Настройка топологии «Звезда» маршрутизатор-маршрутизатор IPSec

Содержание

Введение

В этом документе показано шифрование в топологии типа «звезда» от одного маршрутизатора (центрального) к трем другим (оконечным). На центральном маршрутизаторе имеется только одна криптокарта, которая задает сети после каждых трех одноранговых узлов сети. Криптокарты на каждом из оконечных маршрутизаторов указывают сеть за центральным маршрутизатором.

Шифрование выполняется между следующими сетями:

- от сети 160.160.160.x к сети 170.170.170.x
- Из сети 160.160.160.x в сеть 180.180.180.x
- сеть 160.160.160.x – сеть 190 190 190.x

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Выпуск программного обеспечения Cisco IOS® 12.0.7T или выше
- Маршрутизаторы Cisco 2500

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 Dr_Whoovie
- конфигурация sam-I-am
- конфигурация Thidwick
- конфигурация Yertle

конфигурация Dr_Whoovie

```
Current configuration:
!
version 12.0
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
!--- Configure the Internet Key Exchange (IKE) !---
policy and preshared key for each peer: !--- IKE policy
defined for peers. crypto isakmp policy 1 authentication
```

```
pre-share !--- Preshared keys for different peers.
crypto isakmp key cisco170 address 150.150.150.2 crypto
isakmp key cisco180 address 150.150.150.3 crypto isakmp
key cisco190 address 150.150.150.4 !--- Configure the
IPSec parameters: !--- IPSec transform sets. crypto
ipsec transform-set 170cisco esp-des esp-md5-hmac crypto
ipsec transform-set 180cisco esp-des esp-md5-hmac crypto
ipsec transform-set 190cisco esp-des esp-md5-hmac !
crypto map ETH0 17 ipsec-isakmp !--- Set the peer. set
peer 150.150.150.2 !--- The IPSec transform set is used
for this tunnel. set transform-set 170cisco !---
Interesting traffic for peer 150.150.150.2. match
address 170 crypto map ETH0 18 ipsec-isakmp !--- Set the
peer. set peer 150.150.150.3 !--- The IPSec transform
set is used for this tunnel. set transform-set 180cisco
!--- Interesting traffic for peer 150.150.150.3. match
address 180 crypto map ETH0 19 ipsec-isakmp !--- Set the
peer. set peer 150.150.150.4 !--- The IPSec transform
set is used for this tunnel. set transform-set 190cisco
!--- Interesting traffic for peer 150.150.150.4. match
address 190 ! 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 !---
Apply crypto map on the interface. crypto map ETH0 !
interface Serial0 ip address 160.160.160.1 255.255.255.0
no ip directed-broadcast no ip mroute-cache no fair-
queue ! 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 ip route 190.190.190.0
255.255.255.0 150.150.150.4 no ip http server ! !---
Access list that shows traffic to encryption from
yertle. access-list 170 permit ip 160.160.160.0
0.0.0.255 170.170.170.0 0.0.0.255 !--- Access list that
shows traffic to encryption from thidwick. access-list
180 permit ip 160.160.160.0 0.0.0.255 180.180.180.0
0.0.0.255 !--- Access list that shows traffic to
encryption from sam-i-am. access-list 190 permit ip
160.160.160.0 0.0.0.255 190.190.190.0 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 sam-I-am

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Sam-I-am
!
enable secret 5 $1$HDyw$qubSJdqfIC0f1VLvHmg/P0
enable password ww
!
ip subnet-zero
!
isdn switch-type basic-5ess
isdn voice-call-failure 0
cns event-service server
!--- Configure the IKE policy and preshared key for the
hub: crypto isakmp policy 1 authentication pre-share
crypto isakmp key cisco190 address 150.150.150.1 !---
Configure the IPSec parameters: !--- IPSec transform
```

```
set. crypto ipsec transform-set 190cisco esp-des esp-
md5-hmac !--- Crypto map definition for the hub site.
crypto map ETH0 19 ipsec-isakmp !--- Set the peer. set
peer 150.150.150.1 !--- IPSec transform set. set
transform-set 190cisco !--- Interesting traffic for peer
150.150.150.1 (hub site). match address 190 ! interface
Ethernet0 ip address 150.150.150.4 255.255.255.0 no ip
directed-broadcast no ip route-cache no ip mroute-cache
no mop enabled !--- Apply crypto map on the interface.
crypto map ETH0 ! interface Serial0 ip address
190.190.190.1 255.255.255.0 no ip directed-broadcast no
ip mroute-cache no fair-queue ! ip classless ip route
160.160.160.0 255.255.255.0 150.150.150.1 no ip http
server !--- Access list that shows traffic to encryption
!--- for the hub site (dr_whoovie). access-list 190
permit ip 190.190.190.0 0.0.0.255 160.160.160.0
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 12.0
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
!--- Configure the IKE policy and preshared key for the
hub: crypto isakmp policy 1 authentication pre-share
crypto isakmp key cisco180 address 150.150.150.1 !---
Configure the IPSec parameters: !--- IPSec transform
set. crypto ipsec transform-set 180cisco esp-des esp-
md5-hmac !--- Crypto map definition for the hub site.
crypto map ETH0 18 ipsec-isakmp !--- Set the peer. set
peer 150.150.150.1 !--- IPSec transform set. set
transform-set 180cisco !--- Interesting traffic for peer
150.150.150.1 (hub site). match address 180 ! 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 !--- Apply crypto map on the interface.
crypto map ETH0 ! 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 no ip http server !--- Access list that
shows traffic to encryption !--- for the hub site
(dr_whoovie). access-list 180 permit ip 180.180.180.0
0.0.0.255 160.160.160.0 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 12.0
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
!--- Configure the IKE policy and preshared key for the
hub: crypto isakmp policy 1 authentication pre-share
crypto isakmp key cisco170 address 150.150.150.1 !---
Configure the IPSec parameters: !--- IPSec transform
set. crypto ipsec transform-set 170cisco esp-des esp-
md5-hmac !--- Crypto map definition for the hub site.
crypto map ETH0 17 ipsec-isakmp !--- Set the peer. set
peer 150.150.150.1 !--- IPSec transform set. set
transform-set 170cisco !--- Interesting traffic for peer
150.150.150.1 (hub site). match address 170 ! 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 !--- Apply crypto map on the interface.
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 no ip
http server !--- Access list that shows traffic to
encryption for !--- the hub site (dr_whoovie). access-
list 170 permit ip 170.170.170.0 0.0.0.255 160.160.160.0
0.0.0.255 dialer-list 1 protocol ip permit dialer-list 1
protocol ipx permit ! tftp-server flash:/c2500-jos56i-
l.120-7.T tftp-server flash:c2500-jos56i-l.120-7.T tftp-
server flash: ! 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

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 – отображает согласования ISAKMP на 1-м этапе.**
- **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

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