Настройка туннеля IPSec – концентратор Cisco VPN 5000 к межсетевому экрану Checkpoint 4.1

Содержание

[Введение](#)
[Предварительные условия](#)
[Требования](#)
[Используемые компоненты](#)
[Условные обозначения](#)
[Настройка](#)
[Схема сети](#)
[Конфигурации](#)
[Межсетевой экран Checkpoint 4.1](#)
[Проверка](#)
[Устранение неполадок](#)
[Команды для устранения неполадок концентратора VPN 5000](#)
[Суммирование сетей](#)
[Отладка межсетевого экрана Checkpoint 4.1](#)
[Пример результата отладки](#)
[Дополнительные сведения](#)

Введение

Этот документ демонстрирует, как сформировать туннель IPSec с предварительными ключами для соединения 2-х частных сетей. Это присоединяется к частной сети в Концентраторе Cisco VPN 5000 (192.168.1.x) к частной сети в Контрольной точке 4.1 Межсетевых экрана (10.32.50. x. Предполагается, что трафик из Концентратора VPN и в Контрольной точке к Интернету (представленный в этом документе 172.18.124.x сети) потоки перед началом этой конфигурации.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Концентратор Cisco VPN 5000
- Версия программного обеспечения концентратора 5.2.19.0001 Cisco VPN 5000
- 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

В данном документе используется следующая конфигурация.

Концентратор Cisco VPN 5000

```
[ IP Ethernet 0:0 ]
Mode                    = Routed
SubnetMask              = 255.255.255.0
IPAddress               = 192.168.1.1

[ General ]
EthernetAddress         = 00:00:a5:e9:c8:00
DeviceType              = VPN 5002/8 Concentrator
ConfiguredOn            = Timeserver not configured
ConfiguredFrom          = Command Line, from Console
DeviceName              = "cisco_endpoint"
IPSecGateway            = 172.18.124.34

[ IKE Policy ]
Protection              = SHA_DES_G2

[ Tunnel Partner VPN 1 ]
KeyLifeSecs             = 28800
LocalAccess             = "192.168.1.0/24"
Peer                    = "10.32.50.0/24"
BindTo                  = "ethernet 1:0"
```

```
SharedKey                = "ciscorules"
KeyManage                = Auto
Transform                = esp(sha,des)
Partner                  = 172.18.124.157
Mode                     = Main

[ IP VPN 1 ]
Numbered                 = Off
Mode                     = Routed

[ IP Ethernet 1:0 ]
IPAddress                = 172.18.124.35
SubnetMask               = 255.255.255.240
Mode                     = Routed

[ IP Static ]
10.32.50.0 255.255.255.0 VPN 1 1

Configuration size is 1131 out of 65500 bytes.
```

Межсетевой экран Checkpoint 4.1

Для настройки межсетевого экрана Checkpoint 4.1 выполните следующие шаги.

1. Выберите **Properties> Encryption**, чтобы заставить Сроки действия IPSec Контрольной точки соглашаться с **KeyLifeSecs = 28800** команд VPN Concentrator.**Примечание:** Оставьте сроки службы Протокола IKE Контрольной точки в по умолчанию.
2. **Для настройки объекта внутренней (cpinside) сети за устройством Checkpoint выберите Manage > Network objects > New (или Edit) > Network (Управление > Объекты сетей > Создать (Изменить) > Сеть).** Это должно согласиться с **Узлом = "10.32.50.0/24"** команда VPN Concentrator.
3. Выберите **Manage> Network objects> Edit** для редактирования объекта для шлюза (Контрольная точка "RTPCPVPN") оконечная точка, к которой указывает Концентратор VPN в **команде Partner = <ip>**.Выберите **Internal** под местоположением.**Выбранный шлюз** для типа.Проверьте **VPN-1 и межсетевой экран 1** и **станция управления** под установленными модулями.
4. **Для настройки объекта внешней (inside_cisco) сети за концентратором VPN выберите Manage > Network objects > New (или Edit) > Network (Управление > Объекты сетей > Создать (Изменить) > Сеть).**Это должно согласиться с **LocalAccess = <192.168.1.0/24>** команда VPN Concentrator.
5. **Чтобы добавить объект для внешнего шлюза концентратора VPN (cisco_endpoint) выберите Manage > Network objects > New > Workstation (Управление > Сетевые объекты > Создать > Рабочая станция).**Это - "внешний" интерфейс Концентратора VPN с подключением к Контрольной точке (в этом документе, 172.18.124.35 IP-адрес в **команде IPAddress = <ip>**).Выберите **External** под местоположением. **Выбранный шлюз** для типа.**Примечание:** Не проверяйте 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 на **Шифрование по алгоритму DES (стандарт шифрования данных)** и хеширование **SHA1** для согласия с командой **SHA_DES_G2 VPN Concentrator.Примечание:** "G2" обращается к Группе Диффи-Хеллмана 1 или 2. В тестировании это было обнаружено, что Контрольная точка принимает или "G2" или "G1".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).**
8. Нажмите **Edit Secrets**, чтобы заставить предварительный общий ключ соглашаться с **общим ключом = <ключевая>** команда VPN Concentrator.
9. **Для редактирования вкладки VPN cisco_endpoint Manage > Network objects > Edit (Управление > Сетевые объекты > Изменить).** Под Доменом выберите **Other**, и затем выберите внутреннюю часть сети VPN Concentrator (названный "inside_cisco"). **В разделе Encryption schemes defined (Определенные схемы шифрования) выберите IKE и нажмите кнопку Edit (Редактировать).**
10. Измените Свойства ike на **Шифрование по алгоритму DES (стандарт шифрования данных)** и хеширование **SHA1** для согласия с командой **SHA_DES_G2 VPN Concentrator.Примечание:** "G2" обращается к Группе Диффи-Хеллмана 1 или 2. В тестировании было найдено, что Контрольная точка принимает или "G2" или "G1".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).**
11. Нажмите **Edit Secrets**, чтобы заставить предварительный общий ключ соглашаться с **общим ключом = <ключевая>** команда VPN Concentrator.
12. 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.**
13. **Затем под заголовком Action (Действие) щелкните зеленый значок Encrypt (Шифровать) и выберите пункт Edit properties (Изменить свойства), чтобы настроить политики шифрования.**
14. Выберите **IKE** и нажмите **Edit**.
15. На окне IKE Properties измените эти свойства для согласия с **Преобразованием = особенно (sha, des)** команда VPN Concentrator.**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 внешним шлюзом Концентратора VPN (названный "cisco_endpoint"). **Нажмите кнопку OK.**
16. **После настройки контрольной точки выберите в меню Checkpoint пункты Policy > Install (Политика > Установить), чтобы изменения вступили в силу.**

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Команды для устранения неполадок концентратора VPN 5000

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

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

- **команда vpn trace dump all – отображает сведения о всех соответствующих подключениях VPN, включая сведения о времени, числе VPN, фактический IP-адрес однорангового узла, какие сценарии запущены, а в случае ошибки – в какой подпрограмме и номере строки произошла ошибка.**
- **show system log buffer** — Показывает содержание внутреннего буфера журнала.
- **show vpn statistics** — Показывает эти сведения для пользователей, партнеров и общее количество для обоих. (Для модульных моделей показ включает раздел для каждого модульного слота. См. раздел Примера отладочных выходных данных.) `– .In Negot – .High Water - . – .Tunnel OK – , .Tunnel Starts – .Tunnel Error – .`
- **show vpn statistics verbose: отображает статистику согласования ISAKMP и прочие статистические данные для активных соединений.**

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 концентратор VPN не настроен соответственно, то туннель с большой вероятностью функционировать не будет. 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.

Отладка межсетевого экрана Checkpoint 4.1

Это было установкой Microsoft Windows NT. Поскольку отслеживание было установлено для `Long` в Окне редактора политики (как замечено в Шаге 12), отказ в трафике должен появиться в красном в Log Viewer. Больше многословной отладки может быть получено:

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

и в другом окне:

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

Выполните эти команды для очистки Сопоставлений безопасности (SA) на контрольной точке:

```
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

```
cisco_endpoint#vpn trac dump all 4 seconds -- stepmngr trace enabled -- new script: lan-lan
primary initiator for <no id> (start) manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157]
(start) 38 seconds doing l2lp_init, (0 @ 0) 38 seconds doing l2lp_do_negotiation, (0 @ 0) new
script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157] (start) 38 seconds doing
isa_i_main_init, (0 @ 0) manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done) manage @
38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start) 38 seconds doing isa_i_main_process_pkt_2,
(0 @ 0) manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done) manage @ 38 seconds ::
lan-lan-VPN0:1:[172.18.124.157] (start) 38 seconds doing isa_i_main_process_pkt_4, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done) manage @ 39 seconds :: lan-lan-
VPN0:1:[172.18.124.157] (start) 39 seconds doing isa_i_main_process_pkt_6, (0 @ 0) 39 seconds
doing isa_i_main_last_op, (0 @ 0) end script: ISAKMP secondary Main for lan-lan-
VPN0:1:[172.18.124.157], (0 @ 0) next script: lan-lan primary initiator for lan-lan-
VPN0:1:[172.18.124.157], (0 @ 0) 39 seconds doing l2lp_phase_1_done, (0 @ 0) 39 seconds doing
l2lp_start_phase_2, (0 @ 0) new script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157]
(start) 39 seconds doing iph2_init, (0 @ 0) 39 seconds doing iph2_build_pkt_1, (0 @ 0) 39
seconds doing iph2_send_pkt_1, (0 @ 0) manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157]
(done) manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start) 39 seconds doing
iph2_pkt_2_wait, (0 @ 0) 39 seconds doing ihp2_process_pkt_2, (0 @ 0) 39 seconds doing
iph2_build_pkt_3, (0 @ 0) 39 seconds doing iph2_config_SAs, (0 @ 0) 39 seconds doing
iph2_send_pkt_3, (0 @ 0) 39 seconds doing iph2_last_op, (0 @ 0) end script: phase 2 initiator
for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0) next script: lan-lan primary initiator for lan-lan-
VPN0:1:[172.18.124.157], (0 @ 0) 39 seconds doing l2lp_open_tunnel, (0 @ 0) 39 seconds doing
l2lp_start_i_maint, (0 @ 0) new script: initiator maintenance for lan-lan-
VPN0:1:[172.18.124.157] (start) 39 seconds doing imnt_init, (0 @ 0) manage @ 39 seconds :: lan-
lan-VPN0:1:[172.18.124.157] (done) cisco_endpoint#show vpn stat Current In High Running Tunnel
Tunnel Tunnel Active Negot Water Total Starts OK Error ----------------------------------------
---------- Users 0 0 0 0 0 0 0 Partners 1 0 1 1 1 0 0 Total 1 0 1 1 1 0 0 IOP slot 1:
Current In High Running Tunnel Tunnel Tunnel Active Negot Water Total Starts OK Error ----------
-------------------------------------------------- Users 0 0 0 0 0 0 0 Partners 0 0 0 0 0 0 0
Total 0 0 0 0 0 0 0 cisco_endpoint#show vpn stat verb Current In High Running Tunnel Tunnel
Tunnel Active Negot Water Total Starts OK Error ----------------------------------------------
-------------- Users 0 0 0 0 0 0 0 Partners 1 0 1 1 1 0 0 Total 1 0 1 1 1 0 0 Stats VPN0:1
Wrapped 13 Unwrapped 9 BadEncap 0 BadAuth 0 BadEncrypt 0 rx IP 9 rx IPX 0 rx Other 0 tx IP 13 tx
IPX 0 tx Other 0 IKE rekey 0 Input VPN pkts dropped due to no SA: 0 Input VPN pkts dropped due
to no free queue entries: 0 ISAKMP Negotiation stats Admin packets in 4 Fastswitch packets in 0
No cookie found 0 Can't insert cookie 0 Inserted cookie(L) 1 Inserted cookie(R) 0 Cookie not
inserted(L) 0 Cookie not inserted(R) 0 Cookie conn changed 0 Cookie already inserted 0 Deleted
cookie(L) 0 Deleted cookie(R) 0 Cookie not deleted(L) 0 Cookie not deleted(R) 0 Forwarded to RP
0 Forwarded to IOP 0 Bad UDP checksum 0 Not fastswitched 0 Bad Initiator cookie 0 Bad Responder
cookie 0 Has Responder cookie 0 No Responder cookie 0 No SA 0 Bad find conn 0 Admin queue full 0
Priority queue full 0 Bad IKE packet 0 No memory 0 Bad Admin Put 0 IKE pkt dropped 0 No UDP PBuf
0 No Manager 0 Mgr w/ no cookie 0 Cookie Scavenge Add 1 Cookie Scavenge Rem 0 Cookie Scavenged 0
Cookie has mgr err 0 New conn limited 0 IOP slot 1: Current In High Running Tunnel Tunnel Tunnel
Active Negot Water Total Starts OK Error ------------------------------------------------------
------- Users 0 0 0 0 0 0 0 Partners 0 0 0 0 0 0 0 Total 0 0 0 0 0 0 0 Stats Wrapped Unwrapped
BadEncap BadAuth BadEncrypt rx IP rx IPX rx Other tx IP tx IPX tx Other IKE rekey Input VPN pkts
dropped due to no SA: 0 Input VPN pkts dropped due to no free queue entries: 0 ISAKMP
Negotiation stats Admin packets in 0 Fastswitch packets in 3 No cookie found 0 Can't insert
cookie 0 Inserted cookie(L) 0 Inserted cookie(R) 1 Cookie not inserted(L) 0 Cookie not
inserted(R) 0 Cookie conn changed 0 Cookie already inserted 0 Deleted cookie(L) 0 Deleted
cookie(R) 0 Cookie not deleted(L) 0 Cookie not deleted(R) 0 Forwarded to RP 0 Forwarded to IOP 3
Bad UDP checksum 0 Not fastswitched 0 Bad Initiator cookie 0 Bad Responder cookie 0 Has
Responder cookie 0 No Responder cookie 0 No SA 0 Bad find conn 0 Admin queue full 0 Priority
queue full 0 Bad IKE packet 0 No memory 0 Bad Admin Put 0 IKE pkt dropped 0 No UDP PBuf 0 No
Manager 0 Mgr w/ no cookie 0 Cookie Scavenge Add 1 Cookie Scavenge Rem 0 Cookie Scavenged 0
Cookie has mgr err 0 New conn limited 0
```

Дополнительные сведения

- Объявление об окончании продажи концентраторов Cisco серии VPN 5000
- Согласование IPsec/Протоколы IKE
- Cisco Systems – техническая поддержка и документация