SSLVPN с примером конфигурации IP-телефонов

Содержание

Введение

Этот документ описывает, как настроить IP-телефоны через VPN Уровня защищенных сокетов (VPN SSL), также известный как WebVPN. Два Менеджера Унифицированной связи Cisco (CallManagers) и три типа сертификатов используются с этим решением.
CallManagers:

- Cisco Unified Communications Manager (CUCM)
- Cisco Unified Communications Manager Express (Cisco унифицированный CME)

Типы сертификата:

- Подписанные сертификаты
- Сторонние сертификаты, те, которые Поручают, Thawte и GoDaddy
- Cisco центр сертификации (CA) IOS®/устройства адаптивной защиты (ASA)

Ключевое понятие для понимания - то, что, как только конфигурация на Шлюзе VPN SSL и CallManager завершена, необходимо присоединиться к IP-телефонам локально. Это позволяет телефонам присоединиться к CUCM и использовать корректную информацию VPN и сертификаты. Если к телефонам не присоединяются локально, они не могут найти Шлюз VPN SSL и не имеют корректных сертификатов для завершения квитирования VPN SSL.

Наиболее распространенные конфигурации являются CME CUCM/Unified с подписанными сертификатами ASA и подписанными сертификатами Cisco IOS. Следовательно, их является самым легким настроить.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Cisco Unified Communications Manager (CUCM) или Cisco Unified Communications Manager Express (Cisco унифицированный CME)
- SSL VPN – WebVPN
- Устройство адаптивной защиты Cisco (ASA)
- Типы сертификата, такой, как самоподписано, независимый поставщик и центры сертификации

Используемые компоненты

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

- ASA Premium лицензия.
- Лицензия Телефона AnyConnect VPN.
  - Для Выпуска 8.0.x ASA лицензия является AnyConnect для Телефона Linksys.
  - Для Выпуска 8.2.x ASA или позже, лицензия является AnyConnect для Телефона VPN Cisco.
- Шлюз VPN SSL: ASA 8. 0 или позже (с AnyConnect для Лицензии Телефона VPN Cisco), или Cisco IOS Software Release 12.4T или позже.
  - Cisco IOS Software Release 12.4T или позже формально не поддерживается, как задокументировано в Руководство Конфигурации VPN SSL.
  - В программном обеспечении Cisco IOS версии 15.0(1)M Шлюз VPN SSL является посчитанной на место функцией лицензирования на Cisco 880, Cisco 890, Cisco 1900, Cisco 2900 и платформах Cisco 3900. Действующая лицензия требуется для успешного сеанса VPN SSL.
- (диспетчер вызовов Call Manager): CUCM 8.0.1 или позже, или Унифицированный CME 8.5 или позже.

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.

Настройка

Примечания:

Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

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

Основная конфигурация VPN SSL ASA

Основная конфигурация VPN SSL ASA описана в этих документах:

- ASA 8. x: Доступ к VPN с помощью VPN-клиента AnyConnect, для которого используется пример конфигурации с недоверительным сертификатом
- Соединения клиента AnyConnect VPN Client Настройки

Как только эта конфигурация завершена, удаленный тестовый ПК должен быть в состоянии соединиться со Шлюзом VPN SSL, подключением через AnyConnect, и пропинговать CUCM. Гарантируйте, что ASA имеет AnyConnect для лицензии Cisco IP Phone. (Используйте команду **версии показа**.) И TCP и порт 443 UDP должны быть открыты между шлюзом и клиентом.

Примечание: Распределенная нагрузку VPN SSL не поддерживается для телефонов VPN.

CUCM: VPN SSL ASA с конфигурацией подписанных сертификатов

См. VPN SSL IP-телефона к ASA с помощью AnyConnect для более подробной информации.

ASA должен иметь лицензию на AnyConnect для Телефона VPN Cisco. После настройки VPN SSL вы тогда настраиваете свой CUCM для VPN.

1. Используйте эту команду для экспортирования подписанного сертификата от ASA:

   `ciscoasa(config)# crypto ca export trustpoint name identity-certificate`Эта команда отображает pem-закодированный сертификат идентификации к терминалу.
2. Скопируйте и вставьте сертификат текстовому редактору и сохраните его как файл .pem. Обязательно включайте СЕРТИФИКАТ BEGIN и КОНЕЧНЫЕ линии СЕРТИФИКАТА, или сертификат не импортирует правильно. Не модифицируйте формат сертификата, потому что это вызовет проблемы, когда телефон попытается аутентифицироваться на ASA.
3. Переместитесь к **Cisco по Унифицированному> Certificate Management> Security администрирования Операционной системы> Сертификат/Цепочка сертификатов Загрузки** для загрузки файла сертификата в РАЗДЕЛ УПРАВЛЕНИЯ СЕРТИФИКАТАМИ CUCM.
4. Загрузите CallManager.pem, CAPF.pem и сертификаты Cisco_Manufacturing_CA.pem от

той же области, используемой для загрузки подписанных сертификатов из ASA (см. Шаг 1), и сохраните их к рабочему столу.

1. Например, для импорта CallManager.pem к ASA, используйте эти команды:

```
ciscoasa(config)# crypto ca trustpoint certificate-name
ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config)# crypto ca authenticate certificate-name
```

2. Когда вам предлагают скопировать и вставить соответствующий сертификат для точки доверия, открыть файл, вы сохранили от CUCM, затем скопируйте и вставьте закодированный Base64 сертификат. Обязательно включайте СЕРТИФИКАТ BEGIN и КОНЕЧНЫЕ линии СЕРТИФИКАТА (с дефисами).
3. Введите **конец**, тогда **нажмите клавишу возврата**.
4. Когда предложено принять сертификат, введите **да,** затем нажмите **Enter**.
5. Повторите шаги 1 - 4 для других двух сертификатов (CAPF.pem, Cisco_Manufacturing_CA.pem) от CUCM.

5. Настройте CUCM для корректных конфигураций VPN, как описано в CUCM IPphone VPN config.pdf.

Примечание: Шлюз VPN, настроенный на CUCM, должен совпасть с URL, который настроен на Шлюзе VPN. Если шлюз и URL не совпадают, телефон не может решить адрес, и вы не будете видеть отладок на Шлюзе VPN.

- На CUCM: URL Шлюза VPN является https://192.168.1.1/VPNPhone
- На ASA используйте эти команды:

```
ciscoasa# configure terminal
ciscoasa(config)# tunnel-group VPNPhones webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-url https://192.168.1.1/VPNPhone
enable
ciscoasa(config-tunnel-webvpn)# exit
```

- Можно использовать эти команды на Менеджере устройств адаптивной безопасности (ASDM) (ASDM) или под профилем подключения.

CUCM: VPN SSL ASA со сторонней конфигурацией сертификатов

Эта конфигурация подобна конфигурации, описанной в CUCM: SSLVPN ASA с Разделом конфигурации Подписанных сертификатов, за исключением того, что вы используете сторонние сертификаты. Настройте SSL VPN на ASA со сторонними сертификатами, как описано в ASA 8.x Вручную Сертификаты Поставщика третьей стороны Установки для использования с Примером конфигурации WebVPN.

Примечание: Необходимо скопировать полную цепочку сертификатов от ASA до CUCM и включать все промежуточное звено и корневые сертификаты. Если CUCM не включает полную цепочку, телефоны не имеют необходимых сертификатов для аутентификации и откажут квитирование VPN SSL.

Основная конфигурация VPN SSL IOS

Примечание: IP-телефоны названы как не поддерживаемыми в VPN SSL IOS;

конфигурации находятся в оптимальном уровне только.

Основная конфигурация VPN SSL Cisco IOS описана в этих документах:

- Пример конфигурации клиента SSL VPN на IOS с помощью SDM
- Клиент AnyConnect VPN Client на маршрутизаторе IOS с зоной IOS базирующийся пример конфигурации межсетевого экрана политики

Как только эта конфигурация завершена, удаленный тестовый ПК должен быть в состоянии соединиться со Шлюзом VPN SSL, подключением через AnyConnect, и пропинговать CUCM. В Cisco IOS 15.0 и позже, у вас должна быть допустимая лицензия VPN SSL для выполнения этой задачи. И TCP и порт 443 UDP должны быть открыты между шлюзом и клиентом.

CUCM: VPN SSL IOS с конфигурацией подписанных сертификатов

Эта конфигурация подобна конфигурации, описанной в CUCM: ASA SSLVPN со Сторонней Конфигурацией Сертификатов и CUCM: ASA SSLVPN с Разделами конфигурации Подписанных сертификатов. Различия:

1. Используйте эту команду для экспортирования подписанного сертификата от маршрутизатора:

   ```
   R1(config)# crypto pki export trustpoint-name pem terminal
   ```
2. Используйте эти команды для импорта сертификатов CUCM:

   ```
   R1(config)# crypto pki trustpoint certificate-name
   R1(config-ca-trustpoint)# enrollment terminal
   R1(config)# crypto ca authenticate certificate-name
   ```

Конфигурация контекста WebVPN должна показать этот текст:

```
R1(config)# crypto pki trustpoint certificate-name
R1(config-ca-trustpoint)# enrollment terminal
R1(config)# crypto ca authenticate certificate-name
```

Настройте CUCM, как описано в CUCM: ASA SSLVPN с Разделом конфигурации Подписанных сертификатов.

CUCM: VPN SSL IOS со сторонней конфигурацией сертификатов

Эта конфигурация подобна конфигурации, описанной в CUCM: ASA SSLVPN с Разделом конфигурации Подписанных сертификатов. Настройте свой WebVPN со сторонним сертификатом.

> **Примечание:** Необходимо скопировать полную цепочку сертификатов WebVPN к CUCM и включать все промежуточное звено и корневые сертификаты. Если CUCM не включает полную цепочку, телефоны не имеют необходимых сертификатов для аутентификации и откажут квитирование VPN SSL.

Унифицированный CME: VPN SSL ASA/Маршрутизатора с Самоподписанной

Конфигурацией Сертификатов Сертификатов/Независимого поставщика

Конфигурация для Унифицированного CME подобна конфигурациям CUCM; например, конфигурации оконечной точки WebVPN являются тем же. Единственное существенное различие является конфигурациями Унифицированного агента вызовов CME. Настройте группу VPN и политику VPN для Унифицированного CME, как описано в VPN-клиенте SSL (SVC) Настройки для IP-телефонов SCCP.

> **Примечание:** Унифицированный CME поддерживает только Протокол SCCP и не поддерживает Протокол SIP для телефонов VPN.

> **Примечание:** Нет никакой потребности экспортировать сертификаты от Унифицированного CME до ASA или маршрутизатора. Только необходимо экспортировать сертификаты от ASA или Шлюза WebVPN маршрутизатора к Унифицированному CME.

Для экспортирования сертификатов от Шлюза WebVPN обратитесь к ASA/разделу Маршрутизатор. При использовании стороннего сертификата необходимо включать полную цепочку сертификатов. Для импорта сертификатов к Унифицированному CME используйте тот же метод, как используется к сертификатам импорта в маршрутизатор:

```
CME(config)# crypto pki trustpoint certificate-name
CME(config-ca-trustpoint)# enrollment terminal
CME(config)# crypto ca authenticate certificate-name
```

UC 520 IP-телефонов с конфигурацией VPN SSL

Унифицированная связь Cisco IP-телефон UC 520 Модели серии 500 очень отличается от конфигураций CME и CUCM.

- Так как IP-телефон UC 520 является и CallManager и Шлюзом WebVPN, нет никакой потребности настроить сертификаты между двумя.
- Настройте WebVPN на маршрутизаторе, как вы обычно были бы со сторонними сертификатами или подписанными сертификатами.
- IP-телефон UC 520 имеет созданный в клиенте WebVPN, и можно настроить его так же, как вы были бы обычный ПК для соединения с WebVPN. Введите шлюз, тогда сочетание имени пользователя и пароля.
- IP-телефон UC 520 совместим с SPA IP-телефона Cisco для малого бизнеса 525G телефоны.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

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