Настройка IPSec между тремя маршрутизаторами, использующими частные адреса

Содержание

Введение

Этот документ описывает полностью решетчатую конфигурацию с тремя маршрутизаторами то использование частные адреса. Пример иллюстрирует эти функции:

- Безопасное закрытие полезной нагрузки (ESP) - Стандарт шифрования данных (DES) только
- Предварительные ключи
- Частные сети позади каждого маршрутизатора: 192.168.1.0, 192.168.2.0, и 192.168.3.0
- политика ISAKMP и конфигурация криптокарты
- Туннельный трафик определен с **командами access-list и route-map**. В дополнение к Преобразованию адресов портов (PAT) Карты маршрутизации могут быть применены к непосредственной статической трансляции сетевых адресов (NAT) на релизе 12.2 программного обеспечения Cisco IOS (4) T2 и позже. Для получения дополнительной информации обратитесь к NAT - Способность Использовать Карты маршрутизации с Обзором характеристик Статических преобразований.

Примечание: Технология шифрования подлежит экспортному контролю. Это - ваша обязанность знать законы относительно экспорта технологии шифрования. Все вопросы, касающиеся экспортного контроля, можно присылать по электронной почте на адрес export@cisco.com.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Программное обеспечение Cisco IOS версии 12.3. (7) T.
- Маршрутизаторы Cisco настроены с IPSec.

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:

- Маршрутизатор 1
- Маршрутизатор 2
- Маршрутизатор 3

Маршрутизатор 1

```
Current configuration:
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router1
```

```
!
boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!

!--- Configure Internet Key Exchange (IKE) policy and !-- pre-shared keys for each peer. !--- IKE policy defined for peers. crypto isakmp policy 4 authentication pre-share !--- Pre-shared keys for different peers. crypto isakmp key xxxxxx1234 address 100.228.202.154 crypto isakmp key xxxxxx1234 address 200.154.17.130 ! ! !--- IPSec policies: crypto ipsec transform-set encrypt-des esp-des ! ! crypto map combined local-address Serial0 !--- Set the peer, transform-set and encryption traffic for tunnel peers. crypto map combined 20 ipsec-isakmp set peer 100.228.202.154 set transform-set encrypt-des match address 106 crypto map combined 30 ipsec-isakmp set peer 200.154.17.130 set transform-set encrypt-des match address 105 ! ! interface Serial0 ip address 100.232.202.210 255.255.255.252 ip nat outside serial restart-delay 0 !--- Apply the crypto map to the interface. crypto map combined ! interface FastEthernet0 ip address 192.168.1.1 255.255.255.0 ip nat inside ! ip classless ip route 0.0.0.0 0.0.0.0 100.232.202.209 no ip http server no ip http secure-server ! !--- Define traffic for NAT. ip nat inside source route-map nonat interface Serial0 overload !--- Access control list (ACL) that shows traffic to encrypt over the tunnel. access-list 105 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255 access-list 106 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 !--- ACL to avoid the traffic through NAT over the tunnel. access-list 150 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 access-list 150 deny ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255 !--- ACL to perform NAT on the traffic that does not go over the tunnel. access-list 150 permit ip 192.168.1.0 0.0.0.255 any !--- Do not perform NAT on the IPSec traffic. route-map nonat permit 10 match ip address 150 ! control-plane ! ! line con 0 line aux 0 line vty 0 4 ! ! end
```

Маршрутизатор 2

```
Current configuration:
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router2
!
boot-start-marker
boot-end-marker
!
!
```

```
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!

!--- Configure IKE policy and pre-shared keys for each
peer. !--- IKE policy defined for peers. crypto isakmp
policy 4 authentication pre-share !--- Pre-shared keys
for different peers. crypto isakmp key xxxxxx1234
address 100.228.202.154 crypto isakmp key xxxxxx1234
address 100.232.202.210 ! ! !--- IPSec policies. crypto
ipsec transform-set encrypt-des esp-des ! ! crypto map
combined local-address Ethernet1 !--- Set the peer,
transform-set and encryption traffic for tunnel peers.
crypto map combined 7 ipsec-isakmp set peer
100.232.202.210 set transform-set encrypt-des match
address 105 crypto map combined 8 ipsec-isakmp set peer
100.228.202.154 set transform-set encrypt-des match
address 106 ! ! ! interface Ethernet0 ip address
192.168.3.1 255.255.255.0 ip nat inside ! interface
Ethernet1 ip address 200.154.17.130 255.255.255.224 ip
nat outside !--- Apply the crypto map to the interface.
crypto map combined ! ip classless ip route 0.0.0.0
0.0.0.0 200.154.17.129 no ip http server no ip http
secure-server ! !--- Define traffic for NAT. ip nat
inside source route-map nonat interface Ethernet1
overload !--- ACL shows traffic to encrypt over the
tunnel. access-list 105 permit ip 192.168.3.0 0.0.0.255
192.168.1.0 0.0.0.255 access-list 106 permit ip
192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255 !--- ACL to
avoid the traffic through NAT over the tunnel. access-
list 150 deny ip 192.168.3.0 0.0.0.255 192.168.1.0
0.0.0.255 access-list 150 deny ip 192.168.3.0 0.0.0.255
192.168.2.0 0.0.0.255 !--- ACL to perform NAT on the
traffic that does not go over the tunnel. access-list
150 permit ip any any !--- Do not perform NAT on the
IPSec traffic. route-map nonat permit 10 match ip
address 150 ! ! ! control-plane ! ! line con 0 line aux
0 line vty 0 4 ! ! end
```

Конфигурация маршрутизатора 3

```
Current configuration:
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router3
!
boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
```

```
no ftp-server write-enable
!

!--- Configure IKE policy and pre-shared keys for each
peer. !--- IKE policy defined for peers. crypto isakmp
policy 4 authentication pre-share !--- Pre-shared keys
for different peers. crypto isakmp key xxxxxx1234
address 100.232.202.210 crypto isakmp key xxxxxx1234
address 200.154.17.130 ! ! !--- IPSec policies: crypto
ipsec transform-set encrypt-des esp-des ! ! !--- Set the
peer, transform-set and encryption traffic for tunnel
peers. crypto map combined local-address Serial0 crypto
map combined 7 ipsec-isakmp set peer 100.232.202.210 set
transform-set encrypt-des match address 106 crypto map
combined 8 ipsec-isakmp set peer 200.154.17.130 set
transform-set encrypt-des match address 105 ! !
interface Serial0 ip address 100.228.202.154
255.255.255.252 ip nat outside serial restart-delay 0 !-
-- Apply the crypto map to the interface. crypto map
combined ! interface FastEthernet0 ip address
192.168.2.1 255.255.255.0 ip nat inside ! ip classless
ip route 0.0.0.0 0.0.0.0 100.228.202.153 no ip http
server no ip http secure-server ! !--- Define traffic
for NAT. ip nat inside source route-map nonat interface
Serial0 overload !--- ACL that shows traffic to encrypt
over the tunnel. access-list 105 permit ip 192.168.2.0
0.0.0.255 192.168.3.0 0.0.0.255 access-list 106 permit
ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 !--- ACL
to avoid the traffic through NAT over the tunnel.
access-list 150 deny ip 192.168.2.0 0.0.0.255
192.168.3.0 0.0.0.255 access-list 150 deny ip
192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 !--- ACL to
perform NAT on the traffic that does not go over the
tunnel. access-list 150 permit ip 192.168.2.0 0.0.0.255
any !--- Do not perform NAT on the IPSec traffic. route-
map nonat permit 10 match ip address 150 ! ! ! control-
plane ! ! line con 0 line aux 0 line vty 0 4 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 engine connections active вЂ отображение зашифрованных и дешифрованных пакетов между узлами IPSec.
- show crypto isakmp sa — Показывает все текущие ассоциации безопасности (SA) протокола IKE для узла.
- show crypto ipsec sa– показывает настройки, используемые текущими ассоциациями безопасности IPSec.

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 применять команды отладки, ознакомьтесь с разделом "Важные сведения о командах отладки".

Примечание: Необходимо выполнить следующие команды отладки на обоих (одноранговых) маршрутизаторах IPSec. Очистка SA должна быть сделана на обоих узлах.

- **"debug crypto isakmp" - отображаются ошибки, возникающие в фазе 1.**
- **"debug crypto ipsec" – отображает ошибки в фазе 2.**
- **debug crypto engine– выводит информацию о криптографическом модуле.**
- *идентификатор соединения* **clear crypto connection** *[слот | rsm | vip]* — Завершает в настоящее время происходящий шифрованный сеанс. Шифрованные сеансы обычно завершаются когда времена сеанса. **Для получения значения connection-id используйте команду show crypto cisco connections.**
- **clear crypto isakmp** SA Фазы 1.
- **clear crypto sa** SA Фазы 2.

Дополнительные сведения

- Страница поддержки IPSec
- Техническая поддержка - Cisco Systems