Пример конфигурации коммутации IPSec вручную между маршрутизаторами

Содержание

Введение

Этот пример конфигурации позволяет шифровать трафик между сетями 12.12.12.x и 14.14.14.x при помощи ручного задания ключей IPSec. Для проверки использовались список ACL и команда extended ping для узлов с 12.12.12.12 по 14.14.14.14.

Ручная манипуляция по ключу обычно только необходима, когда устройство Cisco настроено для шифрования трафика к устройству другого поставщика, которое не поддерживает Протокол IKE. Если IKE конфигурируем на обоих устройствах, предпочтительно использовать автоматическое манипулирование. Индексы параметра безопасности устройства Cisco (SPI) находятся в десятичном числе, однако, некоторые поставщики выполняют в шестнадцатеричных SPI. Если это верно, тогда иногда преобразование необходимо.

Предварительные условия

Требования

Для данного документа отсутствуют предварительные условия.

Используемые компоненты

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

- Маршрутизаторы Cisco 3640 и 1605
- Cisco IOS® Software Release 12.3(3). o

Примечание: На всех платформах, которые содержат адаптеры аппаратного шифрования, не поддерживается шифрование в ручном режиме, когда включен адаптер аппаратного шифрования.

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. Если используемая сеть — действующая, необходимо изучить возможные последствия каждой команды.

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:

- Облегченная конфигурация
- Домашняя конфигурация

Облегченная конфигурация

```
light#show running-config Building configuration...
Current configuration : 1177 bytes ! version 12.3
service timestamps debug datetime msec service
timestamps log datetime msec no service password-
encryption ! hostname light ! boot-start-marker boot-
end-marker ! enable password cisco ! no aaa new-model ip
subnet-zero ! no crypto isakmp enable ! !--- IPsec
configuration crypto ipsec transform-set encrypt-des
esp-des esp-sha-hmac ! ! crypto map testcase 8 ipsec-
manual set peer 11.11.11.12 set session-key inbound esp
1001 cipher 1234abcd1234abcd authenticator 20 set
```

```
session-key outbound esp 1000 cipher abcd1234abcd1234
authenticator 20 set transform-set encrypt-des !---
Traffic to encrypt match address 100 ! ! interface
Ethernet2/0 ip address 12.12.12.12 255.255.255.0 half-
duplex<br>! interface Ethernet2/1 ip address 11.11.11.11
255.255.255.0 half-duplex !--- Apply crypto map. crypto
map testcase ! ip http server no ip http secure-server
ip classless ip route 0.0.0.0 0.0.0.0 11.11.11.12 ! ! !-
-- Traffic to encrypt access-list 100 permit ip host
12.12.12.12 host 14.14.14.14 ! ! ! ! line con 0 line aux
0 line vty 0 4 login ! ! !
```

Домашняя конфигурация

```
house#show running-config Current configuration : 1194
bytes ! version 12.3 service timestamps debug uptime
service timestamps log uptime no service password-
encryption ! hostname house ! ! logging buffered 50000
debugging enable password cisco ! no aaa new-model ip
subnet-zero ip domain name cisco.com ! ip cef ! ! no
crypto isakmp enable ! ! !--- IPsec configuration crypto
ipsec transform-set encrypt-des esp-des esp-sha-hmac !
crypto map testcase 8 ipsec-manual set peer 11.11.11.11
set session-key inbound esp 1000 cipher abcd1234abcd1234
authenticator 20 set session-key outbound esp 1001
cipher 1234abcd1234abcd authenticator 20 set transform-
set encrypt-des !--- Traffic to encrypt match address
100 ! ! interface Ethernet0 ip address 11.11.11.12
255.255.255.0 !--- Apply crypto map. crypto map testcase
! interface Ethernet1 ip address 14.14.14.14
255.255.255.0 ! ip classless ip route 0.0.0.0 0.0.0.0
11.11.11.11 no ip http server no ip http secure-server !
! !--- Traffic to encrypt access-list 100 permit ip host
14.14.14.14 host 12.12.12.12 ! ! line con 0 exec-timeout
0 0 transport preferred none transport output none line
vty 0 4 exec-timeout 0 0 password cisco login transport
preferred none transport input none transport output
none ! ! end
```

Проверка

Этот раздел содержит сведения, которые можно использовать для проверки правильности работы конфигурации.

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

- **show crypto ipsec sa** фазе два сопоставления безопасности.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды для устранения неполадок

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".

- **debug crypto ipsec** согласования IPsec фазы два.
- **debug crypto engine– показывает зашифрованный трафик.**

Наборы для преобразования не согласованы

(свет - ah-sha-hmac, дом - esp-des).

```
*Mar  2 01:16:09.849: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 11.11.11.11, remote= 11.11.11.12,
    local_proxy= 12.12.12.12/255.255.255.255/0/0 (type=1),
    remote_proxy= 14.14.14.14/255.255.255.255/0/0 (type=1),
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xACD76816(2899798038), conn_id= 0, keysize= 0, flags= 0x400A
*Mar  2 01:16:09.849: IPSEC(manual_key_stuffing):
keys missing for addr 11.11.11.12/prot 51/spi 0.....
```

Списки управления доступом не совпадают

На стороне_A ("светлый" маршрутизатор) имеется связь внутреннего узла к внутреннему узлу, а на стороне_B ("домашний" маршрутизатор) интерфейс к интерфейсу. ACL должны всегда быть симметричными (это не).

```
hostname house
match address 101
access-list 101 permit ip host 11.11.11.12 host 11.11.11.11
!

hostname light
match address 100
access-list 100 permit ip host 12.12.12.12 host 14.14.14.14
```

Эти выходные данные взяты от эхо-запроса инициирующего side_A:

```
nothing

light#show crypto engine connections active ID Interface IP-Address State Algorithm Encrypt
Decrypt 2000 Ethernet2/1 11.11.11.11 set DES_56_CBC 5 0 2001 Ethernet2/1 11.11.11.11 set
DES_56_CBC 0 0
```

Когда side_A инициирует эхо-запрос, эти выходные данные взяты от side_B:

```
house#
1d00h: IPSEC(epa_des_crypt): decrypted packet failed SA identity check
1d00h: IPSEC(epa_des_crypt): decrypted packet failed SA identity check
1d00h: IPSEC(epa_des_crypt): decrypted packet failed SA identity check
1d00h: IPSEC(epa_des_crypt): decrypted packet failed SA identity check
1d00h: IPSEC(epa_des_crypt): decrypted packet failed SA identity check


house#show crypto engine connections active ID Interface IP-Address State Algorithm Encrypt
Decrypt 2000 Ethernet0 11.11.11.12 set DES_56_CBC 0 0 2001 Ethernet0 11.11.11.12 set DES_56_CBC
0 5
```

Эти выходные данные взяты от эхо-запроса инициирующего side_B:

```
side_ B

%CRYPTO-4-RECVD_PKT_NOT_IPSEC: Rec'd packet not an IPSEC packet.
        (ip) vrf/dest_addr= /12.12.12.12, src_addr= 14.14.14.14, prot= 1
```

У одной стороны есть криптокарта, а у второй - нет

```
%CRYPTO-4-RECVD_PKT_NOT_IPSEC: Rec'd packet not an IPSEC packet.
        (ip) vrf/dest_addr= /14.14.14.14, src_addr= 12.12.12.12, prot= 1
```

Эти выходные данные взяты от side_B, который имеет криптокарту:

```
house#show crypto engine connections active
 ID Interface       IP-Address      State  Algorithm           Encrypt  Decrypt
2000 Ethernet0       11.11.11.12     set    DES_56_CBC                5        0
2001 Ethernet0       11.11.11.12     set    DES_56_CBC                0        0
```

Плата CEA включена

```
1d05h: %HW_VPN-1-HPRXERR: Hardware VPN0/13: Packet
 Encryption/Decryption error, status=4098.....
```

Дополнительные сведения

- Согласование IPsec/Протоколы IKE
- Cisco Systems – техническая поддержка и документация