Cisco Packet Tracer. Межсетевые экраны на сервере и списки контроля доступа на маршрутизаторе

Таблица адресации

Устройство	Частный IP-адрес	Общедоступный IP-адрес	Маска подсети	Сайт
Веб-сервер	—	209.165.201.10	255.255.255.0	Интернет

Задачи

Часть 1. Подключение к веб-серверу

Часть 2. Предотвращение незашифрованных сеансов HTTP

Часть 3. Доступ к межсетевому экрану на сервере электронной почты

Общие сведения

В этом упражнении вы получите доступ к пользователю в узле Metropolis и подключитесь по протоколам HTTP и HTTPS к удаленному веб-серверу. Настройка IP-адресации, сети и сервисов уже завершена. С помощью клиентского устройства в узле Metropolis вы протестируете подключение к удаленному веб-серверу. Чтобы обеспечить защиту узла Metropolis, вы запретите незашифрованное соединение с внешними веб-сеансами.

Часть 1: Подключитесь к веб-серверу.

Шаг 1: Установите доступ к веб-серверу HQ Internet с ПК пользователя Sally по протоколу HTTP.

a. Выберите узел **Metropolis Bank HQ** и выберите ПК **Sally**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Web Browser** (Браузер).

c. Введите URL-адрес **http://www.cisco.corp** и нажмите **Go**.

d. Щелкните ссылку **Login Page**.

Почему пользователь должен быть обеспокоен при отправке информации через этот веб-сайт?

Потому что данные передаются через незащищённый протокол http

Шаг 2: Установите доступ к веб-серверу HQ Internet с компьютера пользователя Sally по протоколу HTTPS.

a. Откройте **веб-обозреватель** на компьютере Sally's.

b. Введите URL-адрес **https://www.cisco.corp** и нажмите Go.

c. Щелкните ссылку **Login Page**.

У пользователя меньше поводов для беспокойства при отправке информации через этот веб-сайт. Почему?

Потому что данные передаются через защищённый протокол https

d. Закройте компьютер пользователя **Sally**.

Часть 2: Предотвращение незашифрованных сеансов HTTP.

Шаг 1: Настройте маршрутизатор HQ_Router.

a. Откройте объект **Metropolis Bank HQ** и выберите маршрутизатор **HQ_Router**.

b. Нажмите вкладку **CLI** и нажмите **Enter**.

c. Для входа в систему маршрутизатора используйте пароль **cisco**.

d. Введите команду **enable**, а затем **configure terminal** для доступа к режиму глобальной настройки.

Чтобы предотвратить передачу незашифрованного HTTP-трафика через головной маршрутизатор, сетевые администраторы могут создать и развернуть списки контроля доступа (ACL).

Следующие команды выходят за рамки этого курса. Они используются для демонстрации возможности предотвращения передачи незашифрованного трафика через маршрутизатор HQ_Router.

e. В командной строке **HQ_Router**(config)**#** в режиме глобальной настройки скопируйте и вставьте показанную ниже конфигурацию списка контроля доступа в **HQ_Router**.

```
!
access-list 101 deny tcp any any eq 80
access-list 101 permit ip any any
!
int gig0/0
ip access-group 101 in
!
end
```

f. Закройте маршрутизатор **HQ_Router**.

Шаг 2: Установите доступ к веб-серверу HQ Internet с ПК пользователя Sally по протоколу HTTP.

a. В узле **Metropolis Bank HQ** нажмите ПК пользователя **Sally**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Web Browser** (Браузер).

c. Введите URL-адрес **http://www.cisco.corp** и нажмите **Go**.

Может ли компьютер пользователя **Sally** получить доступ к веб-серверу HQ Internet по протоколу HTTP?

Нет, т.к. трафик, получаемый по порту 80 был ограничен

Шаг 3: Установите доступ к веб-серверу HQ Internet с компьютера пользователя Sally по протоколу HTTPS.

a. Откройте **веб-обозреватель** на компьютере Sally's.

b. Введите URL-адрес **https://www.cisco.corp** и нажмите Go.

Может ли компьютер пользователя Sally получить доступ к веб-серверу HQ Internet по протоколу HTTP?

Да, потому что https трафик использует порт 443, который не был ограничен

c. Закройте компьютер пользователя **Sally**.

Часть 3: Доступ к межсетевому экрану на сервере электронной почты.

a. В узле **Metropolis Bank HQ** нажмите сервер **Email**.

b. Нажмите вкладку **Desktop** (Рабочий стол) и выберите **Firewall** (Межсетевой экран). Правила межсетевого экрана не заданы.

Чтобы предотвратить отправку или получение через сервер электронной почты трафика, не связанного с ней, сетевые администраторы могут создавать правила межсетевого экрана непосредственно на сервере. Либо, как показано ранее, можно использовать списки контроля доступа (ACL) на сетевом устройстве, например, маршрутизаторе.

Предлагаемый способ подсчета баллов

Раздел упражнений	Вопрос	Максимальное количество баллов	Заработанные баллы
Часть 1. Подключение к веб-серверу	Шаг 1	15	
	Шаг 2	15	
Часть 2. Предотвращение незашифрованных сеансов HTTP	Шаг 2	15	
	Шаг 3	15	
	Вопросы	**60**	
	Балл Packet Tracer	**40**	
	Общее число баллов	**100**	