Настройка IPSec – Cisco Secure VPN Client с центральным маршрутизатором управления доступом

Содержание

Введение

Приведенная ниже конфигурация обычно не используется. Она создана для вывода туннеля IPSec от клиента Cisco Secure VPN Client на центральный маршрутизатор. При установлении туннеля ПК получает свой IP-адрес из пула IP-адресов центрального маршрутизатора (в нашем примере, маршрутизатор назван «moss»), после чего трафик из пула может поступать в локальную сеть за маршрутизатором moss или маршрутизироваться и шифроваться с передачей в сеть за удаленным маршрутизатором (в нашем примере этот маршрутизатор назван «carter»). Кроме того, шифруется трафик из частной сети 10.13.1. X в 10.1.1. X, а; маршрутизаторы выполняют перегрузку NAT.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Операционная система Cisco IOS® версии 12.1. 5. T (c3640-io3s56i-mz.121-5. T
- Cisco Secure VPN Client 1.1

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 в документах см. Cisco Technical Tips Conventions.

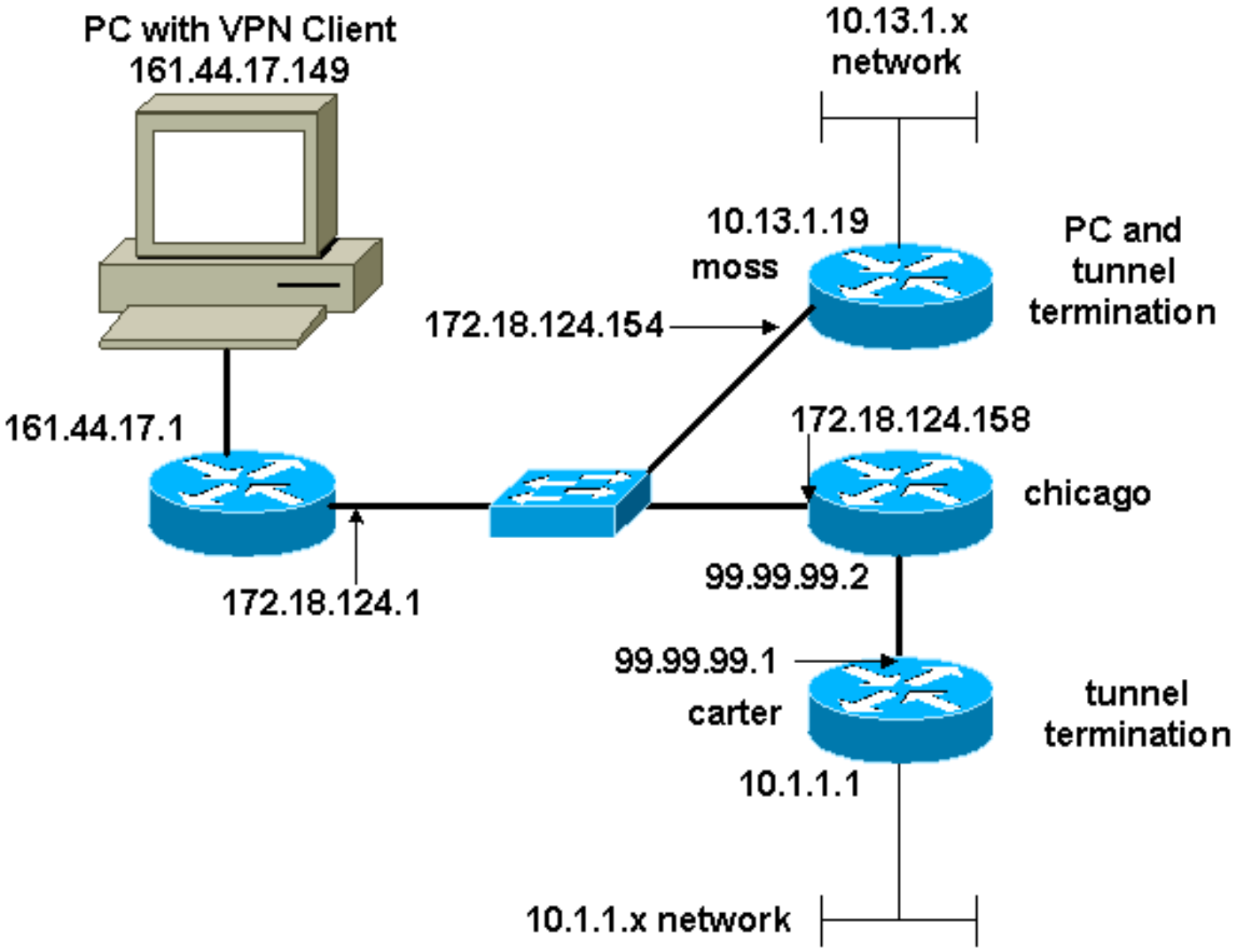
Настройка

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

Примечание: Поиск дополнительной информации о командах в данном документе можно выполнить с помощью средства "Command Lookup" (Поиск команд) (только для зарегистрированных клиентов).

Схема сети

В настоящем документе используется следующая схема сети:



Конфигурации

Эти конфигурации используются в данном документе:

- конфигурация MOSS
- настройка carter

конфигурация MOSS

```
Version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname moss
!
logging rate-limit console 10 except errors
enable password ww
!
ip subnet-zero
!
no ip finger
!
ip audit notify log
ip audit po max-events 100
!
```

```
crypto isakmp policy 1 hash md5 authentication pre-share
crypto isakmp key cisco123 address 99.99.99.1 crypto
isakmp key cisco123 address 0.0.0.0 0.0.0.0 crypto
isakmp client configuration address-pool local RTP-POOL
! crypto ipsec transform-set rtpset esp-des esp-md5-hmac
! crypto dynamic-map rtp-dynamic 20 set transform-set
rtpset ! crypto map rtp client configuration address
initiate crypto map rtp client configuration address
respond !crypto map sequence for network to network
traffic crypto map rtp 1 ipsec-isakmp set peer
99.99.99.1 set transform-set rtpset match address 115 !--
-- crypto map sequence for VPN Client network traffic.
crypto map rtp 10 ipsec-isakmp dynamic rtp-dynamic !
call rsvp-sync ! interface Ethernet2/0 ip address
172.18.124.154 255.255.255.0 ip nat outside no ip route-
cache no ip mroute-cache half-duplex crypto map rtp !
interface Serial2/0 no ip address shutdown ! interface
Ethernet2/1 ip address 10.13.1.19 255.255.255.0 ip nat
inside half-duplex ! ip local pool RTP-POOL 192.168.1.1
192.168.1.254 ip nat pool ETH20 172.18.124.154
172.18.124.154 netmask 255.255.255.0 ip nat inside
source route-map nonat pool ETH20 overload ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.1 ip route 10.1.1.0
255.255.255.0 172.18.124.158 ip route 99.99.99.0
255.255.255.0 172.18.124.158 no ip http server ! !---
Exclude traffic from NAT process. access-list 110 deny
ip 10.13.1.0 0.0.0.255 10.1.1.0 0.0.0.255 access-list
110 deny ip 10.13.1.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 110 permit ip 10.13.1.0 0.0.0.255 any !---
Include traffic in encryption process. access-list 115
permit ip 10.13.1.0 0.0.0.255 10.1.1.0 0.0.0.255 access-
list 115 permit ip 192.168.1.0 0.0.0.255 10.1.1.0
0.0.0.255 route-map nonat permit 10 match ip address 110
! dial-peer cor custom ! line con 0 transport input none
line aux 0 line vty 0 4 login ! end
```

настройка carter

```
Current configuration : 2059 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname carter
!
logging rate-limit console 10 except errors
!
ip subnet-zero
!
no ip finger
!
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 1 hash md5 authentication pre-share
crypto isakmp key cisco123 address 172.18.124.154 !
crypto ipsec transform-set rtpset esp-des esp-md5-hmac !
!--- crypto map sequence for network-to-network traffic.
crypto map rtp 1 ipsec-isakmp set peer 172.18.124.154
set transform-set rtpset match address 115 ! call rsvp-
sync ! interface Ethernet0/0 ip address 99.99.99.1
255.255.255.0 ip nat outside half-duplex crypto map rtp
```

```
! interface FastEthernet3/0 ip address 10.1.1.1
255.255.255.0 ip nat inside duplex auto speed 10 ! ip
nat pool ETH00 99.99.99.1 99.99.99.1 netmask
255.255.255.0 ip nat inside source route-map nonat pool
ETH00 overload ip classless ip route 0.0.0.0 0.0.0.0
99.99.99.2 no ip http server ! !--- Exclude traffic from
NAT process. access-list 110 deny ip 10.1.1.0 0.0.0.255
10.13.1.0 0.0.0.255 access-list 110 deny ip 10.1.1.0
0.0.0.255 192.168.1.0 0.0.0.255 access-list 110 permit
ip 10.1.1.0 0.0.0.255 any !--- Include traffic in
encryption process. access-list 115 permit ip 10.1.1.0
0.0.0.255 10.13.1.0 0.0.0.255 access-list 115 permit ip
10.1.1.0 0.0.0.255 192.168.1.0 0.0.0.255 route-map nonat
permit 10 match ip address 110 ! line con 0 transport
input none line aux 0 line vty 0 4 password ww login !
end
```

Проверка

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

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

- команда show crypto ipsec sa – отображает связи безопасности, соответствующие второму этапу.
- команда show crypto isakmp sa вЂ отображает сопоставления безопасности, соответствующие первому этапу.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды для устранения неполадок

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

Примечание: Прежде чем вызывать команды debug, обратитесь к разделу 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, соответствующие первому этапу.
- clear crypto sa– удаляет ассоциации безопасности, соответствующие второму этапу.

Дополнительные сведения

- Настройка параметров сетевой безопасности IPSec Network Security
- Настройка протокола защищенного обмена ключами IKE
- Страница поддержки Cisco VPN Client
- Страница поддержки IPSec
- Техническая поддержка - Cisco Systems