IPSec Настройки - предварительные совместно используемые подстановочные ключи с Cisco Secure VPN Client и Config без режимов

Содержание

Введение

Этот пример конфигурации иллюстрирует маршрутизатор, настроенный для предварительных совместно используемых подстановочных ключей — все ПК - клиенты совместно используют общий ключ. Удаленный пользователь вводит сеть, поддерживая собственный IP-адрес; данные между ПК удаленного пользователя и маршрутизатором зашифрованы.

Предварительные условия

Требования

Для данного документа отсутствуют предварительные условия.

Используемые компоненты

Сведения в этом документе основаны на версиях оборудования и программного обеспечения, указанных ниже.

- Выпуск 12.2.8 программного обеспечения Cisco IOS. T1

- Версия 1.0 или 1.1 Cisco Secure VPN Client — поддержка закончена
- Маршрутизатор Cisco с DES или образом 3DES

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе с реальной сетью необходимо полностью осознавать возможные результаты использования всех команд.

Условные обозначения

Дополнительные сведения об условных обозначениях в документах см. Cisco Technical Tips Conventions.

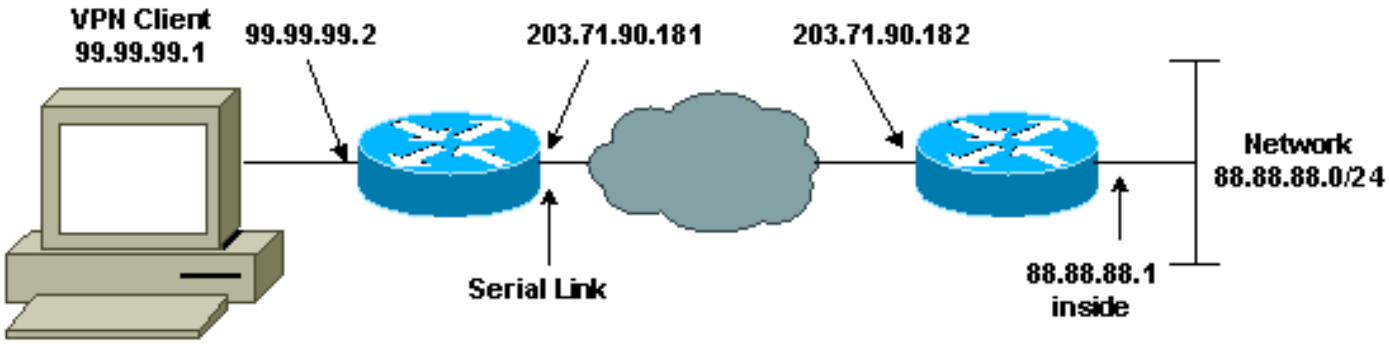
Настройка

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 данном документе используется сетевая установка, показанная на следующей схеме.



Конфигурации

В данном документе используются следующие конфигурации.

- Настройка маршрутизатора
- Конфигурация клиента VPN

Настройка маршрутизатора

```
Current configuration:
!
version 12.2

service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
```

```
hostname RTCisco
!
enable password hjwwkj
!
!
ip subnet-zero
ip domain-name cisco.com
ip name-server 203.71.57.242
!
!
crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key mysecretkey address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set mypolicy esp-des esp-md5-hmac
!
crypto dynamic-map dyna 10
set transform-set mypolicy
!
crypto map test 10 ipsec-isakmp dynamic dyna
!
!
interface Serial0
ip address 203.71.90.182 255.255.255.252
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
crypto map test
!
interface Ethernet0
ip address 88.88.88.1 255.255.255.0
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 203.71.90.181
!
!
line con 0
transport input none
line aux 0
transport input all
line vty 0 4
password cscscs
login
!
end
```

Конфигурация клиента VPN

```
Current configuration:
!
version 12.2

service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RTCisco
!
enable password hjwwkj
!
!
ip subnet-zero
```

```
ip domain-name cisco.com
ip name-server 203.71.57.242
!
!
crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key mysecretkey address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set mypolicy esp-des esp-md5-hmac
!
crypto dynamic-map dyna 10
set transform-set mypolicy
!
crypto map test 10 ipsec-isakmp dynamic dyna
!
!
interface Serial0
ip address 203.71.90.182 255.255.255.252
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
crypto map test
!
interface Ethernet0
ip address 88.88.88.1 255.255.255.0
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 203.71.90.181
!
!
line con 0
transport input none
line aux 0
transport input all
line vty 0 4
password cscscs
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 isakmp sa отображает сопоставления безопасности (SA), соответствующие первому этапу.**
- **show crypto ipsec sa** сопоставления безопасности Фазы 1 и прокси, инкапсуляцию, шифрование, декапсуляцию и информацию для расшифровки.
- **show crypto engine connection active** — Показывают текущие соединения и информацию относительно зашифрованных и расшифрованных пакетов.

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.

Примечание: Необходимо очистить сопоставления безопасности на обоих узлах. Выполните команды маршрутизатора в запрещающем режиме.

Примечание: Необходимо выполнить эти отладки на обоих Узлах IPsec.

- **"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.**
- **clear crypto isakmp —Очищает связи безопасности в фазе 1.**
- **clear crypto sa – удаляет связи безопасности, соответствующие второму этапу.**

Дополнительные сведения

- Страница поддержки IPSec
- Страницы технической поддержки VPN 3000 Client
- Техническая поддержка - Cisco Systems