Настройте телефон AnyConnect VPN с проверкой подлинности сертификата на ASA

Содержание

[Введение](#)
[Предварительные условия](#)
[Требования](#)
[Используемые компоненты](#)
[Условные обозначения](#)
[Телефонные Типы сертификата](#)
[Настройка](#)
[Конфигурации](#)
[Проверка](#)
[Устранение неполадок](#)
[Дополнительные сведения](#)

Введение

Этот документ предоставляет пример конфигурации, который показывает, как настроить Устройство адаптивной защиты (ASA) и Устройства CallManager для обеспечения проверки подлинности сертификата для клиентов AnyConnect, которые работают на Cisco IP Phone. После того, как эта конфигурация завершена, Cisco IP Phone могут установить VPN-подключения к ASA, которые используют сертификаты для обеспечения связи.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- AnyConnect Premium лицензия SSL
- AnyConnect для лицензии телефона VPN Cisco

Зависящий от версии ASA, вы будете видеть или "AnyConnect для телефона Linksys" для Выпуска 8.0.x ASA или "AnyConnect для Телефона VPN Cisco" для Выпуска 8.2.x ASA или позже.

Используемые компоненты

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

- ASA - Выпуск 8.0 (4) или позже
- Модели IP-телефона - 7942 / 7962 / 7945 / 7965 / 7975
- Телефоны - 8961 / 9951 / 9971 с микропрограммным обеспечением Выпуска 9.1 (1)
- Телефон - Выпуск 9.0 (2) SR1S - Протокол SCCP или позже
- Cisco Unified Communications Manager (CUCM) - Выпуск 8.0.1.100000-4 или позже

Версии, используемые в этом примере конфигурации, включают:

- ASA - выпуск 9.1 (1)
- CallManager - выпуск 8.5.1.10000-26

Для полного списка поддерживаемых телефонов в вашей версии CUCM выполните эти шаги:

1. Откройте этот URL: https://*<IP-адрес сервера CUCM>*:8443/cucreports/systemReports.do
2. Выберите **Unified CM Phone Feature List> Generate новый отчёт> Функция: Виртуальная частная сеть**.

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.

Телефонные Типы сертификата

Cisco использует эти Типы сертификата в телефонах:

- Изготовитель установленный сертификат (MIC) - MIC включены во все 7941, 7961, и более новые Cisco IP Phone модели. MIC являются 2048-разрядными ключевыми сертификатами, которые подписаны Центром сертификации (CA) Cisco. Когда MIC присутствует, необязательно для установки логически значимого сертификата (LSC). Для CUCM для доверия сертификату MIC это использует предварительно установленные сертификаты CA CAP-RTP-001, CAP-RTP-002 и Cisco_Manufacturing_CA в его базе доверенных сертификатов сертификата.
- LSC - LSC защищает соединение между CUCM и телефоном после настройки режима безопасности устройства для аутентификации или шифрования.LSC обладает открытым ключом для Cisco IP Phone, который подписан секретным ключом функции представительства сертифицирующей организации (CAPF) CUCM. Это - предпочтительный способ (в противоположность использованию MIC), потому что только Cisco IP Phone, которые вручную настроены администратором, позволяют загрузить и проверить файл CTL.**Примечание:** Из-за риска повышенного уровня

безопасности, Cisco рекомендует использование MIC исключительно для установки LSC а не для продолжительного использования. Клиенты, которые настраивают Cisco IP Phone для использования MIC для аутентификации Transport Layer Security (TLS) или для любой другой цели, делают так в их собственном риске.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

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

Конфигурации

Этот документ описывает эти конфигурации:

- Конфигурация ASA
- Конфигурация CallManager
- Конфигурация VPN на CallManager
- Установка сертификатов на IP-телефонах

Конфигурация ASA

Конфигурация ASA является почти тем же как тогда, когда вы подключаете компьютер клиента AnyConnect с ASA. Однако эти ограничения применяются:

- Туннельная группа должна иметь URL группы. Этот URL будет настроен в CM под URL Шлюза VPN.
- Групповая политика не должна содержать разделение туннеля.

Эта конфигурация использует ранее настроенный и установленный ASA (самоподписанная или третья сторона) сертификат в точке доверия Протокола SSL устройства ASA. Дополнительные сведения см. в следующих документах:

- Цифровые сертификаты Настройки
- ASA 8. x Вручную Сертификаты Поставщика третьей стороны Установки для использования с Примером конфигурации WebVPN
- ASA 8. x: Доступ к VPN с помощью VPN-клиента AnyConnect, для которого используется пример конфигурации с недоверительным сертификатом

Соответствующая конфигурация ASA:

```
ip local pool SSL_Pool 10.10.10.1-10.10.10.254 mask 255.255.255.0
group-policy GroupPolicy_SSL internal
group-policy GroupPolicy_SSL attributes
split-tunnel-policy tunnelall
vpn-tunnel-protocol ssl-client

tunnel-group SSL type remote-access
tunnel-group SSL general-attributes
address-pool SSL_Pool
default-group-policy GroupPolicy_SSL
```

```
tunnel-group SSL webvpn-attributes
authentication certificate
group-url https://asa5520-c.cisco.com/SSL enable

webvpn
enable outside
anyconnect image disk0:/anyconnect-win-3.0.3054-k9.pkg
anyconnect enable

ssl trust-point SSL outside
```

Конфигурация CallManager

Чтобы экспортировать сертификат от ASA и импортировать сертификат в CallManager как Телефонный Трастовый VPN сертификат, выполните эти шаги:

1. Зарегистрируйте генерируемый сертификат в CUCM.
2. Проверьте сертификат, используемый для SSL.`ASA(config)#`**`show run ssl`**
   `ssl trust-point SSL outside`
3. Экспортируйте сертификат.`ASA(config)#`**`crypto ca export SSL identity-certificate`**
   Закодированный сертификат идентификации Privacy Enhanced Mail (PEM) придерживается:
   ```
   -----BEGIN CERTIFICATE-----
   ZHUxFjAUBgkqhkiG9w0BCQIWB0FTQTU1NDAwHhcNMTMwMTMwMTM1MzEwWhcNMjMw
   MTI4MTM1MzEwWjAmMQwwCgYDVQQDEwNlZHUxFjAUBgkqhkiG9w0BCQIWB0FTQTU1
   NDAwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMYcrysjZ+MawKBx8Zk69SW4AR
   FSpV6FPcUL7xsovhw6hsJE/2VDgd3pkawc5jcl5vkcpTkhjbf2xC4C1q6ZQwpahde22sdf1
   wsidpQWq1DDrJD1We83L/oqmhkWJO7QfNrGZhOLv9xOpR7BFpZd1yFyzwAPkoBl1
   -----END CERTIFICATE-----
   ```
4. Скопируйте текст с терминала и сохраните его как файл .pem.
5. Войдите к CallManager и выберите **Unified OS Administration> Security> Certificate Management> Upload Certificate> Select Phone-VPN-trust** для загрузки файла сертификата, сохраненного в предыдущем шаге.

Конфигурация VPN на CallManager

1. Переместитесь к Cisco по унифицированному администрированию CM.
2. От строки меню выберите **Advanced Features> VPN> VPN Gateway**.
3. В Окне конфигурации Шлюза VPN выполните эти шаги:В Поле имени Шлюза VPN введите имя. Это может быть любым названием.В Поле описания Шлюза VPN введите (дополнительное) описание.В поле VPN Gateway URL введите URL группы, определенный в ASA.В Сертификатах VPN в этом поле Location выберите сертификат, который был загружен к CallManager ранее для перемещения его от базы доверенных сертификатов до этого местоположения.
4. От строки меню выберите **Advanced Features> VPN> VPN Group**.
5. В поле All Available VPN Gateways выберите VPN Gateway, ранее определенный. Нажмите стрелку вниз для перемещения выбранного шлюза в Выбранные Шлюзы VPN в этом поле VPN Group.
6. От строки меню выберите **Advanced Features> VPN> VPN Profile**.
7. Для настройки Профиля VPN завершите все поля, которые отмечены звездочкой (*).**Включите Автоматическую Сеть, Обнаружьте:** Если включено, телефон VPN пропинговывает сервер TFTP и если никакой ответ не получен, это автоинициирует VPN-подключение.**Включите Проверку Идентификатора хоста:** Если включено, телефон VPN сравнивает FQDN URL Шлюза VPN против CN/SAN сертификата. Клиент не в состоянии соединяться, если они не совпадают или если используется сертификат

подстановочного знака со звездочкой (*).**Устойчивость Enable Password:** Это позволяет телефону VPN кэшировать имя пользователя и пароль для следующей попытки VPN.

8. В Окне конфигурации Общего телефонного профиля нажмите **Apply Config** для применения новой конфигурации VPN. Можно использовать "Стандартный Общий телефонный профиль" или создать новый профиль.
9. При создании нового профиля для определенных телефонов/пользователей перейдите к Окну конфигурации телефона. В поле Common Phone Profile выберите **Standard Common Phone Profile**.
10. Зарегистрируйте телефон к CallManager снова для загрузки новой конфигурации.

Конфигурация проверки подлинности сертификата

Для настройки проверки подлинности сертификата выполните эти шаги в CallManager и ASA:

1. От строки меню выберите **Advanced Features> VPN> VPN Profile**.
2. Подтвердите, что поле Client Authentication Method установлено в **Сертификат.**
3. Войдите к CallManager. От строки меню выберите **Unified OS Administration> Security> Certificate Management> Find**.
4. Экспортируйте корректный сертификат (сертификаты) для выбранного метода проверки подлинности сертификата:MIC: Cisco_Manufacturing_CA - аутентифицируют IP-телефоны с MICLSC: функция представительства сертифицирующей организации (CAPF) Cisco - аутентифицирует IP-телефоны с LSC
5. Найдите сертификат, или Cisco_Manufacturing_CA или CAPF. Загрузите файл .pem и сохраните как файл .txt
6. Создайте новую точку доверия на ASA и аутентифицируйте точку доверия с предыдущим сохраненным сертификатом. То, когда вам предлагают для base64, закодировало сертификат CA, выберите и вставьте текст в загруженном файле .pem наряду с BEGIN и Конечными линиями. Пример: `ASA (config)#`**`crypto ca trustpoint CM-Manufacturing`**
   ```
   ASA(config-ca-trustpoint)#enrollment terminal
   ASA(config-ca-trustpoint)#exit
   ASA(config)#crypto ca authenticate CM-Manufacturing
   ASA(config)#

   <base-64 encoded CA certificate>

   quit
   ```
7. Подтвердите, что аутентификация на туннельной группе установлена в проверку подлинности сертификата.`tunnel-group SSL webvpn-attributes`
   ```
   authentication certificate
   group-url https://asa5520-c.cisco.com/SSL enable
   ```

Установка сертификатов на IP-телефонах

IP-телефоны могут работать или с MIC или с LSC, но процесс конфигурирования является другим для каждого сертификата.

Установка MIC

По умолчанию все телефоны, которые поддерживают VPN, предварительно загружены с MIC. 7960 и 7940 телефонов не идут с MIC и требуют, чтобы процедура специальной установки для LSC зарегистрировалась надежно.

Примечание: Cisco рекомендует использовать MIC для установки LSC только. Cisco поддерживает LSC для аутентификации TLS подключение с CUCM. Поскольку корневые сертификаты MIC могут поставиться под угрозу, клиенты, которые устанавливают настройки телефонов для использования MIC для аутентификации TLS или для любой другой цели, делают так в их собственном риске. Если MIC поставились под угрозу, Cisco не принимает ответственности.

Установка LSC

1. Включите сервис CAPF на CUCM.
2. После того, как сервис CAPF активирован, назначьте телефонные инструкции генерировать LSC в CUCM. Войдите к Cisco в Унифицированное администрирование CM и выберите **Device> Phone**. Выберите телефон, которого вы установили настройки.
3. В Разделе сведений функции представительства сертифицирующей организации (CAPF) гарантируйте, что все параметры настройки корректны, и операция установлена в будущую дату.
4. Если Режим аутентификации установлен в Пустую строку или Существующий сертификат, никакие дальнейшие действия не требуются.
5. Если Режим аутентификации установлен в строку, вручную выберите**> Security Settings Конфигурация> **#> LSC> Обновление** в телефонной консоли.

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Проверка ASA

```
ASA5520-C(config)#show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : CP-7962G-SEPXXXXXXXXXXXX
Index : 57
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium, AnyConnect for Cisco VPN Phone
Encryption : AnyConnect-Parent: (1)AES128 SSL-Tunnel: (1)AES128
DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)SHA1 SSL-Tunnel: (1)SHA1
DTLS-Tunnel: (1)SHA1Bytes Tx : 305849
Bytes Rx : 270069Pkts Tx : 5645
Pkts Rx : 5650Pkts Tx Drop : 0
Pkts Rx Drop : 0Group Policy :
GroupPolicy_SSL Tunnel Group : SSL
Login Time : 01:40:44 UTC Tue Feb 5 2013
Duration : 23h:00m:28s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
```

```
AnyConnect-Parent:
Tunnel ID : 57.1
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Encryption : AES128 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client Type : AnyConnect Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)
Bytes Tx : 1759 Bytes Rx : 799
Pkts Tx : 2 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 57.2
Public IP : 172.16.250.15
Encryption : AES128 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 50529
TCP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client Type : SSL VPN Client
Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)
Bytes Tx : 835 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 57.3
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Encryption : AES128 Hashing : SHA1
Encapsulation: DTLSv1.0 UDP Src Port : 51096
UDP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client Type : DTLS VPN Client
Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)
Bytes Tx : 303255 Bytes Rx : 269270
Pkts Tx : 5642 Pkts Rx : 5649
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

Проверка CUCM

Устранение неполадок

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

Связанные дефекты

- Идентификатор ошибки Cisco CSCtf09529, Добавляет поддержка функции VPN в CUCM для 8961, 9951, 9971 телефон
- Идентификатор ошибки Cisco CSCuc71462, аварийное переключение VPN IP-телефона занимает 8 минут
- Идентификатор ошибки Cisco CSCtz42052, Поддержка VPN SSL IP-телефона Номеров Порта по умолчанию Non
- Идентификатор ошибки Cisco CSCth96551, Не все ASCII - символы поддерживаются во время телефонного пользователя VPN + вход в систему пароля.
- Идентификатор ошибки Cisco CSCuj71475, Ручная запись TFTP необходима для VPN IP-телефона
- Идентификатор ошибки Cisco CSCum10683, IP-телефоны, не регистрирующие,

отсутствовал, размещенный, или принятые вызовы

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация