Настройка IPSec через ADSL в коммутаторе Cisco 2600/3600 с модулем ADSL-WIC и модулем аппаратного шифрования

Содержание

Введение

По мере того как интернет расширяется, филиалы компании требуют, чтобы их соединения к центральным узлам были и надежны, и безопасны. Virtual Private Networks (VPN) защищает информацию между удалёнными офисами и центральными узлами по мере того, как она перемещается через интернет. IP-безопасность (IPSec) можно использовать для того, чтобы гарантировать, что данные, которые проходят через эти VPN ы. Шифрование предоставляет другой уровень сетевой безопасности.

Эти данные показывают типичный IPSEC VPN. Много удаленных доступов и соединений от узла к узлу включены между филиалами компании и центральными узлами. Обычно, обычные сеть wan ссылки, такие как Frame Relay, ISDN и коммутируемое модемное соединение настроены между узлами. Эти соединения могут включить дорогой однократный сбор за инициализацию и дорогие помесячные абонементные платы. Кроме того, для ISDN и пользователей модема, могут быть длинные времена соединения.

Ассиметричная цифровая абонентская линия (ADSL) предлагает постоянное, вариант с низкими издержками к этим обычным сеть wan ссылкам. Зашифрованные данные IPSec по соединению ADSL предлагают безопасное и надежное соединение и сохраняют деньги заказчиков. Традиционный ADSL Customer Premises Equipment (CPE), установленный в филиале компании, требует ADSL - модема, который соединяется с устройством, которое инициирует и завершает Трафик IPSec. Эти данные показывают стандартную сеть ADSL.

Cisco 2600 и 3600 маршрутизаторов поддерживают интерфейсную карту ADSL WAN (WIC-1ADSL). Этот WIC-1ADSL является мультисервисным доступом и решением для удаленного доступа, разработанным для удовлетворения потребностей филиала компании. Введение WIC-1ADSL и модулей аппаратного шифрования выполняет спрос на IPSec и DSL в филиале компании в решении для одиночного маршрутизатора. WIC-1ADSL избавляет от необходимости отдельный модем DSL. Модуль аппаратного шифрования предоставляет до десяти раз производительность по только программному шифрованию, поскольку это разгружает шифрование, которое обрабатывает от маршрутизатора.

Для получения дополнительной информации об этих двух продуктах обратитесь к Интерфейсным картам ADSL WAN для Cisco 1700, 2600, и Модульные маршрутизаторы доступа серии 3700 и Модули виртуальной частной сети для Cisco 1700, серии 2600, 3600 и 3700.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

Маршрутизаторы серии Cisco 2600/3600:

- Релиз 12.1 программного обеспечения Cisco IOS (5) набор функций 3DES Enterprise Plus септибайта
- DRAM 64 МБ для серии Cisco 2600, DRAM 96 МБ для серии Cisco 3600
- Флэш 16 МБ для серии Cisco 2600, Флэш 32 МБ для серии Cisco 3600
- WIC-1 ADSL
- Модули аппаратного шифрованияAIM-VPN/BP и AIM-VPN/EP для серии Cisco 2600NM-VPN/MP для Cisco 3620/3640AIM-VPN/HP для Cisco 3660

Серия Cisco 6400:

- Cisco IOS Software Release 12.1 (5) DC1
- DRAM 64 МБ
- Флэш 8 МБ

Серия Cisco 6160:

- Cisco IOS Software Release 12.1 (7) DA2
- DRAM 64 МБ
- Флэш 16 МБ

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. Перед выполнением любых команд в активной сети необходимо осознавать потенциальные последствия их применения.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Настройка

В этом разделе вам предоставляется информация для того, чтобы настроить функциональные возможности, описанные в этом документе.

Примечание: Дополнительные сведения о командах, использованных в данном документе, см. в разделе Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

Этот документ использует сетевую установку, показанную эту схему.

Этот тест моделирует соединение IPSEC VPN, которое использует ADSL в типичном окружении филиала.

Cisco 2600/3600 с ADSL-WIC и модулем аппаратного шифрования обучается до мультиплексора доступа к цифровой абонентской линии (DSLAM) (DSLAM) Cisco 6160. Cisco 6400 используется в качестве устройства агрегации, которое завершает сеанс PPP, который инициирует от Маршрутизатора Cisco 2600. Туннель IPSec происходит в CPE 2600 и завершается в Cisco 3600 в центральной ATC, устройстве головной станции IPSec в этом сценарии. Устройство головной станции настроено для принятия соединений от любого клиента вместо индивидуального равноправного информационного обмена. Устройство головной станции также протестировано с только предварительными общими ключами и 3DES и Edge Service Processor (ESP) - Защищенным алгоритмом хэширования (SHA) - Основанный на хэше код аутентификации сообщения (HMAC).

Конфигурации

Эти конфигурации используются в данном документе:

- Маршрутизатор Cisco 2600
- Устройство головной станции IPSec - маршрутизатор Cisco 3600
- DSLAM Cisco 6160
- Процессор маршрута узла (NRP) Cisco 6400

Обратите внимание на эти точки о конфигурациях:

- Предварительный общий ключ используется. Для устанавливания Сеансов IPSec ко множественным одноранговым телефонным соединениям необходимо определить множественные операторы определения ключа, или необходимо настроить динамическую криптокарту. Если все сеансы совместно используют одиночный ключ, необходимо использовать адрес партнера (peer) 0.0.0.0.
- Набор преобразований может быть определен для ESP, Заголовка аутентификации (AH) или обоих для двойной аутентификации.
- По крайней мере одно определение политики шифрования должно быть определено на

узел. Криптокарты решают узел для использования для создания Сеанса IPSec. Решение основывается на соответствии адреса, определенном в списке доступа. В этом случае это - access-list 101.

- Криптокарты должны быть определены для обоих физические интерфейсы (interface ATM 0/0 в этом случае) и virtual-template.
- Конфигурация, представленная в этом документе, обсуждает только Туннель IPSec по подключению DSL. Функции дополнительных мер безопасности, вероятно, необходимы, чтобы гарантировать, что ваша сеть не уязвима. Эти характеристики безопасности могут включать дополнительные списки управления доступом (ACL), Технология NAT и использование межсетевого экрана с внешним блоком или набором функций межсетевого экрана IOS. Каждая из этих функций может быть использована для ограничения трафика не-IPSec и от маршрутизатора.

Маршрутизатор Cisco 2600

```
crypto isakmp policy 10
!--- Defines the ISAKMP parameters to be negotiated.
authentication pre-share !--- Defines the pre-shared key
to be exchanged with the peer. crypto isakmp key pre-
shared address 10.1.1.5 ! crypto ipsec transform-set
strong esp-des esp-sha-hmac !--- Defines the transform
set for ESP and/or AH. ! crypto map vpn 10 ipsec-isakmp
set peer 10.1.1.5 set transform-set strong match address
102 !--- Defines the crypto policy that includes the
peer IP address, !--- transform set that is used, as
well as the access list !--- that defines the packets
that are encrypted. ! interface ATM0/0 no ip address atm
vc-per-vp 256 no atm ilmi-keepalive dsl operating-mode
auto no fair-queue ! interface ATM0/0.1 point-to-point
pvc 0/35 encapsulation aal5mux ppp dialer dialer pool-
member 1 ! crypto map vpn !--- Applies the crypto map to
the ATM sub-interface. ! interface FastEthernet0/1 ip
address 1.1.1.1 255.255.255.0 duplex 100 speed full !
interface Dialer1 ip address 10.1.100.101 255.255.255.0
dialer pool 1 encapsulation ppp ppp pap sent-username
2621a password 7 045802150C2E crypto map vpn !---
Applies the crypto map to the Dialer interface. ! ip
classless ! ip route 2.2.2.0 255.255.255.0 10.1.1.5 ip
route 10.1.1.0 255.255.255.0 10.1.100.1 !--- Static
routes between 2600 CPE and IPSec server. ip route
0.0.0.0 0.0.0.0 Dialer1 ! access-list 102 permit ip
1.1.1.0 0.0.0.255 2.2.2.0 0.0.0.255 !--- Access list
that defines the addresses that are encrypted. ! end
```

Устройство головной станции IPSec - маршрутизатор Cisco 3600

```
crypto isakmp policy 10
!--- Defines the ISAKMP parameters to be negotiated.
authentication pre-share !--- Defines the pre-shared key
to be exchanged with the peer. crypto isakmp key pre-
shared address 10.1.100.101 ! crypto ipsec transform-set
strong esp-des esp-sha-hmac !--- Defines the transform
set for ESP and/or AH. ! crypto map vpn 10 ipsec-isakmp
set peer 10.1.100.101 set transform-set strong match
address 102 !--- Defines the crypto policy that includes
the peer IP address, !--- transform set that are used,
and the access list !--- that defines the packets to be
encrypted. ! interface FastEthernet0/0 ip address
10.1.1.5 255.255.255.0 duplex 100 speed full crypto map
vpn !--- Applies the crypto map to the Fast Ethernet
```

```
interface. ! interface FastEthernet0/1 ip address
2.2.2.1 255.255.255.0 speed full full-duplex ! ip route
1.1.1.0 255.255.255.0 10.1.1.10 ip route 10.1.100.0
255.255.255.0 10.1.1.10 ! access-list 102 permit ip
2.2.2.0 0.0.0.255 1.1.1.0 0.0.0.255 !--- Access list
that defines the addresses to be encrypted. ! end
```

DSLAM Cisco 6160

```
dsl-profile full
 dmt bitrate maximum fast downstream 10240 upstream 1024
 dmt bitrate maximum interleaved downstream 0 upstream 0
 !
 atm address
47.0091.8100.0000.0004.6dd6.7c01.0004.6dd6.7c01.00
 atm router pnni
 no aesa embedded-number left-justified
 none 1 level 56 lowest
 redistribute atm-static
 !
 interface atm0/0
 no ip address
 atm maxvp-number 0
 atm maxvc-number 4096
 atm maxvci-bits 12
 !
 interface atm 1/2
 no ip address
 dsl profile full
 no atm ilmi-keepalive
 atm soft-vc 0 35 dest-address
 47.0091.8100.0000.0004.c12b.cd81.4000.0c80.8000.00 0 36
 rx-cttr 1 tx-cttr 1
!--- The previous two lines need to be on one line. !---
The network service access point (NSAP) !--- address
comes from the NSP on the Cisco 6400. Issue !--- a show
atm address command. !
```

Cisco 6400 NRP

```
!
username cisco password cisco
!
vc-class atm pppoa
 encapsulation aal5mux ppp Virtual-template1
 !
 interface loopback 0
 ip address 10.1.100.1 255.255.255.0
 !
 interface atm 0/0/0
 no ip address
 no ip route-cache
 no ip mroute-cache
 no atm auto-configuration
 atm ilmi-keepalive 10
 pvc 0/16 ilmi
 !
 hold-queue 1000 in
 !
 interface atm 0/0/0.1 multipoint
 no ip route-cache
 no ip mroute-cach
 class-int pppoa
 pvc 0/36
 !
 interface fast 0/0/0
```

```
 ip address 10.1.1.10 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 half-duplex
 !
 interface Virtual-Template1
 ip unnumbered Loopback0
 no ip route-cache
 peer default ip address pool pppoa
 ppp authentication pap chap
 ppp ipcp accept-address
 ppp multilink
 no ppp multilink fragmentation
 !
 ip local pool pppoa 10.1.100.2 10.1.100.100
 !
```

Предупреждения

Соединения ADSL могут быть настроены с virtual-template или интерфейсом номеронабирателя.

Интерфейс номеронабирателя используется для настройки DSL CPE для получения адреса от поставщика услуг (О IP-адресе выполняют согласование). Виртуальный интерфейс является вниз-отключенным-интерфейсом и не поддерживает опцию согласованного адреса, которая необходима в среде DSL. Виртуальные интерфейсы были первоначально внедрены для сред DSL. В настоящее время интерфейс номеронабирателя является рекомендуемой конфигурацией на стороне DSL CPE.

Две проблемы найдены во время конфигурации интерфейсов номеронабирателя с IPSec:

- Идентификатор ошибки Cisco CSCdu30070 (только зарегистрированные клиенты) — Только программный IPSec по DSL: клин входной очереди на интерфейсе номеронабирателя DSL.
- Идентификатор ошибки Cisco CSCdu30335 (только зарегистрированные клиенты) — Аппаратный IPSec по DSL: клин входной очереди на интерфейсе номеронабирателя.

Текущее решение проблемы для обеих из этих проблем должно настроить DSL CPE с использованием виртуального интерфейса, как описано в конфигурации.

Исправляет для обеих из этих проблем, запланированы программное обеспечение Cisco IOS версии 12.2(4)T. После этого выпуска обновленная версия этого документа зарегистрирована для показа конфигурации интерфейса программы для набора номера как другой опции.

Проверка

Этот раздел предоставляет информацию, которую можно использовать, чтобы подтвердить, что конфигурация работает должным образом.

Несколько **команд показа** могут использоваться, чтобы проверить, что Сеанс IPSec установлен между узлами. Команды необходимы только на Узлах IPsec, в этом случае Cisco 2600 и серии 3600.

Некоторые команды show поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды show.

- **show crypto engine connections active – Показывает все встроенные сопоставления безопасности второго этапа и объем отправленного трафика.**
- **show crypto ipsec sa** КОНТЕКСТ БЕЗОПАСНОСТИ IPSEC, созданный между узлами.

Это - пример вывода команды для команды **show crypto engine connection active**.

```
show crypto engine connections active ID Interface IP-Address State Algorithm Encrypt Decrypt 1
<none> <none> set HMAC_SHA+DES_56_CB 0 0 200 Virtual-Template1 10.1.100.101 set HMAC_SHA 0 4 201
Virtual-Template1 10.1.100.101 set HMAC_SHA 4 0
```

Это - пример вывода команды для **команды show crypto ipsec sa**.

```
show crypto ipsec sa Interface: Virtual-Template1 Crypto map tag: vpn, local addr. 10.1.100.101
Local ident (addr/mask/prot/port): (1.1.1.0/255.255.255.0/0/0) Remote ident
(addr/mask/prot/port): (2.2.2.0/255.255.255.0/0/0) Current_peer: 10.1.1.5 PERMIT, flags=
{origin_is_acl,} #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4 #pkts decaps: 4, #pkts
decrypt: 4, #pkts verify 4 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0,
#pkts compr failed: 0, # pkts decompress failed: 0 #send errors 11, #recv errors 0 local crypto
endpt: 10.1.100.101, remote crypto endpt.: 10.1.1.5 path mtu 1500, media mtu 1500 current
outbound spi: BB3629FB inbound esp sas: spi: 0x70C3B00B(1891872779) transform: esp-des, esp-md5-
hmac in use settings ={Tunnel,} slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn sa timing:
remaining key lifetime (k/sec): (4607999/3446) IV size: 8 bytes Replay detection support: Y
Inbound ah sas: Inbound pcp sas: Outbound esp sas: Spi: 0xBB3629FB(3140889083) Transform: esp-
des, esp-md5-hmac In use settings ={Tunnel,} Slot:0, conn id: 2001, flow_id: 2, crypto map: vpn
Sa timing: remaining key lifetime (k/sec): (4607999/3446) IV size: 8bytes Replay detection
support: Y Outbound ah sas: Outbound pcp sas:
```

Устранение неполадок

Этот раздел предоставляет информацию, которую можно использовать для устранения проблем конфигурации.

Сообщение `"Modem state = 0x8"`, о котором сообщает **команда debug atm events** обычно, означает, что WIC1-ADSL неспособен получить Определение несущей от связанного DSLAM. В этой ситуации, потребительские нужды, чтобы проверить, что сигнал DSL настроен на средних двух проводах относительно разъёма RJ11. Некоторые Telco (телефонная компания) настраивают сигнал DSL на внешних двух контактах вместо этого.

Команды устранения неполадок

Некоторые команды show поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды show.

Примечание: Перед запуском **команд отладки** обратитесь к разделу Важные сведения о командах отладки.

Внимание. : Не выполняйте отладку на действующей сети. Объем информации, который показы могут перегрузить ваш маршрутизатор к точке, где не выполнены никакие потоки данных и Сообщения CPUHOG.

- **debug crypto ipsec– показывает события IPSec.**
- **debug crypto isakmp – отображает сообщения о событиях IKE.**

Сводка

Реализация IPSec по соединению ADSL предоставляет безопасное и надежное сетевое подключение между филиалами компании и центральными узлами. Использование серии Cisco 2600/3600 с ADSL-WIC и модулями аппаратного шифрования предлагает снижение затрат владения клиенту как ADSL, и IPSec может теперь быть выполнен в решении для одиночного маршрутизатора. Конфигурация и предупреждения, перечисленные в этой газете, должны служить основными принципами для устанавливания этого типа соединения.

Дополнительные сведения

- Введение в шифрование IPSec
- Маршрутизаторы серии Cisco 2600
- Виртуальные частные сети
- Техническая поддержка DSL И LRE
- Поддержка продуктов универсальных шлюзов
- Набор и поддержка технологии доступа
- Техническая поддержка - Cisco Systems