Нулевые сенсорные развертывания (ZTD) VPN Удаленный Пример конфигурации Офисов/Спиц

Содержание

Введение

Безопасные и эффективные развертывания и условие Удаленных Офисных маршрутизаторов (иногда названный Спицами) могут быть сложной задачей. Удаленные офисы могли бы быть в местоположениях, где это - проблема сделать, чтобы Наладчик настроил маршрутизатор на месте, и большинство инженеров выбирает риск потенциальной угрозы безопасности и not to send pre-configured Spoke routers due to the cost. Этот документ описывает, как опция Zero Touch Deployment (ZTD) является экономически эффективным и масштабируемым решением для таких развертываний.

Предварительные условия

Требования

- Любой маршрутизатор Cisco IOS®, который имеет USB-порт, который поддерживает Карты флэш-памяти с интерфейсом USB. Для получения дополнительной информации посмотрите eToken USB и Поддержку Функций Флэша USB.
- Эта функция подтверждена, чтобы продолжить работать почти любая платформа Cisco 8xx. Для получения дополнительной информации см. Описание технологических решений Файлов конфигурации по умолчанию (Поддержка функций на ISR Серии Cisco 800).

- Другие платформы, которые имеют USB-порты как серия маршрутизатора с интеграцией служб (ISR) G2 и 43xx/44xx.

Используемые компоненты

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

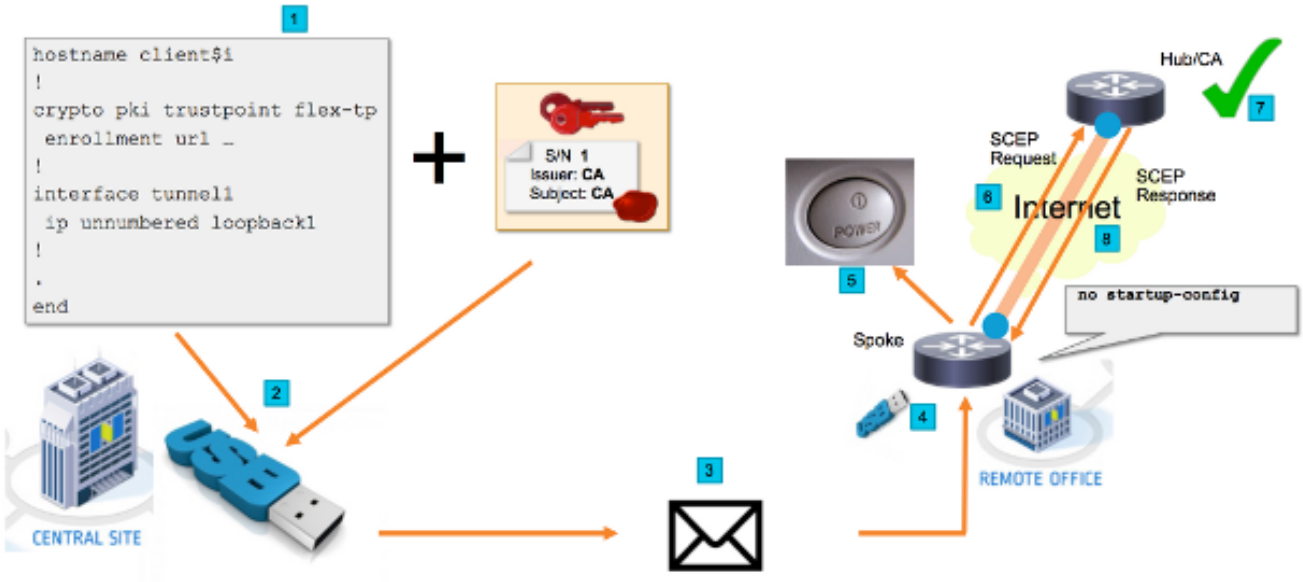
- Протокол SCEP (SCEP)
- Нулевые Сенсорные Развертывания через USB
- DMVPN/FlexVPN/Site-to-site VPN

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

> **Примечание:** Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети



Сетевой поток

1. В Центральном узле (Headquarter Компании) создан шаблон Конфигурации оконечного устройства. Шаблон содержит сертификат Центра сертификации (CA), который подписал сертификат Маршрутизатора концентратора VPN.
2. Шаблон конфигурации инстанцируют на USB - КЛЮЧЕ в файле, названном **ciscortr.cfg**. Этот файл конфигурации содержит Лучевую определенную конфигурацию для маршрутизатора, который будет развернут. **Примечание:** Конфигурация на USB не

содержит уязвимых данных кроме IP-адресов и сертификата CA. Нет никакого секретного ключа Луча или CA Сервера.

3. Карта флэш-памяти с интерфейсом USB передается Удаленному офису через почту или компанию доставки пакета.
4. Маршрутизатор на конце луча также передается Удаленному офису непосредственно от Производства Cisco.
5. В Удаленном офисе маршрутизатор связан с питанием и телеграфирован к сети, как объяснено в инструкциях, которые включены с картой флэш-памяти с интерфейсом USB. Затем карта флэш-памяти с интерфейсом USB вставлена в маршрутизатор. **Примечание:** Нет мало ни к каким техническим навыкам, вовлеченным в этот шаг, таким образом, он может легко быть выполнен любым офисным персоналом.
6. Однажды загрузки маршрутизатора это читает конфигурацию из **usbflash0:/ciscortr.cfg.** Как только маршрутизатор включился, запрос Протокола SCEP (SCEP) отправлен к Серверу CA.
7. На Сервере CA или Ручное или Автоматическое Предоставление может быть настроено на основе политики безопасности компании. Когда настроено для ручного предоставления сертификата, внеполосная проверка Запроса SCEP должна быть выполнена (Проверка проверки IP-адреса, учетная проверка для персонала , который выполняет развертывания, и т.д.). Этот шаг мог бы отличаться на основе Сервера CA t, шляпа используется.
8. Как только Ответ SCEP получен Маршрутизатором на конце луча, который теперь имеет подтвержденный сертификат, сеанс IKE аутентифицируется с Концентратором VPN, и Туннель успешно устанавливает.

Конфигурации/Шаблон

Этот пример выходных данных показывает образцовому FlexVPN Удаленное Конфигурирование станции, которое помещено на флэш-накопитель в **usbflash0:/ciscortr.cfg** файле.

```
hostname client1




!
interface GigabitEthernet0
 ip address dhcp
!
crypto pki trustpoint client1
! CA Server's URL
 enrollment url http://10.122.162.242:80
! These fields needs to be filled, to avoid prompt while doing enroll
serial-number none
 ip-address none
 password
 subject-name cn=client1.cisco.com ou=cisco ou
!
crypto pki certificate chain client1
 certificate ca 01
 ! CA Certificate here
       quit
!
```

```
crypto ikev2 profile default
 match identity remote any
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint client1
 aaa authorization group cert list default default
!
interface Tunnel1
 ip unnumbered GigabitEthernet0
 tunnel source GigabitEthernet0
 tunnel mode ipsec ipv4
! Destination is Internet IP Address of VPN Hub
 tunnel destination 172.16.0.2
 tunnel protection ipsec profile default
!
event manager applet import-cert
! Start importing certificates only after 60s after bootup
! Just to give DHCP time to boot up
 event timer watchdog time 60
 action 1.0 cli command "enable"
 action 2.0 cli command "config terminal"
! Enroll spoke's certificate
 action 3.0 cli command "crypto pki enroll client1"
! After enrollement request is sent, remove that EEM script
 action 4.0 cli command "no event manager applet import-cert"
 action 5.0 cli command "exit"
event manager applet write-mem
 event syslog pattern "PKI-6-CERTRET"
 action 1.0 cli command "enable"
 action 2.0 cli command "write memory"
 action 3.0 syslog msg "Automatically saved configuration"
```

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

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

Если туннели восстановили работоспособность, можно проверить на Луче:

```
client1#show crypto session
Crypto session current status

Interface: Tunnel1
Profile: default
Session status: UP-ACTIVE
Peer: 172.16.0.2 port 500
 Session ID: 1
 IKEv2 SA: local 172.16.0.1/500 remote 172.16.0.2/500 Active
 IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
       Active SAs: 2, origin: crypto map
```

Если сертификат был зарегистрирован правильно, можно также проверить на Луче:

```
client1#show crypto pki certificates
Certificate
 Status: Available
 Certificate Serial Number (hex): 06
 Certificate Usage: General Purpose
 Issuer:
```

```
    cn=CA
  Subject:
    Name: client1
    hostname=client1
    cn=client1.cisco.com ou=cisco ou
  Validity Date:
    start date: 01:34:34 PST Apr 26 2015
    end  date: 01:34:34 PST Apr 25 2016
  Associated Trustpoints: client1
  Storage: nvram:CA#6.cer

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=CA
  Subject:
    cn=CA
  Validity Date:
    start date: 01:04:46 PST Apr 26 2015
    end  date: 01:04:46 PST Apr 25 2018
  Associated Trustpoints: client1
  Storage: nvram:CA#1CA.cer
```

Устранение неполадок

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

Известные предупреждения и проблемы

Идентификатор ошибки Cisco CSCuu93989 - Мастер Config Останавливается, поток PnP на платформах G2 мог бы заставить систему не загружать конфигурацию из usbflash:/ciscortr.cfg. Вместо этого система могла бы остановиться в функции Мастера Config:

```
client1#show crypto pki certificates
Certificate
  Status: Available
  Certificate Serial Number (hex): 06
  Certificate Usage: General Purpose
  Issuer:
    cn=CA
  Subject:
    Name: client1
    hostname=client1
    cn=client1.cisco.com ou=cisco ou
  Validity Date:
    start date: 01:34:34 PST Apr 26 2015
    end  date: 01:34:34 PST Apr 25 2016
  Associated Trustpoints: client1
  Storage: nvram:CA#6.cer

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=CA
  Subject:
```

```
  cn=CA
Validity Date:
  start date: 01:04:46 PST Apr 26 2015
  end  date: 01:04:46 PST Apr 25 2018
Associated Trustpoints: client1
Storage: nvram:CA#1CA.cer
```

Гарантируйте использование версии, которая содержит исправление для этого дефекта.

ZTD через USB по сравнению с Файлами конфигурации по умолчанию

Обратите внимание на то, что функцией **Файлов конфигурации по умолчанию**, которую использует этот документ, является другая функция, чем **Нулевой Сенсорный Deployement через USB** desribed в Обзоре Развертываний ISR Серии Cisco 800.

-	**Нулевой Сенсорный Deployement через USB**	**Файлы конфигурации умолчанию**
Поддерживаемые платформы	Ограниченный только немногими 8xx маршрутизаторы. Для получения дополнительной информации см. Обзор Развертываний ISR Серии Cisco 800	Все ISR G2, 43xx и 44x
Имя файла	*.cfg	ciscortr.cfg
Сохраняет конфигурацию на локальной флэш-памяти	Да, автоматически	Нет, Встроенный Диспетчер событий (E требуется

Поскольку больше платформ поддерживается функцией **Файлов конфигурации по умолчанию**, эта технология была выбрана для решения, представленного в этой статье.

Сводка

Конфигурация по умолчанию USB (с именем файла **ciscortr.cfg** от карты флэш-памяти с интерфейсом USB) дает администраторам сети способность развернуть Удаленные VPN Маршрутизатора на конце луча офиса (но не ограниченная просто VPN) без потребности войти в устройство в удаленном местоположении.

Дополнительные сведения

- Протокол SCEP (SCEP)
- Нулевые Сенсорные Развертывания через USB
- DMVPN/FlexVPN/VPN от узла к узлу
- Cisco Systems – техническая поддержка и документация