

# IOS Легкая VPN: IPsec по Поддержке TCP на любом порте с Примером конфигурации Cisco Configuration Professional

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Настройка](#)

[Устранение неполадок](#)

[Дополнительные сведения](#)

## Введение

Этот документ описывает, как настроить Легкую VPN (EzVPN) сервер и клиент для поддержки Cisco, Туннелирующей Протокол управления (сTCP). Этот пример конфигурации демонстрирует конфигурацию для IPsec по TCP на любом порту. Эта функция представлена в Выпуске 12.4 (9) T программного обеспечения Cisco IOS и теперь поддерживается в Cisco IOS Software Release 12.4 (20) T и позже.

Cisco, Туннелирующая, Протокол управления позволяет клиентам VPN действовать в средах, где не разрешен стандарт ESP протокол (порт 50) или протокол IKE (порт 500 UDP). По ряду причин межсетевые экраны не могут разрешить ESP или трафик IKE, который блокирует связь VPN. сTCP решает эту проблему, потому что это инкапсулирует ESP и трафик IKE в заголовке TCP так, чтобы межсетевые экраны не видели его.

## Предварительные условия

### Требования

Гарантируйте, что ваша Легкая VPN (EzVPN) сервер настроена для клиентских соединений. Именуйте [маршрутизатор Cisco IOS как Сервер Easy VPN Использование Примера конфигурации Cisco Configuration Professional](#) для получения информации о том, как настроить маршрутизатор Cisco IOS как Сервер Easy VPN.

### Используемые компоненты

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

- Маршрутизатор Cisco 1841 с программным обеспечением Cisco IOS версии 12.4(20)T
- Версия 2.1 CP Cisco

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

[Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.](#)

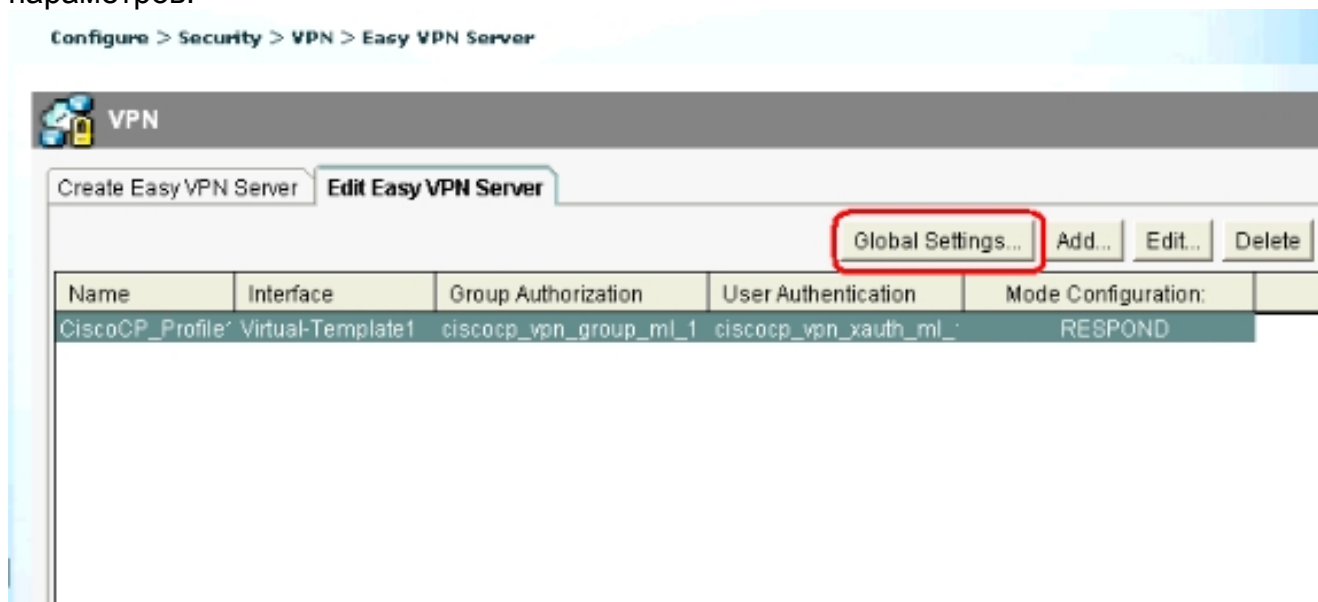
## Настройка

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

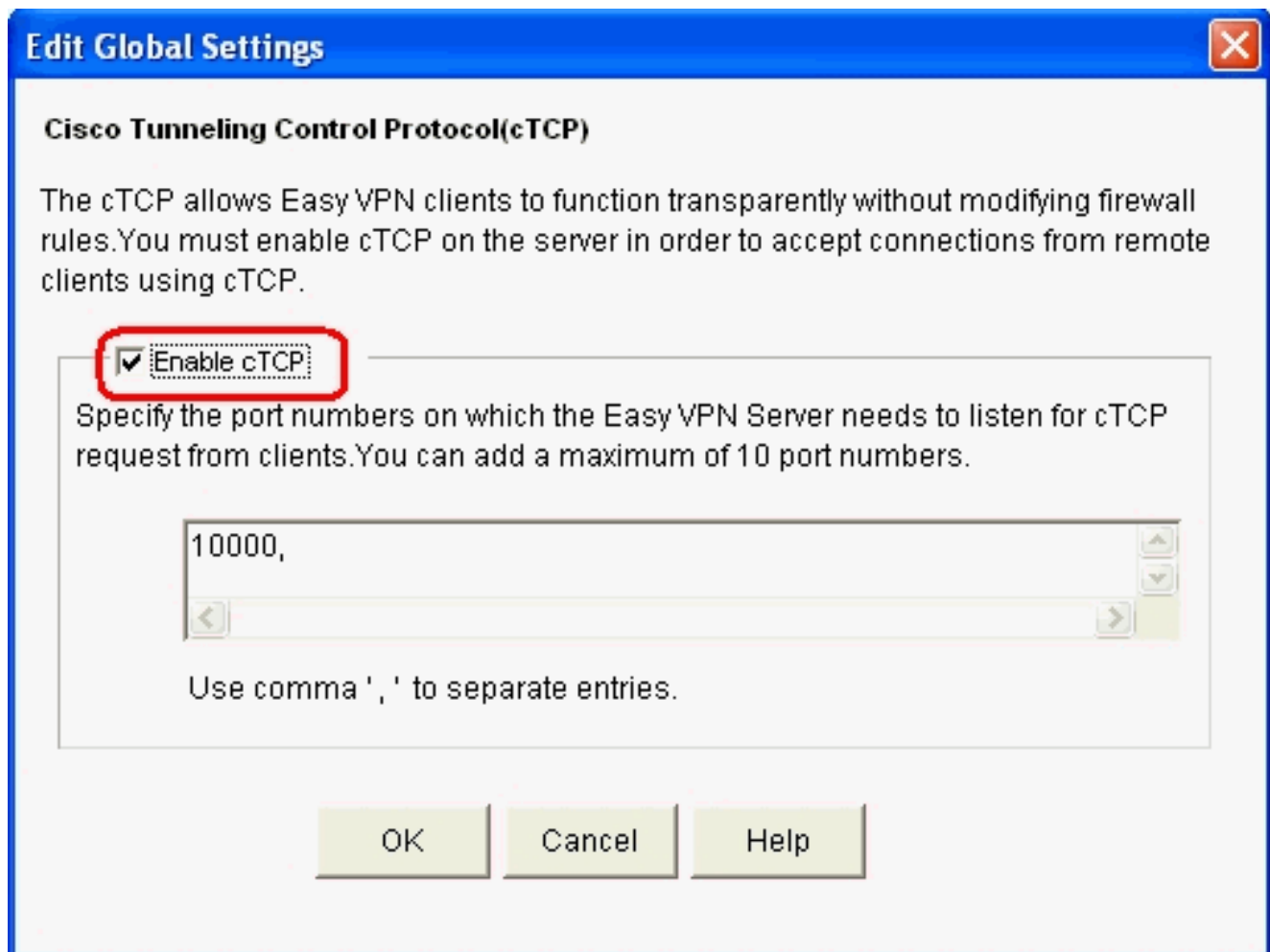
### Маршрутизатор Cisco IOS как сервер Easy VPN

Выполните эти шаги для настройки маршрутизатора Cisco IOS (Сервер Easy VPN) для поддержки sTCP на порту 10000:

1. Выберите **> Security Configure > VPN > Сервер Easy VPN** и нажмите **Global Settings** для редактирования Глобальных параметров.



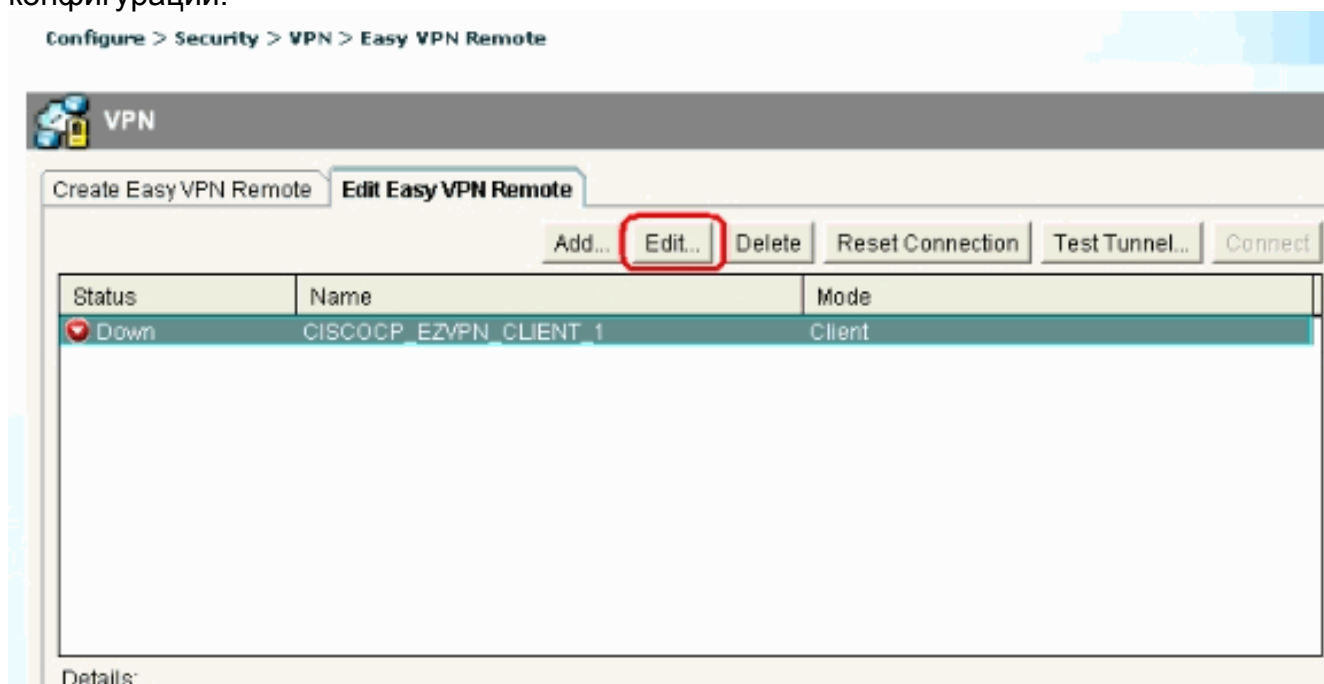
2. Проверьте **Разрешение sTCP** флажок для включения sTCP. **Примечание:** Номер порта 10000 используется по умолчанию. При необходимости номер порта может быть изменен.



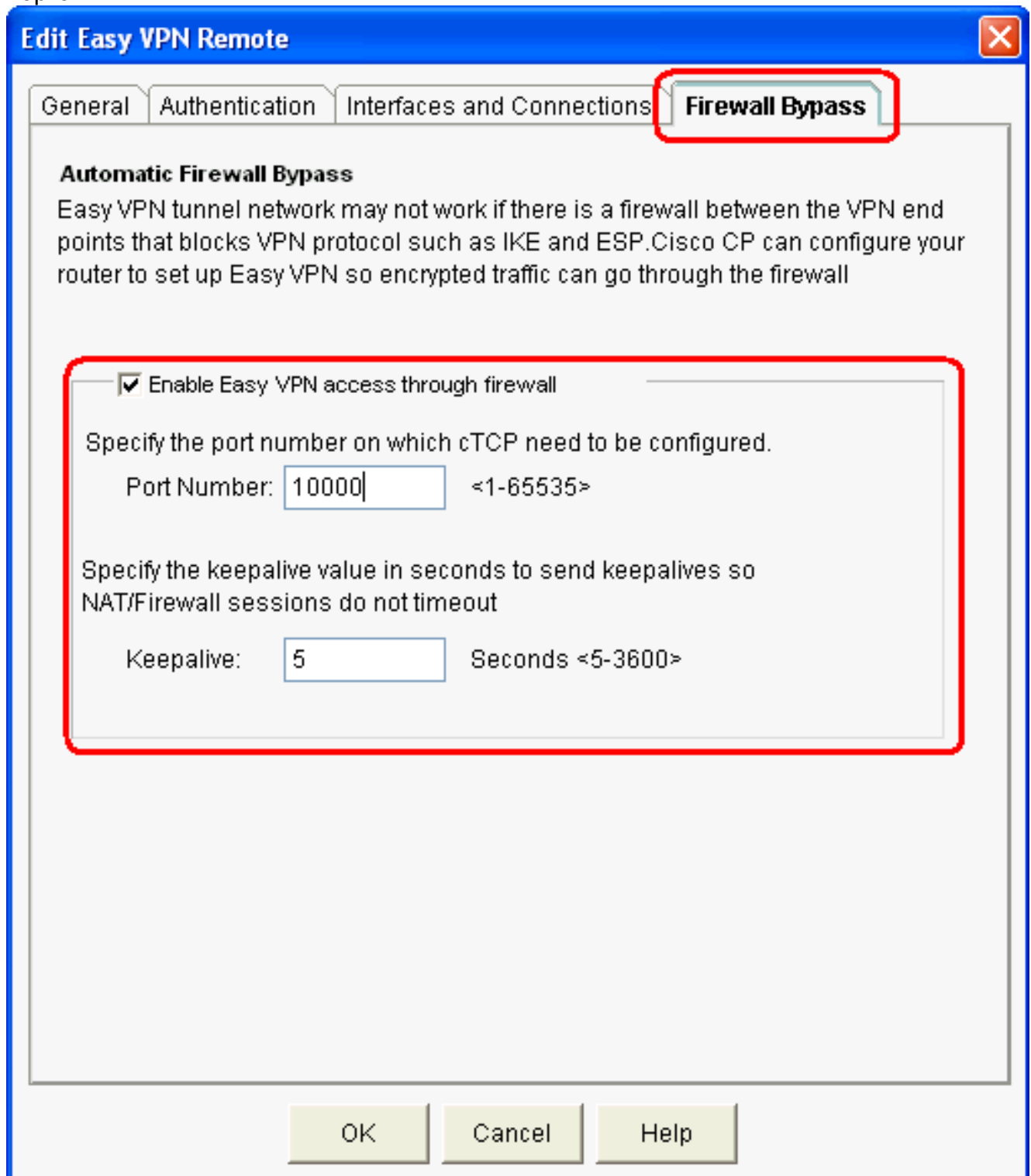
## [Маршрутизатор Cisco IOS как клиент Easy VPN](#)

Выполните следующие действия:

1. Выберите **Security Configure > VPN > Easy VPN Remote** и нажмите **Edit** для редактирования клиентских параметров настройки для cTCP конфигурации.



2. Нажмите вкладку **Firewall Bypass**, и под **Автоматическим Межсетевым экраном Обход** разделяет и задает время **Номера порта** и **Поддержки активности** в секундах. Гарантируйте, что флажок рядом с **Включает Легкий доступ VPN через межсетевой экран**, проверен. **Примечание:** Номер порта 10000 используется по умолчанию. При необходимости номер порта может быть изменен. Согласуйте с удаленным администратором для проверки, какой номер порта используется на Сервере Easy VPN, так как сервер и клиент должны использовать номер того же порта.



The screenshot shows the 'Edit Easy VPN Remote' dialog box with the 'Firewall Bypass' tab selected. The 'Automatic Firewall Bypass' section is active, and the 'Enable Easy VPN access through firewall' checkbox is checked. The 'Port Number' is set to 10000, and the 'Keepalive' value is set to 5 seconds. The dialog box has a blue title bar and a close button in the top right corner. The 'Firewall Bypass' tab is highlighted with a red box, and the configuration area is also highlighted with a red box.

**Edit Easy VPN Remote**

General Authentication Interfaces and Connections **Firewall Bypass**

**Automatic Firewall Bypass**

Easy VPN tunnel network may not work if there is a firewall between the VPN end points that blocks VPN protocol such as IKE and ESP. Cisco CP can configure your router to set up Easy VPN so encrypted traffic can go through the firewall

Enable Easy VPN access through firewall

Specify the port number on which cTCP need to be configured.

Port Number:  <1-65535>

Specify the keepalive value in seconds to send keepalives so NAT/Firewall sessions do not timeout

Keepalive:  Seconds <5-3600>

OK Cancel Help

3. Нажмите **ОК** для завершения конфигурации.

## [Устранение неполадок](#)

Нет никаких сведений об устранении проблем, доступных для этой конфигурации.

## [Дополнительные сведения](#)

- [Вопросы и ответы Cisco Easy VPN](#)
- [Запросы комментариев \(RFC\)](#)
- [Cisco Systems – техническая поддержка и документация](#)