Маршрутизатор IOS как сервер Easy VPN Использование примера конфигурации профессионала конфигурации

Содержание

Введение

Этот документ описывает, как настроить маршрутизатор Cisco IOS® как Легкую VPN (EzVPN) Сервер с помощью Cisco Configuration Professional (CP Cisco) и CLI. Функция Easy VPN Server позволяет пользователю на удаленной стороне обмениваться данными с использованием протокола защиты IPSec с любым шлюзом виртуальной частной сети (VPN) на базе Cisco IOS. Централизованно управляемые политики IPsec «пробрасываются» на клиентское устройство сервером с минимумом настроек, выполняемых конечным пользователем.

Для получения дополнительной информации о Сервере Easy VPN обращаются к разделу Сервера Easy VPN Безопасной Библиотеки Руководства Конфигурации связности, Cisco IOS Release 12.4T.

Предварительные условия

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного

обеспечения и оборудования:

- Маршрутизатор Cisco 1841 с Cisco IOS Software Release 12.4 (15T)
- Версия 2.1 CP Cisco

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.

Установите CP Cisco

Выполните эти шаги для установки CP Cisco:

1. Cisco CP V2.1 загрузки от Центра ПО Cisco (только зарегистрированные клиенты) и устанавливает его на вашем локальном компьютере.Последняя версия CP Cisco может быть найдена в веб-сайте CP Cisco.
2. Запустите CP Cisco от своего локального компьютера до **Пуска> Программы> Cisco Configuration Professional (CCP)** и выберите **Community**, который имеет маршрутизатор, который вы хотите настроить.
3. Для обнаружения устройства, вы хотите настроить, выделить маршрутизатор и нажать **Discover**.

Примечание: Для получения информации о моделях маршрутизатора Cisco и IOS Release, которые совместимы с Cisco CP v2.1, обратитесь к Совместимому разделу Cisco IOS Release.

Примечание: Для получения информации о требованиях ПК, что Cisco CP v2.1 выполнений, обратитесь к разделу Системных требований.

Конфигурация маршрутизатора для выполнения CP Cisco

Выполните эти действия настройки для выполнения CP Cisco на маршрутизаторе Cisco:

1. Соединитесь со своим маршрутизатором с помощью Telnet, SSH, или через консоль.Введите режим глобальной конфигурации с помощью этой команды:`Router(config)#`**`enable`** `Router(config)#`
2. Если HTTP и HTTPS включены и настроены для использования нестандартных номеров портов, можно пропустить этот шаг и просто использовать номер порта, уже настроенный.Включите HTTP маршрутизатора или сервер HTTPS с помощью этих Программных команд Cisco IOS:`Router(config)#` **`ip http server`** `Router(config)#` **`ip http secure-server`** `Router(config)#` **`ip http authentication local`**
3. Создайте пользователя с уровнем привилегий 15:`Router(config)#` **`username`** *`<username>`* **`privilege 15 password 0`** *`<password>`* **Примечание:** *Вместо <username> и <password> введите имя пользователя и пароль, которые следует настроить.*
4. Настройте SSH и Telnet для локального входа и уровня привилегий 15.`Router(config)#` **`line vty 0 4`** `Router(config-line)#` **`privilege level 15`** `Router(config-line)#` **`login local`** `Router(config-line)#` **`transport input telnet`** `Router(config-line)#` **`transport input telnet ssh`** `Router(config-line)#` **`exit`**
5. (Необязательно) Позвольте локальному ведению журнала поддержать регистрационную функцию мониторинга:`Router(config)#` **`logging buffered 51200 warning`**

Требования

Этот документ предполагает, что маршрутизатор Cisco полностью в рабочем состоянии и настроен, чтобы позволить CP Cisco изменять конфигурацию.

Для полной информации о том, как начать использовать CP Cisco, обратитесь к Началу работы с Cisco Configuration Professional.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Настройка

В этом разделе вам предоставляют информацию по настройке базовые параметры для маршрутизатора в сети.

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

Схема сети

В настоящем документе используется следующая схема сети:

Примечание: Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. Это адреса RFC 1918, используемые в лабораторной среде.

CP Cisco - настройка сервера Easy VPN

Выполните эти шаги для настройки маршрутизатора Cisco IOS как Сервера Easy VPN:

1. Выберите**> Security Configure> VPN>, Сервер Easy VPN> Создает Сервер Easy VPN** и нажимает **Launch Easy VPN Server Wizard** для настройки маршрутизатора Cisco IOS как Сервера Easy VPN:
2. Нажмите **Next** для перехода **Настройку сервера Easy VPN**.
3. В получающемся окне **Виртуальный интерфейс** будет настроен как часть Настройки сервера Easy VPN. Предоставьте **IP-адрес Виртуального туннельного интерфейса** и также выберите **Метод аутентификации**, используемый для аутентификации клиентов VPN. Здесь, **Предварительные общие ключи** являются используемым методом аутентификации. **Нажмите кнопку Next:**
4. Задайте **Алгоритм шифрования, алгоритм аутентификации и метод обмена ключами**, который будет использоваться этим маршрутизатором при согласовании с удаленным устройством. Набор правил IKE по умолчанию присутствует на маршрутизаторе, который может использоваться при необходимости. Если вы хотите добавить новый Набор правил IKE, нажмите Add.

5. **Укажите алгоритм шифрования, алгоритм аутентификации и метод обмена ключами, как показано на рисунке, после чего нажмите кнопку OK:**
6. **Набор правил IKE По умолчанию** используется в данном примере. В результате выберите Набор правил IKE по умолчанию и нажмите **Next**.
7. В новом окне должна быть предоставлена подробная информация **Набора преобразований**. **Набор преобразований задаются алгоритмы шифрования и аутентификации, используемые для защиты данных в VPN-туннеле**. **Нажмите Add** для предоставления этой подробной информации. Когда вы **нажмите Add** и предоставляете подробную информацию, можно добавить любое количество Наборов преобразований по мере необходимости.**Примечание: Набор преобразований CP По умолчанию** присутствует по умолчанию на маршрутизаторе, когда настроено с помощью **CP Cisco**.
8. Предоставьте подробную информацию **Набора преобразований** (**Шифрование и Алгоритм аутентификации**) и нажмите **OK**.
9. Названный **Набор преобразований CP Набора преобразований По умолчанию По умолчанию** используется в данном примере. В результате выберите Набор преобразований по умолчанию и нажмите **Next**.
10. В новом окне выберите сервер, на котором будут настроены групповые политики, который может быть или **Локальным** или **RADIUS** или и **Локальным и RADIUS**. В данном примере мы используем **Локальный сервер** для настройки групповых политик. Выберите **Local** и нажмите **Next**.
11. Выберите сервер, который будет использоваться для Проверки подлинности пользователя в этом новом окне, которое может быть или **Локальным Только** или **RADIUS** или и **Локальным Только и RADIUS**. В данном примере мы используем **Локальный сервер** для настройки Учетных данных пользователя для аутентификации. Удостоверьтесь, что флажок рядом с **Включает Проверку подлинности пользователя**, проверен. Выберите **Local Only** и нажмите **Next**.
12. **Нажмите Add**, чтобы создать новую групповую политику и добавить удаленных пользователей в этой группе.
13. В окне **Add Group Policy** предоставьте имя группы в пространстве, обеспечивают **Название Этой Группы** (**Cisco** в данном примере) наряду с **Предварительным общим ключом** и **Пулом IP** (**Стартовый IP-адрес** и **Конечный IP-адрес**) информация как показано и нажимают **OK**.**Примечание:** Можно создать новый пул IP или использовать существующий пул IP если подарок.
14. Теперь выберите новую **Групповую политику**, созданную с **Cisco** названия, и затем нажмите, флажок рядом с **Настраивают Счетчик простоя** как требуется для настройки **Счетчика простоя**. **Нажмите кнопку Next.**
15. Включите **Cisco, Туннелирующую Протокол управления** (cTCP) при необходимости. В противном случае нажмите **Next**.
16. Рассмотрите **сводку конфигурации**. **Нажмите кнопку Finish.**
17. В **Отправлять Конфигурации к Окну маршрутизатора** нажмите **Deliver** для отправки конфигурации маршрутизатору. Можно щелкнуть **по Save к файлу** для сохранения конфигурации как файла на ПК.
18. **Окно состояния Доставки Команды** показывает статус доставки команд к маршрутизатору. Это появляется как **Конфигурация, отправленная маршрутизатору**. **Нажмите кнопку OK.**
19. Вы видите недавно созданный Сервер Easy VPN. Можно отредактировать существующий сервер путем выбора **Edit Easy VPN Server**. Это завершает Настройку

сервера Easy VPN на маршрутизаторе Cisco IOS.

Конфигурация интерфейса командой строки CLI

Настройка маршрутизатора

```
Router#show run Building configuration... Current
configuration : 2069 bytes ! version 12.4 service
timestamps debug datetime msec service timestamps log
datetime msec no service password-encryption hostname
Router boot-start-marker boot-end-marker no logging
buffered enable password cisco !---AAA enabled using aaa
newmodel command. Also AAA Authentication and
Authorization are enabled---! aaa new-model ! ! aaa
authentication login ciscocp_vpn_xauth_ml_1 local aaa
authorization network ciscocp_vpn_group_ml_1 local ! !
aaa session-id common ip cef ! ! ! ! ip domain name
cisco.com ! multilink bundle-name authenticated ! ! !---
Configuration for IKE policies. !--- Enables the IKE
policy configuration (config-isakmp) !--- command mode,
where you can specify the parameters that !--- are used
during an IKE negotiation. Encryption and Policy details
are hidden as the default values are chosen. crypto
isakmp policy 1 encr 3des authentication pre-share group
2 crypto isakmp keepalive 10 ! crypto isakmp client
configuration group cisco key cisco123 pool SDM_POOL_1
crypto isakmp profile ciscocp-ike-profile-1 match
identity group cisco client authentication list
ciscocp_vpn_xauth_ml_1 isakmp authorization list
ciscocp_vpn_group_ml_1 client configuration address
respond virtual-template 1 ! ! !--- Configuration for
IPsec policies. !--- Enables the crypto transform
configuration mode, !--- where you can specify the
transform sets that are used !--- during an IPsec
negotiation. crypto ipsec transform-set ESP-3DES-SHA
esp-3des esp-sha-hmac ! crypto ipsec profile
CiscoCP_Profile1 set security-association idle-time
86400 set transform-set ESP-3DES-SHA set isakmp-profile
ciscocp-ike-profile-1 ! ! ! !--- RSA certificate
generated after you enable the !--- ip http secure-
server command. crypto pki trustpoint TP-self-signed-
1742995674 enrollment selfsigned subject-name cn=IOS-
Self-Signed-Certificate-1742995674 revocation-check none
rsakeypair TP-self-signed-1742995674 !--- Create a user
account named cisco123 with all privileges. username
cisco123 privilege 15 password 0 cisco123 archive log
config hidekeys ! ! !--- Interface configurations are
done as shown below---! interface Loopback0 ip address
10.10.10.10 255.255.255.0 ! interface FastEthernet0/0 ip
address 10.77.241.111 255.255.255.192 duplex auto speed
auto ! interface Virtual-Template1 type tunnel ip
unnumbered Loopback0 tunnel mode ipsec ipv4 tunnel
protection ipsec profile CiscoCP_Profile1 ! !--- VPN
pool named SDM_POOL_1 has been defined in the below
command---! ip local pool SDM_POOL_1 192.168.1.1
192.168.1.254 !--- This is where the commands to enable
HTTP and HTTPS are configured. ip http server ip http
authentication local ip http secure-server ! ! ! !
control-plane ! line con 0 line aux 0 !--- Telnet
enabled with password as cisco. line vty 0 4 password
cisco transport input all scheduler allocate 20000 1000
! ! ! ! end
```

Проверка

Сервер Easy VPN - команды показа

Этот раздел позволяет убедиться, что конфигурация работает правильно.

- **show crypto isakmp sa — отображает все текущие ассоциации безопасности (SA) IKE узла.**
```
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.77.241.111   172.16.1.1      QM_IDLE           1003    0 ACTIVE
```
- **show crypto ipsec sa — отображает все текущие ассоциации безопасности (SA) IPsec узла.**
```
Router#show crypto ipsec sa
interface: Virtual-Access2
Crypto map tag: Virtual-Access2-head-0, local addr 10.77.241.111
protected vrf: (none)
local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.1.3/255.255.255.255/0/0)
current_peer 172.16.1.1 port 1086
PERMIT, flags={origin_is_acl,}
#pkts encaps: 28, #pkts encrypt: 28, #pkts digest: 28
#pkts decaps: 36, #pkts decrypt: 36, #pkts verify: 36
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 2
local crypto endpt.: 10.77.241.111, remote crypto endpt.: 172.16.1.1
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x186C05EF(409732591)
inbound esp sas:
spi: 0x42FC8173(1123844467)
transform: esp-3des esp-sha-hmac
```

Устранение неполадок

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. Посредством OIT можно анализировать выходные данные команд show.

Примечание: Обратитесь к документу Важная информация о командах отладки, прежде чем использовать команды debug.

Дополнительные сведения

- Согласование IPsec/Протоколы IKE
- Краткое руководство по началу работы Cisco Configuration Professional
- Страница поддержки продуктов Cisco - маршрутизаторы
- Cisco Systems – техническая поддержка и документация