Настройка полносвязной ячеистой структуры сети по протоколу IPSec от маршрутизатора к маршрутизатору

Содержание

Введение

Этот пример конфигурации показывает полносвязное шифрование между тремя маршрутизаторами с помощью одной криптокарты на каждом маршрутизаторе к сетям позади каждого из его двух узлов.

Шифрование следует выполнять из:

- от сети 160.160.160.x к сети 170.170.170.x
- Из сети 160.160.160.x в сеть 180.180.180.x
- 170.170.170.x сеть к 180.180.180.x сеть

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Выпуск 12.2.7C и 12.2.8 (T) 4 программного обеспечения Cisco IOS
- Cisco 2500 и 3600 маршрутизаторов

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 Технические рекомендации Cisco. Условные обозначения.

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 этом документе используются настройки сети, показанные на данной диаграмме.

Конфигурации

Эти конфигурации используются в данном документе.

- Конфигурация Dr_Whoovie
- Конфигурация Yertle
- Конфигурация Thidwick

Примечание: Эти конфигурации были недавно протестированы с текущим кодом (ноябрь 2003) в рамках документа.

Конфигурация Dr_Whoovie

```
Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname dr_whoovie
!
enable secret 5 $1$KxKv$cbqKsZtQTLJLGPN.tErFZ1
enable password ww
!
ip subnet-zero
!
cns event-service server
!
!--- Internet Key Exchange (IKE) Policies: crypto isakmp
```

```
policy 1 authentication pre-share crypto isakmp key
cisco123 address 150.150.150.3 crypto isakmp key
cisco123 address 150.150.150.2 ! !--- IPSec Policies:
crypto ipsec transform-set 170cisco esp-des esp-md5-hmac
crypto ipsec transform-set 180cisco esp-des esp-md5-hmac
! crypto map ETH0 17 ipsec-isakmp set peer 150.150.150.2
set transform-set 170cisco !--- Include the
160.160.160.x to 170.170.170.x network !--- in the
encryption process. match address 170 crypto map ETH0 18
ipsec-isakmp set peer 150.150.150.3 set transform-set
180cisco !--- Include the 160.160.160.x to 180.180.180.x
network !--- in the encryption process. match address
180 ! interface Ethernet0 ip address 150.150.150.1
255.255.255.0 no ip directed-broadcast no ip route-cache
no ip mroute-cache no mop enabled crypto map ETH0 !
interface Ethernet1 no ip address no ip directed-
broadcast shutdown ! interface Serial0 ip address
160.160.160.1 255.255.255.0 no ip directed-broadcast no
ip mroute-cache no fair-queue ! interface Serial1 no ip
address no ip directed-broadcast clockrate 4000000 ! ip
classless ip route 170.170.170.0 255.255.255.0
150.150.150.2 ip route 180.180.180.0 255.255.255.0
150.150.150.3 no ip http server ! !--- Include the
160.160.160.x to 170.170.170.x network !--- in the
encryption process. access-list 170 permit ip
160.160.160.0 0.0.0.255 170.170.170.0 0.0.0.255 !---
Include the 160.160.160.x to 180.180.180.x network !---
in the encryption process. access-list 180 permit ip
160.160.160.0 0.0.0.255 180.180.180.0 0.0.0.255 dialer-
list 1 protocol ip permit dialer-list 1 protocol ipx
permit ! line con 0 transport input none line aux 0 line
vty 0 4 password ww login ! end
```

Конфигурация Yertle

```
Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname yertle
!
enable secret 5 $1$me5Q$2kF5zKlPPTvHEBdGiEZ9m/
enable password ww
!
ip subnet-zero
!
cns event-service server
!
!--- IKE Policies: crypto isakmp policy 1 authentication
pre-share crypto isakmp key cisco123 address
150.150.150.3 crypto isakmp key cisco123 address
150.150.150.1 ! !--- IPSec Policies: crypto ipsec
transform-set 160cisco esp-des esp-md5-hmac crypto ipsec
transform-set 180cisco esp-des esp-md5-hmac ! crypto map
ETH0 16 ipsec-isakmp set peer 150.150.150.1 set
transform-set 160cisco !--- Include the 170.170.170.x to
160.160.160.x network !--- in the encryption process.
match address 160 crypto map ETH0 18 ipsec-isakmp set
peer 150.150.150.3 set transform-set 180cisco !---
Include the 170.170.170.x to 180.180.180.x network !---
in the encryption process. match address 180 ! interface
Ethernet0 ip address 150.150.150.2 255.255.255.0 no ip
```

```
directed-broadcast no ip route-cache no ip mroute-cache
no mop enabled crypto map ETH0 ! interface Serial0 no ip
address no ip directed-broadcast no ip mroute-cache
shutdown no fair-queue ! interface Serial1 ip address
170.170.170.1 255.255.255.0 no ip directed-broadcast !
ip classless ip route 160.160.160.0 255.255.255.0
150.150.150.1 ip route 180.180.180.0 255.255.255.0
150.150.150.3 no ip http server ! !--- Include the
170.170.170.x to 160.160.160.x network !--- in the
encryption process. access-list 160 permit ip
170.170.170.0 0.0.0.255 160.160.160.0 0.0.0.255 !---
Include the 170.170.170.x to 180.180.180.x network !---
in the encryption process. access-list 180 permit ip
170.170.170.0 0.0.0.255 180.180.180.0 0.0.0.255 dialer-
list 1 protocol ip permit dialer-list 1 protocol ipx
permit ! line con 0 transport input none line aux 0 line
vty 0 4 password ww login ! end
```

Конфигурация Thidwick

```
Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname thidwick
!
enable secret 5 $1$Pcpo$fj4FNS1dEDY9lGg3Ne6FK1
enable password ww
!
ip subnet-zero
!
isdn switch-type basic-5ess
isdn voice-call-failure 0
cns event-service server
!
!--- IKE Policies: crypto isakmp policy 1 authentication
pre-share crypto isakmp key cisco123 address
150.150.150.1 crypto isakmp key cisco123 address
150.150.150.2 ! !--- IPSec Policies: crypto ipsec
transform-set 160cisco esp-des esp-md5-hmac crypto ipsec
transform-set 170cisco esp-des esp-md5-hmac ! crypto map
ETH0 16 ipsec-isakmp set peer 150.150.150.1 set
transform-set 160cisco !--- Include the 180.180.180.x to
160.160.160.x network !--- in the encryption process.
match address 160 crypto map ETH0 17 ipsec-isakmp set
peer 150.150.150.2 set transform-set 170cisco !---
Include the 180.180.180.x to 170.170.170.x network !---
in the encryption process. match address 170 ! interface
Ethernet0 ip address 150.150.150.3 255.255.255.0 no ip
directed-broadcast no ip route-cache no ip mroute-cache
no mop enabled crypto map ETH0 ! interface Serial0 no ip
address no ip directed-broadcast no ip mroute-cache no
fair-queue clockrate 4000000 ! interface Serial1 ip
address 180.180.180.1 255.255.255.0 no ip directed-
broadcast clockrate 4000000 ! interface BRI0 no ip
address no ip directed-broadcast shutdown isdn switch-
type basic-5ess ! ip classless ip route 160.160.160.0
255.255.255.0 150.150.150.1 ip route 170.170.170.0
255.255.255.0 150.150.150.2 no ip http server ! !---
Include the 180.180.180.x to 160.160.160.x network !---
in the encryption process. access-list 160 permit ip
180.180.180.0 0.0.0.255 160.160.160.0 0.0.0.255 !---
```

```
Include the 180.180.180.x to 170.170.170.x network !---
in the encryption process. access-list 170 permit ip
180.180.180.0 0.0.0.255 170.170.170.0 0.0.0.255 dialer-
list 1 protocol ip permit dialer-list 1 protocol ipx
permit ! 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.

- **show crypto ipsec sa** параметры настройки, используемые текущим [IPSec] сопоставления безопасности.
- **show crypto isakmp sa** все текущие сопоставления безопасности IKE в узле.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды для устранения неполадок

Примечание: Прежде чем вызывать команды debug, обратитесь к разделу Важные сведения о командах отладки.

- **debug crypto ipsec – отображает согласования IPSec на Этапе 2.**
- **debug crypto isakmp** согласования Протокола ISAKMP фазы 1.
- **debug crypto engine– показывает зашифрованный трафик.**
- **clear crypto isakmp– удаляет ассоциации безопасности, соответствующие первому этапу.**
- **clear crypto sa– удаляет ассоциации безопасности, соответствующие второму этапу.**

Дополнительные сведения

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