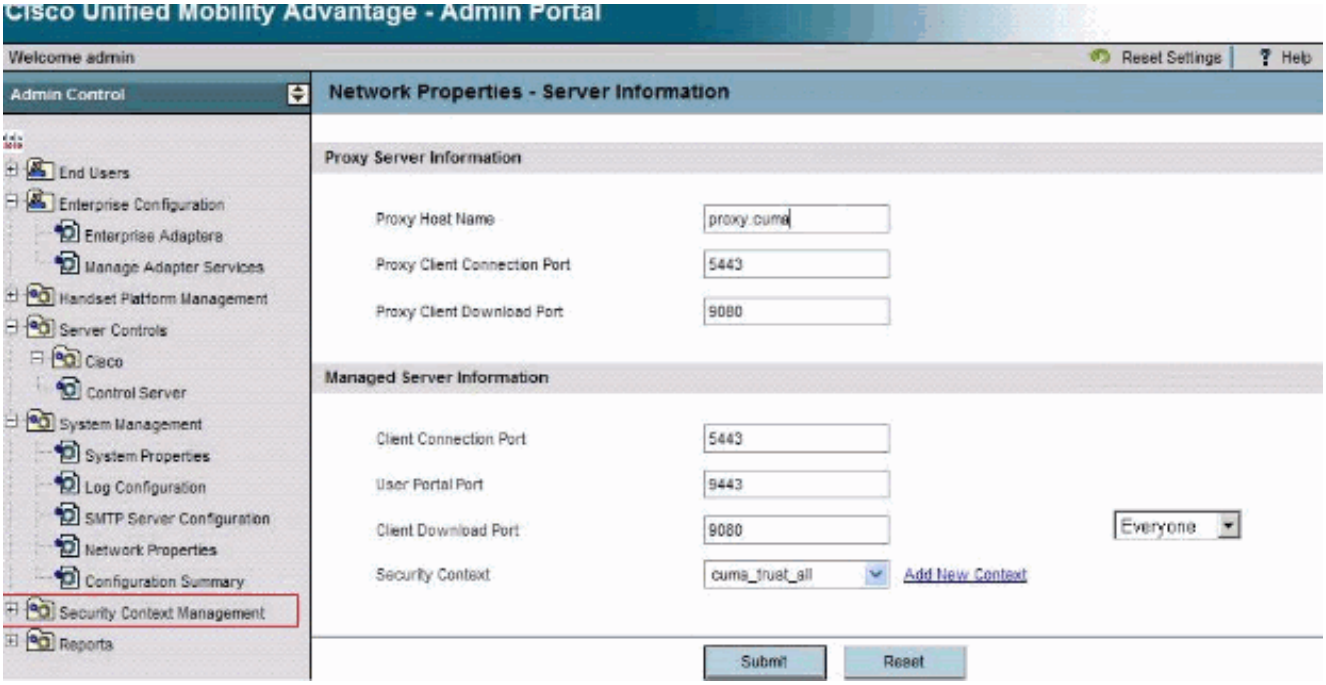
Установка Cisco подписанный сертификат сервера UMA в базе доверенных сертификатов устройства адаптивной безопасности необходима для устройства адаптивной безопасности для аутентификации Cisco сервер UMA во время квитирования между прокси устройства адаптивной безопасности и Cisco сервер UMA.

Установите Cisco Подписанный сертификат сервера UMA

Задачи, которые будут сделаны на сервере CUMA

Эти шаги должны быть выполнены на сервере CUMA. С этими шагами вы создаете подписанный сертификат на CUMA для обмена с ASA с CN=portal.aipc.com. Это должно быть установлено на базе доверенных сертификатов ASA. Выполните следующие действия:

1. Создайте самоподписанное свидетельство на сервере CUMA.Регистрируйтесь к порталу Admin Cisco Unified Mobility Advantage.Выберите **[+]** около менеджмента контекста
   безопасности.



Выберите **Security Contexts**.Выберите **Add Context**.Введите эти сведения:`Do you want to create/upload a new certificate? create`
`Context Name "cuma"`
`Description "cuma"`
`Trust Policy "Trusted Certificates"`
`Client Authentication Policy "none"`
`Client Password "changeme"`
`Server Name cuma.ciscodom.com`
`Department Name "vsec"`
`Company Name "cisco"`
`City "san jose"`
`State "ca"`
`Country "US"`

2. Загрузите Подписанные сертификаты от Cisco Unified Mobility Advantage. Выполните эти шаги для выполнения задачи:Выберите **[+]** около менеджмента контекста безопасности.Выберите **Security Contexts**.Выберите **Manage Context** около контекста безопасности, который держит сертификат для загрузки.Выберите **Download Certificate**.**Примечание:** Если сертификат является цепочкой и привязал корневые или промежуточные сертификаты, только первый сертификат в цепочке загружен. Это достаточно для подписанных сертификатов.Сохраните файл.
3. Следующий шаг должен добавить подписанный сертификат от Cisco Unified Mobility Advantage на ASA. Выполните эти шаги на ASA:Откройте подписанный сертификат от Cisco Unified Mobility Advantage в текстовом редакторе.Импортируйте сертификат в базу доверенных сертификатов устройства адаптивной защиты Cisco:`cuma-asa(config)# crypto ca trustpoint cuma-server-id-cert cuma-asa(config-ca-trustpoint)# enrollment terminal cuma-asa(config-ca-trustpoint)# crypto ca authenticate cuma-server-id-cert Enter the base 64 encoded CA certificate. End with the word "quit" on a line by itself ----BEGIN CERTIFICATE---- ** paste the contents from wordpad ** ----END CERTIFICATE----`
4. Подписанный сертификат ASA экспорта на сервере CUMA. Необходимо настроить Cisco Unified Mobility Advantage для требования сертификата от устройства адаптивной защиты Cisco. Выполните эти шаги для обеспечения требуемого подписанного сертификата. Эти шаги должны быть выполнены на ASA.Генерируйте новую пару ключей:`cuma-asa(config)# crypto key generate rsa label asa-id-key mod 1024 INFO: The name for the keys will be: asa-id-key Keypair generation process begin. Please wait...`Добавьте новую точку доверия:`cuma-asa(config)# crypto ca trustpoint asa-self-signed-id-cert cuma-asa(config-ca-trustpoint)# keypair asa-id-key cuma-asa(config-ca-trustpoint)# enrollment`

`self` Зарегистрируйте точку доверия:`cuma-asa(config-ca-trustpoint)# crypto ca enroll asa-self-signed-id-cert % The fully-qualified domain name in the certificate will be: cuma-asa.cisco.com % Include the device serial number in the subject name? [yes/no]: n Generate Self-Signed Certificate? [yes/no]: y`Экспортируйте сертификат в текстовый файл.`cuma-asa(config)# crypto ca export asa-self-signed-id-cert identity-certificate The PEM encoded identity certificate follows: -----BEGIN CERTIFICATE----- Certificate data omitted -----END CERTIFICATE-----`

5. Скопируйте предыдущие выходные данные к текстовому файлу и добавьте его к базе доверенных сертификатов сервера CUMA и используйте эту процедуру:Выберите **[+]** около менеджмента контекста безопасности.Выберите **Security Contexts**.Выберите **Manage Context** около Контекста безопасности, в который вы импортируете подписанный сертификат.Выберите **Import** в панели Надежных сертификатов.Вставьте текст сертификата.Назовите сертификат.Выберите **Import**.**Примечание:** Для Удаленной Целевой конфигурации звоните в настольный телефон, чтобы определить, звонит ли сотовый телефон в то же время. Это подтвердило бы, что мобильное подключение работает и что нет никакой проблемы с Удаленной Целевой конфигурацией.

Проблема, добавляющая Запрос сертификата CUMA к другим центрам сертификации

Проблема 1

Много установок демонстрации/прототипа, где помогает, работает ли решение CUMC/CUMA с надежными сертификатами, самоподписаны или получены из *других центров сертификации*. Сертификаты Verisign являются дорогими, и требуется много времени для получения этих сертификатов. Это хорошо если подписанные сертификаты поддержки решений и сертификаты от другого CAs.

Текущими поддерживаемыми сертификатами является GeoTrust и Verisign. Это задокументировано в идентификатор ошибки Cisco CSCta62971 (только зарегистрированные клиенты)

Ошибка: Неспособный соединиться

Когда вы пытаетесь обратиться к пользовательской странице портала, например, `https://<host>:8443`, сообщение об ошибках `Unable to connect` появляется.

Решение

Эта проблема задокументирована в идентификатор ошибки Cisco CSCsm26730 (только зарегистрированные клиенты). Для доступа к пользовательской странице портала завершите этот обходной путь:

Причиной этой проблемы является долларовый символ, так выйдите из долларового символа с другим долларовым символом в **server.xml файле** управляемого сервера. Например, отредактируйте/opt/cuma/jboss-4.0.1sp1/server/cuma/deploy/jbossweb-tomcat50.sar/server.xml.

В линии: **keystorePass = "pa$word"** maxSpareThreads = "15"

Замените символ $ $$. Это похоже **на keystorePass = "$word pa$"** maxSpareThreads = "15".

Некоторые страницы в Портале Admin CUMA не доступны

Эти страницы не могут быть просмотрены в **Портале Admin CUMA**:

- активируйте/деактивируйте пользователя
- поиск/обслуживание

Если пользователь щелкает по одной из вышеупомянутых двух страниц в меню налево, браузер, кажется, указывает, что это загружает страницу, но ничто не происходит (только предыдущая страница, которая была в браузере, видимо).

Решение

Для решения этого вопроса, отнесенного к странице пользователя, измените порт, используемый для Active Directory к **3268**, и перезапустите CUMA.

Дополнительные сведения

- Прокси ASA-CUMA пошаговая Конфигурация
- V1 Introduccion al ASR5000
- Обновление Cisco Unified Mobility Advantage
- Поддержка голосовых технологий
- Поддержка продуктов Голосовой и Унифицированной связи
- Cisco Systems – техническая поддержка и документация