Настройка подключения маршрутизатор-маршрутизатор IPSec с перегрузкой NAT и Cisco Secure VPN Client

Содержание

Введение

В этом примере конфигурации выполняется шифрование трафика из сети за шлюзом Light в сеть за шлюзом House (из сети 192.168.100.x в сеть 192.168.200.x). Также выполняется перегрузка преобразования сетевых адресов (NAT). Сеансы VPN-клиента с шифрованием разрешены на шлюзе Light с шаблоном, предварительными общими ключами и конфигурацией режима. Трафик в Интернет проходит преобразование адресов, но не шифруется.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Выпуск 12.2.7 и 12.2.8T программного обеспечения Cisco IOS
- Cisco Secure VPN Client 1.1 (показанный как 2.1.12 в меню **IRE client Help> About**)

- Маршрутизаторы Cisco 3600**Примечание:** При использовании Маршрутизаторы серии Cisco 2600 для этого вида сценария VPN, то маршрутизаторы должны быть установлены с крипто-Образами IOS IPSec VPN.

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.

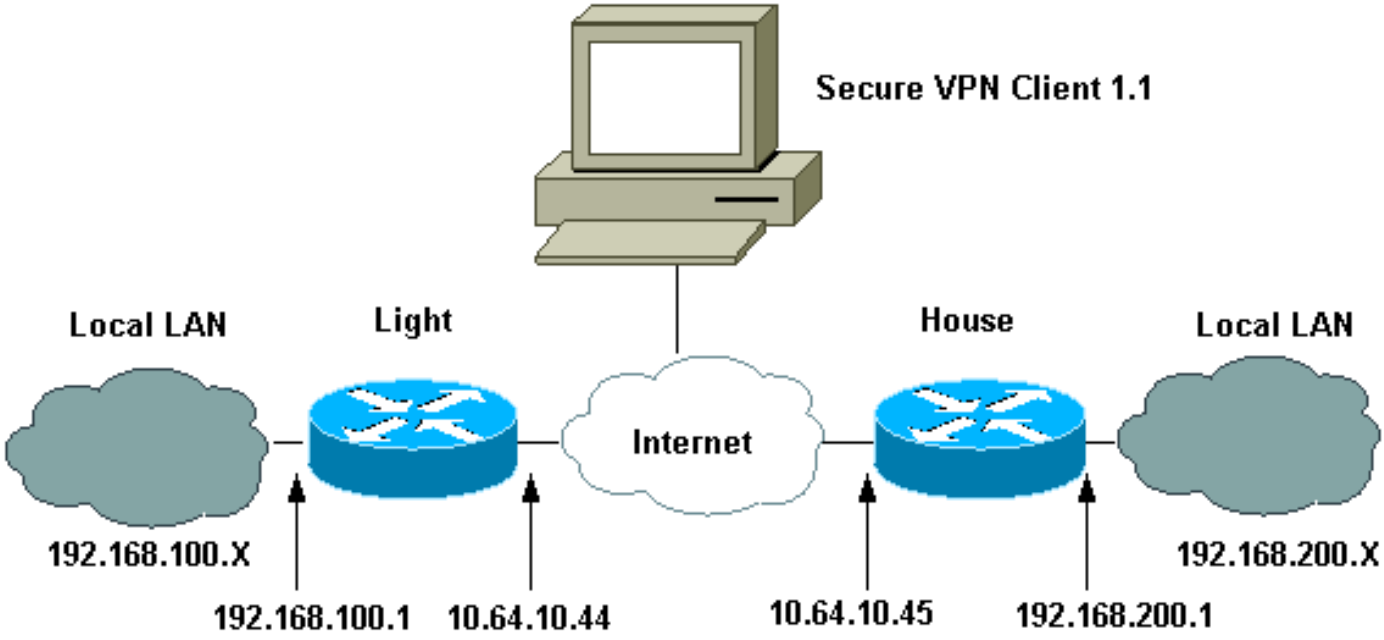
Настройка

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.

- Облегченная конфигурация
- Домашняя конфигурация
- Конфигурация клиента VPN

Облегченная конфигурация

```
 Current configuration : 2047 bytes
 !
 version 12.2
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname Light ! boot system flash:c3660-ik9o3s-mz.122-
8T ! ip subnet-zero ! ip audit notify log ip audit po
max-events 100 ip ssh time-out 120 ip ssh
authentication-retries 3 ! !--- IPsec Internet Security
Association and !--- Key Management Protocol (ISAKMP)
policy. crypto isakmp policy 5 hash md5 authentication
pre-share !--- ISAKMP key for static LAN-to-LAN tunnel
!--- without extended authenticaton (xauth). crypto
isakmp key cisco123 address 10.64.10.45 no-xauth !---
ISAKMP key for the dynamic VPN Client. crypto isakmp key
123cisco address 0.0.0.0 0.0.0.0 !--- Assign the IP
address to the VPN Client. crypto isakmp client
configuration address-pool local test-pool ! ! ! crypto
ipsec transform-set testset esp-des esp-md5-hmac !
crypto dynamic-map test-dynamic 10 set transform-set
testset ! ! !--- VPN Client mode configuration
negotiation, !--- such as IP address assignment and
xauth. crypto map test client configuration address
initiate crypto map test client configuration address
respond !--- Static crypto map for the LAN-to-LAN
tunnel. crypto map test 5 ipsec-isakmp set peer
10.64.10.45 set transform-set testset !--- Include the
private network-to-private network traffic !--- in the
encryption process. match address 115 !--- Dynamic
crypto map for the VPN Client. crypto map test 10 ipsec-
isakmp dynamic test-dynamic ! call rsvp-sync ! ! ! ! !
fax interface-type modem mta receive maximum-recipients
0 ! controller E1 2/0 ! ! ! interface FastEthernet0/0 ip
address 10.64.10.44 255.255.255.224 ip nat outside
duplex auto speed auto crypto map test ! interface
FastEthernet0/1 ip address 192.168.100.1 255.255.255.0
ip nat inside duplex auto speed auto ! interface BRI4/0
no ip address shutdown ! interface BRI4/1 no ip address
shutdown ! interface BRI4/2 no ip address shutdown !
interface BRI4/3 no ip address shutdown ! !--- Define
the IP address pool for the VPN Client. ip local pool
test-pool 192.168.1.1 192.168.1.254 !--- Exclude the
private network and VPN Client !--- traffic from the NAT
process. ip nat inside source route-map nonat interface
FastEthernet0/0 overload ip classless ip route 0.0.0.0
0.0.0.0 10.64.10.33 ip http server ip pim bidir-enable !
!--- Exclude the private network and VPN Client !---
traffic from the NAT process. access-list 110 deny ip
192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255 access-
list 110 deny ip 192.168.100.0 0.0.0.255 192.168.1.0
0.0.0.255 access-list 110 permit ip 192.168.100.0
0.0.0.255 any !--- Include the private network-to-
private network traffic !--- in the encryption process.
access-list 115 permit ip 192.168.100.0 0.0.0.255
192.168.200.0 0.0.0.255 ! !--- Exclude the private
network and VPN Client !--- traffic from the NAT
process. route-map nonat permit 10 match ip address 110
! ! dial-peer cor custom ! ! ! ! ! line con 0 line 97
108 line aux 0 line vty 0 4 ! end
```

Домашняя конфигурация

```
Current configuration : 1689 bytes
 !
 version 12.2
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname house ! boot system flash:c3660-jk8o3s-mz.122-
7.bin ! ip subnet-zero ! ! no ip domain-lookup ! ip
audit notify log ip audit po max-events 100 ip ssh time-
out 120 ip ssh authentication-retries 3 ! !--- IPsec
ISAKMP policy. crypto isakmp policy 5 hash md5
authentication pre-share !--- ISAKMP key for static LAN-
to-LAN tunnel without xauth authenticaton. crypto isakmp
key cisco123 address 10.64.10.44 no-xauth ! ! crypto
ipsec transform-set testset esp-des esp-md5-hmac ! !---
Static crypto map for the LAN-to-LAN tunnel. crypto map
test 5 ipsec-isakmp set peer 10.64.10.44 set transform-
set testset !--- Include the private network-to-private
network traffic !--- in the encryption process. match
address 115 ! call rsvp-sync cns event-service server !
! ! ! ! fax interface-type modem mta receive maximum-
recipients 0 ! ! ! interface FastEthernet0/0 ip address
10.64.10.45 255.255.255.224 ip nat outside duplex auto
speed auto crypto map test ! interface FastEthernet0/1
ip address 192.168.200.1 255.255.255.0 ip nat inside
duplex auto speed auto ! interface BRI2/0 no ip address
shutdown ! interface BRI2/1 no ip address shutdown !
interface BRI2/2 no ip address shutdown ! interface
BRI2/3 no ip address shutdown ! interface
FastEthernet4/0 no ip address shutdown duplex auto speed
auto ! !--- Exclude the private network traffic !---
from the dynamic (dynamic association to a pool) NAT
process. ip nat inside source route-map nonat interface
FastEthernet0/0 overload ip classless ip route 0.0.0.0
0.0.0.0 10.64.10.33 no ip http server ip pim bidir-
enable ! !--- Exclude the private network traffic from
the NAT process. access-list 110 deny ip 192.168.200.0
0.0.0.255 192.168.100.0 0.0.0.255 access-list 110 permit
ip 192.168.200.0 0.0.0.255 any !--- Include the private
network-to-private network traffic !--- in the
encryption process. access-list 115 permit ip
192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255 !---
Exclude the private network traffic from the NAT
process. route-map nonat permit 10 match ip address 110
! ! ! dial-peer cor custom ! ! ! ! ! line con 0 line aux
0 line vty 0 4 login ! end
```

Конфигурация клиента VPN

```
Network Security policy:
       1- TOLIGHT
       My Identity
       Connection security: Secure
       Remote Party Identity and addressing
       ID Type: IP subnet
       192.168.100.0
       255.255.255.0
       Port all Protocol all

  Connect using secure tunnel
         ID Type: IP address
         10.64.10.44
```

```
Pre-shared Key=123cisco


Authentication (Phase 1)
       Proposal 1
       Authentication method: pre-shared key
       Encryp Alg: DES
       Hash Alg: MD5
       SA life: Unspecified
       Key Group: DH 1


Key exchange (Phase 2)
       Proposal 1
       Encapsulation ESP
       Encrypt Alg: DES
       Hash Alg: MD5
       Encap: tunnel
       SA life: Unspecified
       no AH


2- Other Connections
       Connection security: Non-secure
       Local Network Interface
       Name: Any
       IP Addr: Any
       Port: All
```

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

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

- **show crypto ipsec sa** Сопоставления безопасности фазы 2 (SA).
- **show crypto isakmp sa– показывает ассоциации безопасности, соответствующие первому этапу.**

Устранение неполадок

Используйте этот раздел для устранения неполадок своей 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".

- команда debug crypto ipsec отображает согласование IPSec на втором этапе.
- debug crypto isakmp – вывод данных о согласовании ISAKMP в фазе 1.
- "debug crypto engine" - отображается зашифрованный трафик.
- clear crypto isakmp– удаляет ассоциации безопасности, связанные с 1-м этапом.
- clear crypto sa– удаляет ассоциации безопасности, связанные со 2-м этапом.

Дополнительные сведения

- Настройка параметров сетевой безопасности IPSec Network Security
- Настройка протокола защищенного обмена ключами IKE
- Страница поддержки IPsec Negotiation/IKE
- Страницы технической поддержки Cisco Secure VPN Client
- Техническая поддержка - Cisco Systems