Настройка туннеля IPsec - от маршрутизатора Cisco к брандмауэру Checkpoint Firewall 4.1

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Условные обозначения
Настройка
Схема сети
Конфигурации
Проверка
Устранение неполадок
Команды для устранения неполадок
Суммирование сетей
Контрольная точка
Пример результата отладки
Дополнительные сведения

Введение

Этот документ демонстрирует, как сформировать туннель IPSec с предварительными ключами для соединения 2-х частных сетей: частной сети 192.168.1.x в маршрутизаторе Cisco и частной сети 10.32.50.x за межсетевым экраном Checkpoint.

Предварительные условия

Требования

Этот пример конфигурации предполагает, что трафик из маршрутизатора и в Контрольной точке к Интернету (представленный здесь 172.18.124.x сети) потоки перед началом конфигурации.

Используемые компоненты

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

- Маршрутизатор Cisco 3600

- Программное обеспечение Cisco IOS (C3640-JO3S56I-M), релиз 12.1 (5) T, РЕЛИЗ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (fc1)
- Межсетевой экран Checkpoint 4.1

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

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Настройка

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

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

Схема сети

В настоящем документе используется следующая схема сети:

Конфигурации

Эти конфигурации используются в данном документе.

- Настройка маршрутизатора
- Конфигурация межсетевого экрана Checkpoint

Настройка маршрутизатора

Конфигурация маршрутизатора Cisco 3600
Current configuration : 1608 bytes ! version 12.1 no service single-slot-reload-enable service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname cisco_endpoint ! logging rate-limit console 10 except errors ! ip subnet-zero ! no ip finger ! ip audit notify log ip audit po max-events 100

```
!
!--- Internet Key Exchange (IKE) configuration crypto
isakmp policy 1 authentication pre-share crypto isakmp
key ciscorules address 172.18.124.157 ! !--- IPsec
configuration crypto ipsec transform-set rtpset esp-des
esp-sha-hmac ! crypto map rtp 1 ipsec-isakmp set peer
172.18.124.157 set transform-set rtpset match address
115 ! call rsvp-sync cns event-service server !
controller T1 1/0 ! controller T1 1/1 ! interface
Ethernet0/0 ip address 172.18.124.35 255.255.255.240 ip
nat outside no ip mroute-cache half-duplex crypto map
rtp ! interface Ethernet0/1 ip address 192.168.1.1
255.255.255.0 ip nat inside half-duplex ! interface
FastEthernet1/0 no ip address shutdown duplex auto speed
auto ! ip kerberos source-interface any ip nat pool
INTERNET 172.18.124.36 172.18.124.36 netmask
255.255.255.240 ip nat inside source route-map nonat
pool INTERNET ip classless ip route 0.0.0.0 0.0.0.0
172.18.124.34 no ip http server ! access-list 101 deny
ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255 access-
list 101 permit ip 192.168.1.0 0.0.0.255 any access-list
115 permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255
access-list 115 deny ip 192.168.1.0 0.0.0.255 any route-
map nonat permit 10 match ip address 101 ! dial-peer cor
custom ! line con 0 transport input none line aux 0 line
vty 0 4 login ! end
```

Конфигурация межсетевого экрана Checkpoint

Выполните эти шаги для настройки Межсетевого экрана Checkpoint.

1. Так как IKE и Времена жизни IPsec по умолчанию отличаются между поставщиками, выбирают **Properties> Encryption**, чтобы заставить Времена жизни контрольной точки соглашаться с Cisco по умолчанию.Срок действия IKE Cisco по умолчанию составляет 86400 секунд (= 1440 минут), и он может модифицироваться этими командами:**crypto isakmp policy #срок действия #**Конфигурируемый Срок действия IKE Cisco с 60-86400 секунд. Срок действия IPSec Cisco по умолчанию составляет 3600 секунд, и он может модифицироваться **секундами crypto ipsec security-association lifetime #** команда.Настраиваемый срок действия Cisco IPSec с 120-86400 секунд.
2. Выберите**> new (or edit)> network Manage> Network objects** для настройки объекта для внутренней сети (названный "cpinside") позади Контрольной точки.Это должно согласиться с сетью назначения (дополнительная) в **команде access-list 115 permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255** Cisco.Выберите **Internal** под местоположением.
3. Выберите **Manage> Network objects> Edit** для редактирования объекта для Контрольной точки RTPCPVPN (шлюз) оконечная точка, к которой указывает маршрутизатор Cisco в **команде set peer 172.18.124.157**.Выберите **Internal** под Местоположением. **В поле Type (Тип) выберите Gateway (Шлюз)**. Под Установленными Модулями установите флажок **VPN-1 & FireWall 1**, и также выберите **Флажок Management Station**:
4. Выберите **Manage> Network objects> New> Network** для настройки объекта для внешней сети (названный "inside_cisco") позади маршрутизатора Cisco.Это должно согласовать с источником (первую) сеть в **команде access-list 115 permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255** Cisco.Выберите **External** под местоположением.
5. Выберите **Manage> Network objects> New> Workstation** для добавления объекта для

внешнего шлюза маршрутизатора Cisco (названный "cisco_endpoint"). Это - Интерфейс Cisco, к которому применена команда *имени криптокарты*.Выберите **External** под местоположением. **В поле Type (Тип) выберите Gateway (Шлюз).Примечание:** Не выбирать флажок "VPN-1/FireWall-1".

6. **Для изменения параметров на вкладке VPN оконечного устройства шлюза Checkpoint (именуемого RTPCPVPN) выберите Manage > Network objects > Edit (Управление > Сетевые объекты > Изменить). На вкладке Domain (Домен) выберите Other (Другой) и затем адрес внутри сети Checkpoint (cpinside) в раскрывающемся списке. В разделе Encryption schemes defined (Определенные схемы шифрования) выберите IKE и нажмите кнопку Edit (Редактировать).**
7. Измените Свойства ike для Шифрования по алгоритму DES (стандарт шифрования данных) для согласия с этими командами:**crypto isakmp policy #шифрование desПримечание:** Шифрование по алгоритму DES (стандарт шифрования данных) является по умолчанию, таким образом, это не видимо в Конфигурации CISCO.
8. Измените Свойства ike на хеширование SHA1 для согласия с этими командами:**crypto isakmp policy #хэш shaПримечание:** Алгоритм хеширования SHA является по умолчанию, таким образом, это не видимо в Конфигурации CISCO.Измените следующие настройки:**Отмените Aggressive Mode (Агрессивный режим).Отметьте флажок Supports Subnets (Поддерживает подсети).В разделе Authentication Method (Метод аутентификации) отметьте флажок Pre-Shared Secret (Предварительно согласованный секретный ключ).** Это соглашается с этими командами:**crypto isakmp policy #authentication pre-share**
9. Нажмите **Edit Secrets**, чтобы заставить предварительный общий ключ соглашаться с командой *адреса основного адреса* **crypto isakmp key** Cisco:
10. **Для редактирования вкладки VPN cisco_endpoint Manage > Network objects > Edit (Управление > Сетевые объекты > Изменить). В разделе Domain (Домен) выберите Other (Другой) и затем укажите внутреннее пространство сети Cisco (inside_cisco). В разделе Encryption schemes defined (Определенные схемы шифрования) выберите IKE и нажмите кнопку Edit (Редактировать).**
11. Измените Шифрование по алгоритму DES (стандарт шифрования данных) Свойств ike для согласия с этими командами:**crypto isakmp policy #шифрование desПримечание:** Шифрование по алгоритму DES (стандарт шифрования данных) является по умолчанию, таким образом, это не видимо в Конфигурации CISCO.
12. Измените Свойства ike на хеширование SHA1 для согласия с этими командами:**crypto isakmp policy #хэш shaПримечание:** Алгоритм хеширования SHA является по умолчанию, таким образом, это не видимо в Конфигурации CISCO.Измените следующие настройки:**Отмените Aggressive Mode (Агрессивный режим).Отметьте флажок Supports Subnets (Поддерживает подсети).В разделе Authentication Method (Метод аутентификации) отметьте флажок Pre-Shared Secret (Предварительно согласованный секретный ключ).** Это соглашается с этими командами:**crypto isakmp policy #authentication pre-share**
13. Нажмите **Edit Secrets**, чтобы заставить предварительный общий ключ соглашаться с командой Cisco *адреса основного адреса* **crypto isakmp key**.
14. В окне Policy Editor (Редактор политик) вставьте правило, в качестве источника и назначения для которого используется inside_cisco и cpinside (двустороннее соединение). **Задайте параметры: Service=Any, Action=Encrypt и Track=Long.**
15. Нажмите **зеленый значок шифрования** и выберите **Edit properties** для настройки политики шифрования под заголовком Действия.

16. **Выберите IKE, затем выберите Edit (Редактировать).**
17. На окне IKE Properties изменитесь, эти свойства для согласия с Cisco IPSec преобразовывает в команду **crypto ipsec transform-set rtpset esp-des esp-sha-hmac:В разделе Transform (Преобразование) выберите Encryption + Data Integrity (ESP) (Шифрование + контроль целостности данных [инкапсулирующая защита содержимого]).** Алгоритм шифрования должен быть **DES**, Целостность данных должна быть **SHA1**, и Позволенный Шлюз одноранговой сети должен быть шлюзом внешнего маршрутизатора (названный "cisco_endpoint"). **Нажмите кнопку OK.**
18. **После настройки контрольной точки выберите в меню Checkpoint пункты Policy > Install (Политика > Установить), чтобы изменения вступили в силу.**

Проверка

В этом разделе содержатся сведения, которые помогают убедиться в надлежащей работе конфигурации.

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

- **"show crypto isakmp sa" - просмотр всех текущих сопоставлений безопасности IKE (SA IKE) на одноранговом узле.**
- **show crypto ipsec sa — просмотр параметров, используемых текущими SA.**

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды для устранения неполадок

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

- **debug crypto engine** сообщения отладки о ядрах шифрования, которые выполняют шифрование и расшифровку.
- **debug crypto isakmp – отображает сообщения о событиях IKE.**
- **debug crypto ipsec– показывает события IPSec.**
- **clear crypto isakmp** все соединения активного предложения IKE.
- **clear crypto sa** все контексты безопасности IPSec.

Суммирование сетей

При настройке нескольких смежных внутренних сетей в домене шифрования на устройстве Checkpoint последнее может автоматически суммировать сети с точки зрения трафика, представляющего интерес. Если маршрутизатор не будет настроен для соответствия, то туннель, вероятно, откажет. Например, если внутренние сети 10.0.0.0/24 и 10.0.1.0/24 настроены на включение в туннель, они могут быть суммированы как 10.0.0.0/23.

Контрольная точка

Поскольку в окне Policy Editor (Редактор политик) для отслеживания задан параметр Long (Длительно), в окне Log Viewer (Просмотр журнала) отклоненный трафик должен отображаться красным цветом. Для получения более подробных отладочных данных выполните команды:

```
C:\WINNT\FW1\4.1\fwstop
C:\WINNT\FW1\4.1\fw d -d
```

и в другом окне:

```
C:\WINNT\FW1\4.1\fwstart
```

Примечание: Это было установкой Microsoft Windows NT.

Для сброса ассоциаций безопасности на устройстве Checkpoint выполните следующие команды:

```
fw tab -t IKE_SA_table -x
fw tab -t ISAKMP_ESP_table -x
fw tab -t inbound_SPI -x
fw tab -t ISAKMP_AH_table -x
```

На вопрос Are you sure? (Вы уверены?) ответьте yes (да).

Пример результата отладки

```
Configuration register is 0x2102

cisco_endpoint#debug crypto isakmp Crypto ISAKMP debugging is on cisco_endpoint#debug crypto
isakmp Crypto IPSEC debugging is on cisco_endpoint#debug crypto engine Crypto Engine debugging
is on cisco_endpoint# 20:54:06: IPSEC(sa_request): , (key eng. msg.) src= 172.18.124.35, dest=
172.18.124.157, src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4), dest_proxy=
10.32.50.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-sha-hmac , lifedur=
3600s and 4608000kb, spi= 0xA29984CA(2727969994), conn_id= 0, keysize= 0, flags= 0x4004
20:54:06: ISAKMP: received ke message (1/1) 20:54:06: ISAKMP: local port 500, remote port 500
20:54:06: ISAKMP (0:1): beginning Main Mode exchange 20:54:06: ISAKMP (0:1): sending packet to
172.18.124.157 (I) MM_NO_STATE 20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I)
MM_NO_STATE 20:54:06: ISAKMP (0:1): processing SA payload. message ID = 0 20:54:06: ISAKMP
(0:1): found peer pre-shared key matching 172.18.124.157 20:54:06: ISAKMP (0:1): Checking ISAKMP
transform 1 against priority 1 policy 20:54:06: ISAKMP: encryption DES-CBC 20:54:06: ISAKMP:
hash SHA 20:54:06: ISAKMP: default group 1 20:54:06: ISAKMP: auth pre-share 20:54:06: ISAKMP
(0:1): atts are acceptable. Next payload is 0 20:54:06: CryptoEngine0: generate alg parameter
20:54:06: CRYPTO_ENGINE: Dh phase 1 status: 0 20:54:06: CRYPTO_ENGINE: Dh phase 1 status: 0
20:54:06: ISAKMP (0:1): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_SA_SETUP 20:54:06: ISAKMP (0:1):
received packet from 172.18.124.157 (I) MM_SA_SETUP 20:54:06: ISAKMP (0:1): processing KE
payload. message ID = 0 20:54:06: CryptoEngine0: generate alg parameter 20:54:06: ISAKMP (0:1):
processing NONCE payload. message ID = 0 20:54:06: ISAKMP (0:1): found peer pre-shared key
matching 172.18.124.157 20:54:06: CryptoEngine0: create ISAKMP SKEYID for conn id 1 20:54:06:
ISAKMP (0:1): SKEYID state generated 20:54:06: ISAKMP (1): ID payload next-payload : 8 type : 1
protocol : 17 port : 500 length : 8 20:54:06: ISAKMP (1): Total payload length: 12 20:54:06:
CryptoEngine0: generate hmac context for conn id 1 20:54:06: ISAKMP (0:1): sending packet to
172.18.124.157 (I) MM_KEY_EXCH 20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I)
MM_KEY_EXCH 20:54:06: ISAKMP (0:1): processing ID payload. message ID = 0 20:54:06: ISAKMP
(0:1): processing HASH payload. message ID = 0 20:54:06: CryptoEngine0: generate hmac context
for conn id 1 20:54:06: ISAKMP (0:1): SA has been authenticated with 172.18.124.157 20:54:06:
ISAKMP (0:1): beginning Quick Mode exchange, M-ID of 1855173267 20:54:06: CryptoEngine0:
generate hmac context for conn id 1 20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I)
QM_IDLE 20:54:06: CryptoEngine0: clear dh number for conn id 1 20:54:06: ISAKMP (0:1): received
packet from 172.18.124.157 (I) QM_IDLE 20:54:06: CryptoEngine0: generate hmac context for conn
```

```
id 1 20:54:06: ISAKMP (0:1): processing HASH payload. message ID = 1855173267 20:54:06: ISAKMP
(0:1): processing SA payload. message ID = 1855173267 20:54:06: ISAKMP (0:1): Checking IPSec
proposal 1 20:54:06: ISAKMP: transform 1, ESP_DES 20:54:06: ISAKMP: attributes in transform:
20:54:06: ISAKMP: encaps is 1 20:54:06: ISAKMP: SA life type in seconds 20:54:06: ISAKMP: SA
life duration (basic) of 3600 20:54:06: ISAKMP: SA life type in kilobytes 20:54:06: ISAKMP: SA
life duration (VPI) of 0x0 0x46 0x50 0x0 20:54:06: ISAKMP: authenticator is HMAC-SHA 20:54:06:
validate proposal 0 20:54:06: ISAKMP (0:1): atts are acceptable. 20:54:06:
IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) dest= 172.18.124.157, src=
172.18.124.35, dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4), src_proxy=
192.168.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-sha-hmac ,
lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 20:54:06: validate proposal
request 0 20:54:06: ISAKMP (0:1): processing NONCE payload. message ID = 1855173267 20:54:06:
ISAKMP (0:1): processing ID payload. message ID = 1855173267 20:54:06: ISAKMP (0:1): processing
ID payload. message ID = 1855173267 20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ipsec allocate flow 0 20:54:06: ipsec allocate flow 0 20:54:06: ISAKMP (0:1): Creating
IPSec SAs 20:54:06: inbound SA from 172.18.124.157 to 172.18.124.35 (proxy 10.32.50.0 to
192.168.1.0) 20:54:06: has spi 0xA29984CA and conn_id 2000 and flags 4 20:54:06: lifetime of
3600 seconds 20:54:06: lifetime of 4608000 kilobytes 20:54:06: outbound SA from 172.18.124.35 to
172.18.124.157 (proxy 192.168.1.0 to 10.32.50.0) 20:54:06: has spi 404516441 and conn_id 2001
and flags 4 20:54:06: lifetime of 3600 seconds 20:54:06: lifetime of 4608000 kilobytes 20:54:06:
ISAKMP (0:1): sending packet to 172.18.124.157 (I) QM_IDLE 20:54:06: ISAKMP (0:1): deleting node
1855173267 error FALSE reason "" 20:54:06: IPSEC(key_engine): got a queue event... 20:54:06:
IPSEC(initialize_sas): , (key eng. msg.) dest= 172.18.124.35, src= 172.18.124.157, dest_proxy=
192.168.1.0/255.255.255.0/0/0 (type=4), src_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 3600s and 4608000kb, spi=
0xA29984CA(2727969994), conn_id= 2000, keysize= 0, flags= 0x4 20:54:06: IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.18.124.35, dest= 172.18.124.157, src_proxy=
192.168.1.0/255.255.255.0/0/0 (type=4), dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 3600s and 4608000kb, spi=
0x181C6E59(404516441), conn_id= 2001, keysize= 0, flags= 0x4 20:54:06: IPSEC(create_sa): sa
created, (sa) sa_dest= 172.18.124.35, sa_prot= 50, sa_spi= 0xA29984CA(2727969994), sa_trans=
esp-des esp-sha-hmac , sa_conn_id= 2000 20:54:06: IPSEC(create_sa): sa created, (sa) sa_dest=
172.18.124.157, sa_prot= 50, sa_spi= 0x181C6E59(404516441), sa_trans= esp-des esp-sha-hmac ,
sa_conn_id= 2001 cisco_endpoint#sho cry ips sa interface: Ethernet0/0 Crypto map tag: rtp, local
addr. 172.18.124.35 local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0) remote
ident (addr/mask/prot/port): (10.32.50.0/255.255.255.0/0/0) current_peer: 172.18.124.157 PERMIT,
flags={origin_is_acl,} #pkts encaps: 14, #pkts encrypt: 14, #pkts digest 14 #pkts decaps: 14,
#pkts decrypt: 14, #pkts verify 14 #pkts compressed: 0, #pkts decompressed: 0 #pkts not
compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0, #send errors 1, #recv errors
0 local crypto endpt.: 172.18.124.35, remote crypto endpt.: 172.18.124.157 path mtu 1500, media
mtu 1500 current outbound spi: 181C6E59 inbound esp sas: spi: 0xA29984CA(2727969994) transform:
esp-des esp-sha-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2000, flow_id: 1, crypto
map: rtp --More-- sa timing: remaining key lifetime (k/sec): (4607998/3447) IV size: 8 bytes
replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi:
0x181C6E59(404516441) transform: esp-des esp-sha-hmac , in use settings ={Tunnel, } slot: 0,
conn id: 2001, flow_id: 2, crypto map: rtp sa timing: remaining key lifetime (k/sec):
(4607997/3447) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas:
cisco_endpoint#show crypto isakmp sa dst src state conn-id slot 172.18.124.157 172.18.124.35
QM_IDLE 1 0 cisco_endpoint#exit
```

Дополнительные сведения

- Согласование IPsec/Протоколы IKE
- Настройка параметров сетевой безопасности IPSec Network Security
- Настройка протокола защищенного обмена ключами IKE
- Cisco Systems – техническая поддержка и документация