**Пояснение, почему мало баллов:**

**Скорее всего какая-то ошибка в PKT с названием, т.к он не засчитывает создание списка контроля доступа, но засчитывает применение его к интерфейсу**

**Packet Tracer. Настройка расширенных списков контроля доступа. Сценарий 2**

**Таблица адресации**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Устройство** | **Интерфейс** | **IP-адрес** | **Маска подсети** | **Шлюз по умолчанию** |
| RT1 | G0/0 | 172.31.1.126 | 255.255.255.224 | — |
| *RT1* | S0/0/0 | 209.165.1.2 | 255.255.255.252 | *—* |
| PC1 | NIC | 172.31.1.101 | 255.255.255.224 | 172.31.1.126 |
| PC2 | NIC | 172.31.1.102 | 255.255.255.224 | 172.31.1.126 |
| PC3 | NIC | 172.31.1.103 | 255.255.255.224 | 172.31.1.126 |
| Server1 | NIC | 64.101.255.254 | *Пустой экран* | *Пустой экран* |
| Server2 | NIC | 64.103.255.254 | *Пустой экран* | *пусто* |

**Задачи**

**Часть 1. Настройка именованного расширенного списка контроля доступа**

**Часть 2. Применение и проверка расширенного списка контроля доступа**

**Общие сведения/сценарий**

В этом сценарии определенным устройствам в локальной сети разрешен доступ к различным сервисам на серверах в Интернете.

**Инструкция**

**Часть 1.Настройка именованного расширенного списка контроля доступа**

Используйте один именованный список контроля доступа для реализации следующей политики.

         Блокируйте доступ по протоколам HTTP и HTTPS от **PC1** к серверам **Server1** и **Server2.**Серверы находятся в облаке, и известны только их IP-адреса.

         Блокируйте доступ по FTP от **PC2** к **Server1** и **Server2**.

         Блокируйте доступ по ICMP от **PC3** к **Server1** и **Server2**.

**Примечание.** Для правильной оценки вы должны настроить записи списка контроля доступа в порядке, указанном ниже.

**Шаг 1.Запретите узлу PC1 доступ к сервисам HTTP и HTTPS на серверах Server1 и Server2.**

a.     Создайте расширенный именованный список контроля доступа по протоколу IP, который запретит узлу **PC1** доступ к сервисам HTTP и HTTPS серверов **Server1** и **Server2**. Требуется четыре оператора управления доступом.

Вопрос:

Какая команда запускает настройку расширенного списка доступа с именем **ACL**?

*Откройте окно конфигурации*

б.     Запишите выражение, запрещающее доступ от **PC1** к **Server1** только для HTTP (порт 80). Обратитесь к таблице адресов для получения IP-адреса **PC1** и **Server1**.

RT1(config-ext-nacl)# **deny tcp host 172.31.1.101 host 64.101.255.254 eq 80**

в.     Запишите выражение, запрещающее доступ от **PC1** к **Server1** только для HTTPS (порт 443).

RT1(config-ext-nacl)# **deny tcp host 172.31.1.101 host 64.101.255.254 eq 443**

г.     Запишите выражение, запрещающее доступ от **PC1** к **Server2** только для HTTP. Обратитесь к таблице адресов для получения IP-адреса **Server2 .**

RT1(config-ext-nacl)# **deny tcp host 172.31.1.101 host 64.103.255.254 eq 80**

д.     Запишите выражение, запрещающее доступ от **PC1** к **Server2** только для HTTPS.

RT1(config-ext-nacl)# **deny tcp host 172.31.1.101 host 64.103.255.254 eq 443**

**Шаг 2. Запретите узлу PC2 доступ к сервисам FTP на серверах Server1 и Server2.**

Обратитесь к таблице адресов для получения IP-адреса **PC2**.

a.     Запишите выражение, запрещающее доступ от **PC2** к **Server1** только для FTP (порт 21).

RT1(config-ext-nacl)# **deny tcp host 172.31.1.102 host 64.101.255.254 eq 21**

б.     Запишите выражение, запрещающее доступ от **PC2** к **Server2** только для FTP (порт 21).

RT1(config-ext-nacl)# **deny tcp host 172.31.1.102 host 64.103.255.254 eq 21**

**Шаг 3. Запретите узлу PC3 отправлять эхо-запросы к Server1 и Server2.**

Обратитесь к таблице адресов для получения IP-адреса **PC3.**

a.     Создайте правило, запрещающее доступ по ICMP от **PC3** к серверу **Server1**.

RT1(config-ext-nacl)# **deny icmp host 172.31.1.103 host 64.101.255.254**

б.     Создайте правило, запрещающее доступ по ICMP от **PC3** к серверу **Server2**.

RT1(config-ext-nacl)# **deny icmp host 172.31.1.103 host 64.103.255.254**

**Шаг 4.Разрешите весь остальной IP-трафик.**

По умолчанию список контроля доступа запрещает весь трафик, не соответствующий ни одному правилу в списке. Введите команду, разрешающую весь трафик, который не соответствует ни одному из настроенных инструкций списка доступа.

**Шаг 5. Проверьте конфигурацию списка доступа, прежде чем применить его к интерфейсу.**

Перед применением списка доступа необходимо проверить конфигурацию, чтобы убедиться в отсутствии опечаток и правильности инструкций. Чтобы просмотреть текущую конфигурацию списка доступа, используйте команду **show access-lists** или команду **show running-config.**

**RT1# show access-lists**

**Extended IP access list ACL**

**10 deny tcp host 172.31.1.101 host 64.101.255.254 eq www**

**20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443**

**30 deny tcp host 172.31.1.101 host 64.103.255.254 eq www**

**40 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443**

**50 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp**

**60 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp**

**70 deny icmp host 172.31.1.103 host 64.101.255.254**

**80 deny icmp host 172.31.1.103 host 64.103.255.254**

**90 permit ip any any**

**RT1# show running-config | begin access-list**

**ip access-list extended ACL**

**deny tcp host 172.31.1.101 host 64.101.255.254 eq www**

**deny tcp host 172.31.1.101 host 64.101.255.254 eq 443**

**deny tcp host 172.31.1.101 host 64.103.255.254 eq www**

**deny tcp host 172.31.1.101 host 64.103.255.254 eq 443**

**deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp**

**deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp**

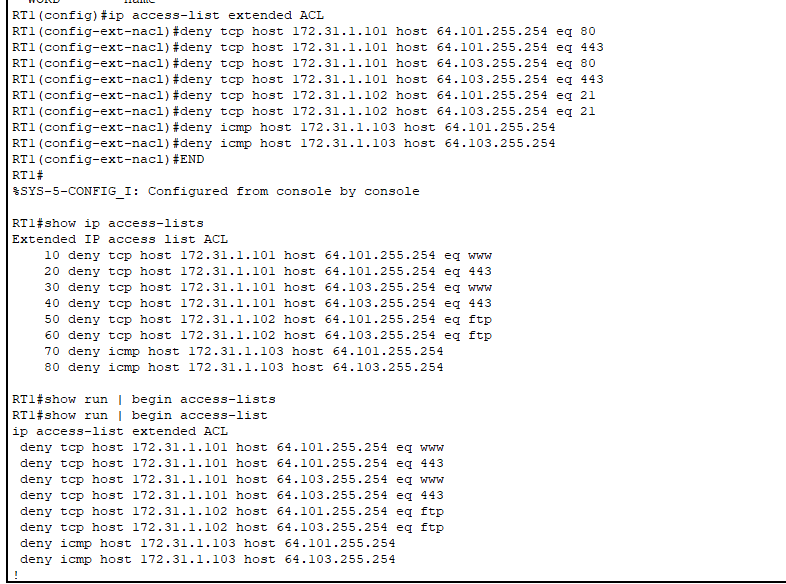
**deny icmp host 172.31.1.103 host 64.101.255.254**

**deny icmp host 172.31.1.103 host 64.103.255.254**

**permit ip any any**

***Закройте окно настройки.***

**Примечание. Разница между выводами команды show access-lists и выводами команды show running-config заключается в том, что команда show access-lists включает порядковые номера, назначенные операторы конфигурации. Эти порядковые номера позволяют редактировать, удалять и вставлять отдельные строки в конфигурации списка доступа. Последовательные номера также определяют порядок обработки отдельных операторов управления доступом, начиная с наименьшего порядкового номера.**

****

**Часть 2. Применение и проверка расширенного списка контроля доступа**

**Трафик, подлежащий фильтрации, поступает из сети 172.31.1.96/27 и предназначен для удаленных сетей. Подходящее размещение списка контроля доступа также зависит от взаимосвязей трафика в отношении RT1. Как правило, списки расширенного доступа должны размещаться на интерфейсе, близком к источнику трафика.**

**Шаг 1.Примените список контроля доступа на соответствующем интерфейсе и в правильном направлении.**

**Примечание. В реальной операционной сети непроверенный ACL никогда не должен применяться к активному интерфейсу. Это не является хорошей практикой и может нарушить работу сети.**

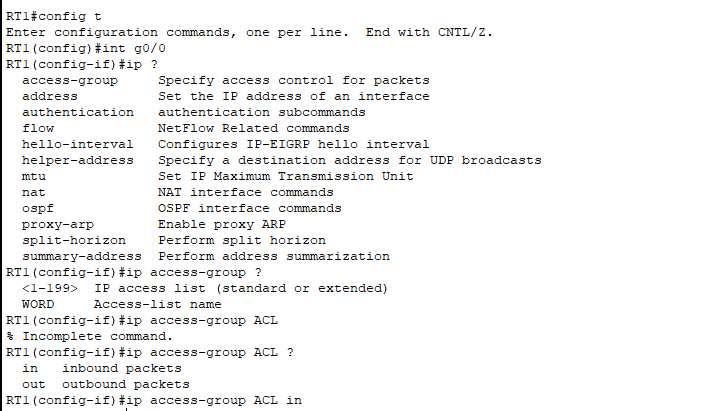
Вопрос:

**На каком интерфейсе должен быть применен именованный ACL и в каком направлении?**

**G0/0/0 in**

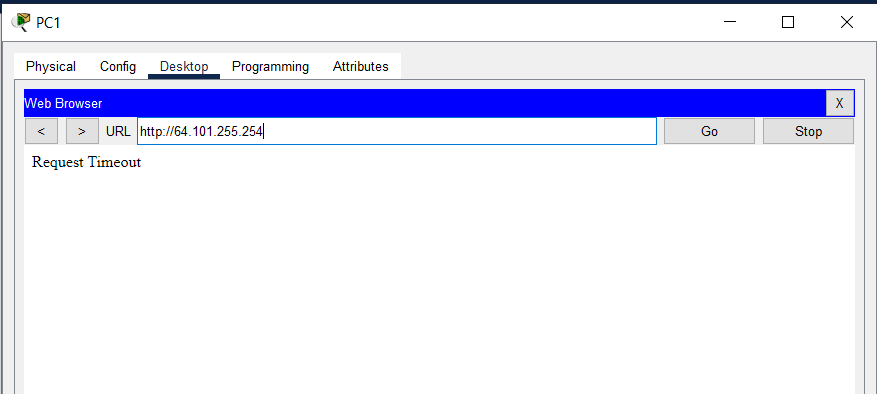
***Откройте окно конфигурации***

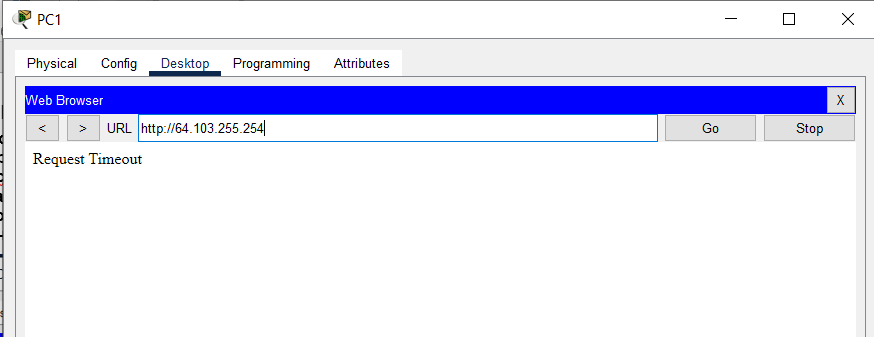
**Войдите в режим настройки интерфейса и примените ACL-список.**

****

**Шаг 2. Протестируйте доступ для каждого ПК.**

1. **Получите доступ к веб-сайтам Server1 и Server2, используя веб-браузер PC1. Используйте протоколы HTTP и HTTPS. Используйте команду show access-lists, чтобы просмотреть, какой оператор списка доступа разрешен или запрещен трафик. Выходные данные команды show access-lists показывают количество пакетов, соответствующих каждой инструкции с момента последнего очистки счетчиков или перезагрузки маршрутизатора.**



****

**Примечание. Чтобы очистить счетчики в списке доступа, используйте команду clear access-list counters.**

**RT1#show ip access-lists**

**Extended IP access list ACL**

**10 deny tcp host 172.31.1.101 host 64.101.255.254 eq www (12 match(es))**

**20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443 (12 match(es))**

**30 deny tcp host 172.31.1.101 host 64.103.255.254 eq www**

**40 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443**

**50 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp**

**60 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp**

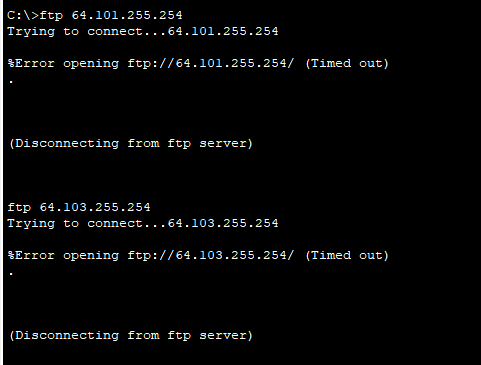
**70 deny icmp host 172.31.1.103 host 64.101.255.254**

**80 deny icmp host 172.31.1.103 host 64.103.255.254**

**90 permit ip any any**

***Закройте окно настройки.***

**б.     Доступ к FTP серверов Server1 и Server2 с помощью PC1. Имя пользователя и пароль — cisco.**

****

**в.     Запустите Ping до Server1 и Server2 с PC1.**

**Пинг не проходит**

**г.     Повторите шаги 2a–2c для узлов PC2 и PC3, чтобы проверить правильную работу списка контроля доступа.**

***Конец документа***

Для PC2 и PC3 ситуация идентична