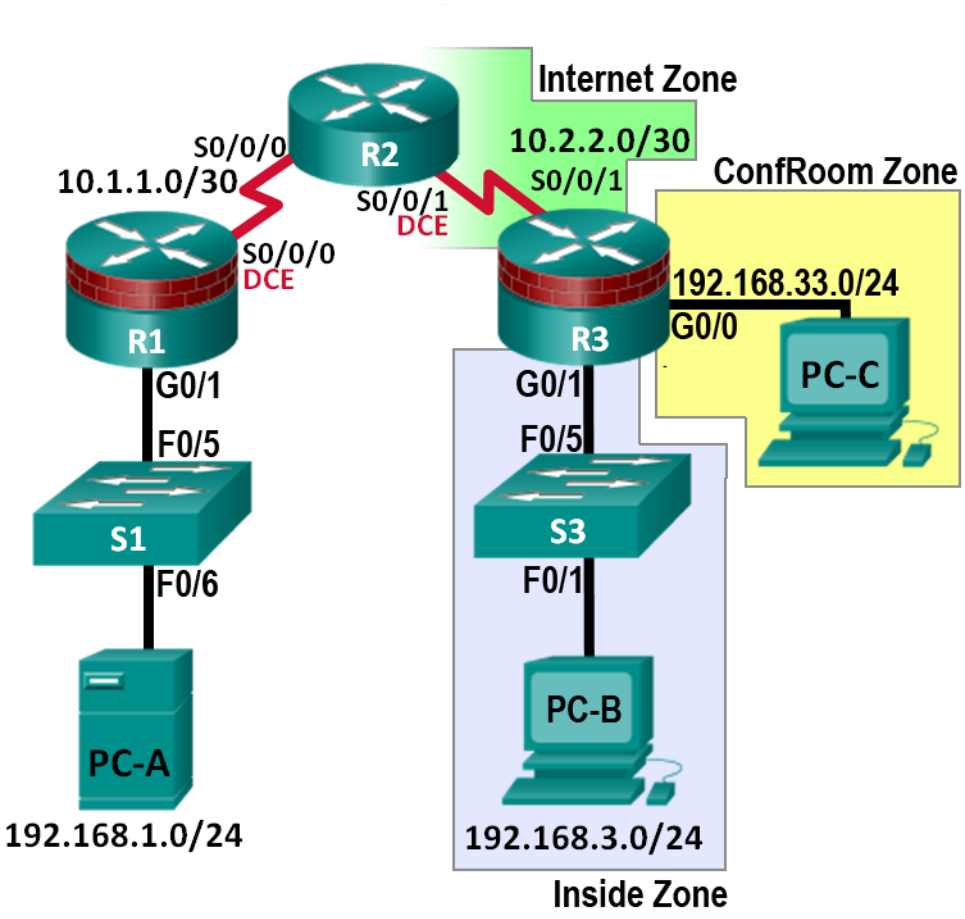
CCNA Security

Лабораторная работа. Настройка зональных межсетевых экранов

Топология



Примечание. В устройствах ISR G1 используются интерфейсы FastEthernet, а не GigabitEthernet.

Таблица IP-адресов

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию	Порт коммутатора
R1	G0/1	192.168.1.1	255.255.255.0	Н/П	S1 F0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Н/П	Н/П
R2	S0/0/0	10.1.1.2	255.255.255.252	Н/П	Н/П
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Н/П	Н/П
R3	G0/0	192.168.33.1	255.255.255.0	Н/П	Н/П
	G0/1	192.168.3.1	255.255.255.0	Н/П	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	Н/П	Н/П
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-B	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/1
PC-C	NIC	192.168.33.3	255.255.255.0	192.168.33.1	Н/П

Задачи

Часть 1. Основная конфигурация маршрутизаторов

- Настройте имена хостов, IP-адреса интерфейсов и пароли для доступа.
- Настройте статические маршруты для организации сквозной связи.

Часть 2. Настройка зонального межсетевого экрана (ZPF)

- Используйте CLI для настройки зонального межсетевого экрана.
- Используйте CLI для проверки конфигурации.

Общие сведения

В наиболее простых межсетевых экранах Cisco IOS используются списки контроля доступа (ACL) для фильтрации IP-трафика и отслеживания заданных шаблонов трафика. Традиционные межсетевые экраны Cisco IOS основаны на применении списков ACL.

Более новые межсетевые экраны Cisco IOS используют зональный подход, основанный на функциях интерфейса, а не списках контроля доступа. Зональный межсетевой экран (ZPF) позволяет применять различные политики инспектирования для групп хостов, подключенных к одному и тому же интерфейсу маршрутизатора. Его можно настроить для обеспечения расширенного и очень подробного контроля с учетом конкретного протокола. Он запрещает трафик между разными зонами межсетевого экрана благодаря применению политики по умолчанию deny-all. ZPF может применяться для нескольких интерфейсов с одинаковыми или разными требованиями по безопасности.

В данной лабораторной работе вы построите сеть, содержащую несколько маршрутизаторов, настроите маршрутизаторы и хосты, а также зональный межсетевой экран с использованием командного интерфейса Cisco IOS (CLI).

Примечание. В данной лабораторной работе используются команды и выходные данные для маршрутизатора Cisco 1941 с ПО Cisco IOS версии 15.4(3)M2 (UniversalK9-M). Допускается использование других маршрутизаторов и версий Cisco IOS. См. сводную таблицу по интерфейсам маршрутизаторов в конце этой лабораторной работы для определения идентификаторов интерфейсов с учетом оборудования в лаборатории. В зависимости от модели маршрутизатора и версии Cisco IOS, доступные команды и выходные данные могут отличаться от указанных в данной лабораторной работе.

Примечание. Убедитесь, что маршрутизаторы и коммутаторы сброшены и не имеют конфигурацию запуска.

Необходимые ресурсы

- 3 маршрутизатора (Cisco 1941 с образом Cisco IOS Release 15.4(3)M2 или аналогичным)
- 2 коммутатора (Cisco 2960 или аналогичный)
- 3 ПК (Windows Vista или 7)
- Последовательные кабели и кабели Ethernet, как показано на топологической схеме
- Консольные кабели для настройки сетевых устройств Cisco

Часть 1: Основная конфигурация маршрутизаторов

В части 1 этой лабораторной работы вы создадите топологию сети и настроите основные параметры, такие как IP-адреса интерфейсов, статическая маршрутизация, доступ к устройствам и пароли.

Примечание. На маршрутизаторах R1, R2 и R3 должны быть выполнены все задачи. Процедуры показаны только для одного из маршрутизаторов.

Шаг 1: Подключите сетевые кабели, как показано на топологической схеме.

Присоедините устройства, как показано на топологической схеме, и установите необходимые кабельные соединения.

Шаг 2: Настройте основные параметры для каждого маршрутизатора.

a. Задайте имена хостов, как показано на топологической схеме.

b. Настройте IP-адреса, как показано в таблице IP-адресов.

c. Настройте тактовую частоту последовательных интерфейсов маршрутизаторов с помощью последовательного DCE-кабеля.

```
R2(config)# interface S0/0/0
R2(config-if)# clock rate 64000
```

Шаг 3: Отключите поиск DNS.

Чтобы предотвратить попытки маршрутизатора неправильно интерпретировать введенные команды, отключите функцию DNS-поиска.

```
R2(config)# no ip domain-lookup
```

Шаг 4: Настройте статические маршруты на маршрутизаторах R1, R2 и R3.

a. Чтобы обеспечить сквозную связь по IP, на маршрутизаторах R1, R2 и R3 необходимо настроить соответствующие статические маршруты. R1 и R3 – это маршрутизаторы-заглушки. Поэтому для них необходимо указать только маршрут по умолчанию к маршрутизатору R2. Маршрутизатор R2, выполняющий роль ISP, должен знать, как достичь внутренних сетей маршрутизаторов R1 и R3: это необходимо для обеспечения сквозной связи по IP. Ниже указаны настройки статических маршрутов для маршрутизаторов R1, R2 и R3. На маршрутизаторе R1 используйте следующую команду:

```
R1(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2
```

b. На маршрутизаторе R2 используйте следующие команды:

```
R2(config)# ip route 192.168.1.0 255.255.255.0 10.1.1.1
R2(config)# ip route 192.168.3.0 255.255.255.0 10.2.2.1
R2(config)# ip route 192.168.33.0 255.255.255.0 10.2.2.1
```

c. На маршрутизаторе R3 используйте следующую команду:

```
R3(config)# ip route 0.0.0.0 0.0.0.0 10.2.2.2
```


Шаг 5: Настройте параметры IP для хоста.

Настройте статический IP-адрес, маску подсети и шлюз по умолчанию для компьютеров PC-A, PC-B и PC-C, как показано в таблице IP-адресов.

Шаг 6: Проверьте базовую связь по сети.

a. Отправьте эхо-запрос с маршрутизатора R1 на R3.

Если запрос был выполнен с ошибкой, проведите диагностику основных параметров устройства перед тем, как продолжить.

b. Отправьте эхо-запрос с компьютера PC-A в локальной сети маршрутизатора R1 на компьютер PC-C в локальной сети маршрутизатора R3.

Если запрос был выполнен с ошибкой, проведите диагностику основных параметров устройства перед тем, как продолжить.

Примечание. Если эхо-запросы с компьютера PC-A на PC-C выполняются без ошибок, это означает наличие сквозной связи по IP . Если эхо-запросы были выполнены с ошибкой, но интерфейсы устройств находятся в состоянии UP и IP-адреса заданы верно, воспользуйтесь командами **show interface**, **show ip interface** и **show ip route**, чтобы определить источник проблемы.

Шаг 7: Настройте учетную запись пользователя, шифрованные пароли и криптографические ключи для SSH.

Примечание. В данной задаче установлена минимальная длина пароля в 10 символов, однако для облегчения процесса выполнения лабораторной работы пароли были относительно упрощены. В рабочих сетях рекомендуется использовать более сложные пароли.

a. Используйте команду **security passwords**, чтобы задать минимальную длину пароля в 10 символов.

```
R1(config)# security passwords min-length 10
```

b. Настройте доменное имя.

```
R1(config)# ip domain-name ccnasecurity.com
```

c. Настройте криптографические ключи для SSH.

```
R1(config)# crypto key generate rsa general-keys modulus 1024
```

d. Создайте учетную запись пользователя admin01, используя **algorithm-type scrypt** для шифрования и пароль cisco12345.

```
R1(config)# username admin01 algorithm-type scrypt secret cisco12345
```

e. Настройте линию 0 консоли на использование локальной базы данных пользователей для входа в систему. Для дополнительной безопасности команда **exec-timeout** обеспечивает выход из системы линии, если в течение 5 минут отсутствует активность. Команда **logging synchronous** предотвращает прерывание ввода команд сообщениями консоли.

Примечание. Чтобы исключить необходимость постоянного повторного входа в систему во время лабораторной работы, вы можете ввести команду **exec-timeout** с параметрами **0 0**, чтобы отключить проверку истечения времени ожидания. Однако такой подход не считается безопасным.

```
R1(config)# line console 0
R1(config-line)# login local
R1(config-line)# exec-timeout 5 0
R1(config-line)# logging synchronous
```

f. Настройте линию aux 0 на использование локальной базы данных пользователей для входа в систему.

```
R1(config)# line aux 0
R1(config-line)# login local
R1(config-line)# exec-timeout 5 0
```


g. Настройте линию vty 0 4 на использование локальной базы данных пользователей для входа в систему и разрешите доступ только для соединений по SSH.

```
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exec-timeout 5 0
```

h. Настройте пароль привилегированного доступа с криптостойким шифрованием.

```
R1(config)# enable algorithm-type scrypt secret class12345
```

Шаг 8: Сохраните основную текущую конфигурацию для каждого маршрутизатора.

Сохраните текущую конфигурацию в конфигурацию запуска через командную строку в привилегированном режиме.

```
R1# copy running-config startup-config
```

Часть 2: Настройка зонального межсетевого экрана (ZPF)

В части 2 данной лабораторной работы необходимо настроить на маршрутизаторе R3 зональный межсетевой экран (ZPF) с использованием командной строки (CLI).

Задача 1: Проверка текущей конфигурации маршрутизаторов.

В этой задаче перед внедрением ZPF необходимо проверить сквозную связь по сети.

Шаг 1: Проверьте сквозную связь по сети.

a. Отправьте эхо-запрос с маршрутизатора R1 на R3. Используйте IP-адреса интерфейса Gigabit Ethernet маршрутизатора R3.

Если запрос был выполнен с ошибкой, проведите диагностику основных параметров устройства перед тем, как продолжить.

b. Отправьте эхо-запрос с компьютера PC-A в локальной сети маршрутизатора R1 на компьютер PC-C в локальной сети конференц-зала маршрутизатора R3.

Если запрос был выполнен с ошибкой, проведите диагностику основных параметров устройства перед тем, как продолжить.

c. Отправьте эхо-запрос с компьютера PC-A в локальной сети маршрутизатора R1 на компьютер PC-B во внутренней локальной сети маршрутизатора R3.

Если запрос был выполнен с ошибкой, проведите диагностику основных параметров устройства перед тем, как продолжить.

Шаг 2: Отобразите текущие конфигурации маршрутизатора R3.

a. Введите команду **show ip interface brief** на маршрутизаторе R3 и убедитесь, что назначены корректные IP-адреса. Для проверки используйте таблицу IP-адресов.

b. Введите команду **show ip route** на маршрутизаторе R3 и убедитесь, что у него есть статический маршрут по умолчанию, указывающий на последовательный интерфейс 0/0/1 маршрутизатора R2.

c. Введите команду **show run** для проверки текущей базовой конфигурации маршрутизатора R3.

d. Проверьте базовую конфигурацию маршрутизатора R3 по аналогии с частью 1 данной лабораторной работы. Есть ли какие-то команды безопасности, относящиеся к контролю доступа?

_____

Задача 2: Создание зонального межсетевого экрана.

В данной задаче необходимо создать на маршрутизаторе R3 зональный межсетевой экран, чтобы он работал не только как маршрутизатор, но и как межсетевой экран. Маршрутизатор R3 теперь отвечает за маршрутизацию пакетов в трех подключенных к нему сетях. Роли интерфейсов маршрутизатора R3 настроены следующим образом.

Последовательный интерфейс 0/0/1 подключен к Интернету. Так как это общедоступная сеть, она считается *недоверенной* сетью и должна иметь самый низкий уровень безопасности.

G0/1 подключен к внутренней сети. Только авторизованные пользователи имеют доступ к этой сети. Кроме того, в этой сети также расположены жизненно важные ресурсы организации. Внутренняя сеть должна считаться *доверенной* и иметь наивысший уровень безопасности.

G0/0 подключен к конференц-залу. Конференц-зал используется для проведения совещаний с людьми, не являющимися сотрудниками компании.

Политика безопасности, которая должна применяться маршрутизатором R3, когда он работает в качестве межсетевого экрана, определяет следующее.

- Никакой трафик, поступающий из Интернета, не должен попадать во внутреннюю сеть или в сеть конференц-зала.
- Возвратный трафик из Интернета (возвратные пакеты, приходящие из Интернета на маршрутизатор R3 в ответ на запросы, отправленные из любой из сетей маршрутизатора R3) должен быть разрешен.
- Компьютеры во внутренней сети маршрутизатора R3 считаются *доверенными*, и им разрешено инициировать любой тип трафика (TCP-, UDP- или ICMP-трафик).
- Компьютеры в конференц-зале маршрутизатора R3 считаются *недоверенными*, и им разрешено отправлять только веб-трафик в Интернет (HTTP или HTTPS).
- Между внутренней сетью и сетью конференц-зала любой трафик запрещен. Учитывая состояние гостевых компьютеров в сети конференц-зала, гарантий безопасности нет. Такие компьютеры могут быть заражены вредоносным ПО и могут пытаться генерировать спам или другой вредный трафик.

Шаг 1: Создайте зоны безопасности.

Зона безопасности – это группа интерфейсов со сходными свойствами и требованиями безопасности. Например, если у маршрутизатора есть три интерфейса, подключенные к внутренним сетям, все они могут быть помещены в одну зону под названием «внутренняя». Так как свойства безопасности настраиваются для зоны, а не для каждого интерфейса маршрутизатора, то архитектура межсетевого экрана становится более масштабируемой.

В данной лабораторной работе маршрутизатор R3 имеет три интерфейса: один подключен к внутренней доверенной сети, второй – к сети конференц-зала, а третий – к Интернету. Так как все три сети имеют разные свойства и требования безопасности, необходимо создать три зоны безопасности.

a. Зоны безопасности создаются в режиме глобальной настройки, и команда позволяет определить имена зон. На маршрутизаторе R3 создайте три зоны с именами **INSIDE**, **CONFROOM** и **INTERNET**:

```
R3(config)# zone security INSIDE
R3(config)# zone security CONFROOM
R3(config)# zone security INTERNET
```


Шаг 2: Создайте политики безопасности.

Прежде чем ZPF сможет определить, пропускать определенный трафик или нет, ему нужно вначале объяснить, *какой* трафик следует проверять. Для выбора трафика в Cisco IOS используются карты классов. *Интересный трафик* – распространенное обозначение трафика, который был выбран с помощью карты классов.

И хотя трафик выбирают карты классов, они не решают, что сделать с таким выбранным трафиком. *Судьбу* выбранного трафика определяют карты политик.

В качестве карт политик определены политики трафика ZPF, которые используют карты классов для выбора трафика. Другими словами, карты классов определяют, *какой* трафик должен быть ограничен, а карты политик – какое *действие* должно быть предпринято в отношении выбранного трафика.

Карты политик могут отбрасывать, пропускать или инспектировать трафик. Так как мы хотим, чтобы межсетевой экран *наблюдал* за движением трафика в направлении пар зон, необходимо создать карты политик inspect (инспектирование). Карты политик inspect разрешают динамическую обработку возвратного трафика.

Сначала необходимо создать карты классов. После создания карт классов необходимо создать карты политик и прикрепить карты классов к картам политик.

a. Создайте карту классов inspect, чтобы разрешать трафик из зоны INSIDE в зону **INTERNET.** Так как мы доверяем зоне INSIDE, мы разрешаем все основные протоколы.

   В следующих командах, показанных ниже, первая строка создает карту классов inspect. Ключевое слово **match-any** сообщает маршрутизатору, что любой из операторов протокола **match** будет квалифицироваться как положительное совпадение в применяемой политике. Результатом будет совпадение для пакетов TCP, UDP или ICMP.

   Команды **match** относятся к специальным протоколам, поддерживаемым в Cisco NBAR. Дополнительная информация о Cisco NBAR: Cisco Network-Based Application Recognition (Распознавание приложений по параметрам сетевого трафика).

```
R3(config)# class-map type inspect match-any INSIDE_PROTOCOLS
R3(config-cmap)# match protocol tcp
R3(config-cmap)# match protocol udp
R3(config-cmap)# match protocol icmp
```

b. Аналогичным образом создайте карту классов для выбора разрешенного трафика из зоны **CONFROOM** в зону **INTERNET.** Так как мы не полностью доверяем зоне **CONFROOM,** мы должны ограничить информацию, которую сервер может отправлять в Интернет:

```
R3(config)# class-map type inspect match-any CONFROOM_PROTOCOLS
R3(config-cmap)# match protocol http
R3(config-cmap)# match protocol https
R3(config-cmap)# match protocol dns
```

c. Теперь, когда карты классов созданы, можно создать карты политик.

   В следующих командах, показанных ниже, первая строка создает карту политик inspect с именем **INSIDE_TO_INTERNET**. Вторая строка привязывает ранее созданную карту классов **INSIDE_PROTOCOLS** к карте политик. Все пакеты, отмеченные картой класса **INSIDE_PROTOCOLS**, будут обработаны способом, указанным в карте политики **INSIDE_TO_INTERNET.** Наконец, третья строка определяет фактическое действие, которое карта политик будет применять к соответствующим пакетам. В нашем случае такие пакеты будут инспектироваться.

   Следующие три строки создают похожую карту политик с именем **CONFROOM_TO_INTERNET** и присоединяют карту классов **CONFROOM_PROTOCOLS.**

Команды указаны ниже:

```
R3(config)# policy-map type inspect INSIDE_TO_INTERNET
R3(config-pmap)# class type inspect INSIDE_PROTOCOLS
R3(config-pmap-c)# inspect
R3(config)# policy-map type inspect CONFROOM_TO_INTERNET
R3(config-pmap)# class type inspect CONFROOM_PROTOCOLS
R3(config-pmap-c)# inspect
```

Шаг 3: Создайте пары зон.

Пара зон позволяет создать однонаправленную политику межсетевого экрана между двумя зонами безопасности.

К примеру, широко применяемая политика безопасности определяет, что внутренняя сеть может инициировать любой трафик в Интернет, но любой трафик из Интернета не должен проникать во внутреннюю сеть.

Эта политика трафика требует только одну пару зон – **INTERNAL -> INTERNET**. Так как пары зон определяют однонаправленный поток трафика, должна быть создана другая пара зон, если инициируемый в Интернет трафик должен проходить в направлении **INTERNET -> INTERNAL.**

Обратите внимание, что Cisco ZPF можно настроить на инспектирование трафика, передаваемого в направлении, определяемом парой зон. В этой ситуации межсетевой экран *наблюдает* за трафиком и динамически формирует правила, позволяющие возвратному или связанному трафику проходить обратно через маршрутизатор.

Для определения пары зон используйте команду **zone-pair security.** Направление трафика указывается зонами отправления и назначения.

В этой лабораторной работе вы создадите две пары зон.

INSIDE_TO_INTERNET: позволяет трафику выходить из внутренней сети в Интернет.

CONFROOM_TO_INTERNET: разрешает доступ в Интернет из сети конференц-зала.

a. Создание пар зон:

```
R3(config)# zone-pair security INSIDE_TO_INTERNET source INSIDE destination INTERNET
R3(config)# zone-pair security CONFROOM_TO_INTERNET source CONFROOM destination
INTERNET
```

b. Убедитесь, что пары зон были созданы корректно, используя команду **show zone-pair security.** Обратите внимание, что на данный момент с парами зон не ассоциирована ни одна политика. Политики безопасности будут применены к парам зон на следующем шаге.

```
R3# show zone-pair security
Zone-pair name INSIDE_TO_INTERNET
    Source-Zone INSIDE  Destination-Zone INTERNET
    service-policy not configured
Zone-pair name CONFROOM_TO_INTERNET
    Source-Zone CONFROOM  Destination-Zone INTERNET
    service-policy not configured
```


Шаг 4: Примените политики безопасности.

a. На последнем шаге настройки примените карты политик к парам зон:

```
R3(config)# zone-pair security INSIDE_TO_INTERNET
R3(config-sec-zone-pair)# service-policy type inspect INSIDE_TO_INTERNET
R3(config)# zone-pair security CONFROOM_TO_INTERNET
R3(config-sec-zone-pair)# service-policy type inspect CONFROOM_TO_INTERNET
```

b. Введите команду **show zone-pair security** еще раз, чтобы проверить настройки пар зон. Обратите внимание, что сейчас отображаются сервисные политики:

```
R3#show zone-pair security
Zone-pair name INSIDE_TO_INTERNET
    Source-Zone INSIDE  Destination-Zone INTERNET
    service-policy INSIDE_TO_INTERNET
Zone-pair name CONFROOM_TO_INTERNET
    Source-Zone CONFROOM  Destination-Zone INTERNET
    service-policy CONFROOM_TO_INTERNET
```

Чтобы получить больше информации о парах зон, их картах политик, картах классов и счетчиках соответствия, используйте команду **show policy-map type inspect zone-pair.**

```
R3#show policy-map type inspect zone-pair
policy exists on zp INSIDE_TO_INTERNET
  Zone-pair: INSIDE_TO_INTERNET

  Service-policy inspect : INSIDE_TO_INTERNET

    Class-map: INSIDE_PROTOCOLS (match-any)
      Match: protocol tcp
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol udp
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol icmp
        0 packets, 0 bytes
        30 second rate 0 bps

   Inspect
        Session creations since subsystem startup or last reset 0
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [0:0:0]
        Last session created never
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 0
        Last half-open session total 0
        TCP reassembly statistics
        received 0 packets out-of-order; dropped 0
        peak memory usage 0 KB; current usage: 0 KB
        peak queue length 0


    Class-map: class-default (match-any)
      Match: any
      Drop
           0 packets, 0 bytes
<output omitted>
```


Шаг 5: Назначьте интерфейсы соответствующим зонам безопасности.

Интерфейсы (физические и логические) назначаются зонам безопасности с помощью команды интерфейса **zone-member security.**

a. Назначьте интерфейс G0/0 маршрутизатора R3 зоне безопасности **CONFROOM**:

```
R3(config)# interface g0/0
R3(config-if)# zone-member security CONFROOM
```

b. Назначьте интерфейс G0/1 маршрутизатора R3 зоне безопасности INSIDE:

```
R3(config)# interface g0/1
R3(config-if)# zone-member security INSIDE
```

c. Назначьте интерфейс S0/0/1 маршрутизатора R3 зоне безопасности **INTERNET**:

```
R3(config)# interface s0/0/1
R3(config-if)# zone-member security INTERNET
```

Шаг 6: Проверьте назначение зон.

a. Введите команду show zone security и убедитесь, что зоны корректно созданы, а интерфейсы корректно назначены.

```
R3# show zone security
zone self
  Description: System defined zone

zone CONFROOM
  Member Interfaces:
    GigEthernet0/0

zone INSIDE
  Member Interfaces:
    GigEthernet0/1

zone INTERNET
  Member Interfaces:
    Serial0/0/1
```

b. Несмотря на то что команды для создания зоны self (собственной) не вводились, она все равно присутствует в выходных данных выше. Почему маршрутизатор R3 отображает зону с именем self? Каково значение этой зоны?

_____

_____

_____

_____

Часть 3: Проверка ZPF

Задача 1: Проверка работоспособности межсетевого экрана ZPF.

Шаг 1: Трафик, сгенерированный в Интернете

a. Для проверки эффективности межсетевого экрана отправьте эхо-запрос на компьютер PC-B с PC-A. На компьютере PC-A откройте командную строку и введите:

```
C:\Users\NetAcad> ping 192.168.3.3
```

Эхо-запрос выполнен успешно? Поясните ответ.

_____

_____

_____

_____

_____

b. Отправьте эхо-запрос на компьютер PC-C с компьютера PC-A. На PC-A откройте командное окно и введите:

```
C:\Users\NetAcad> ping 192.168.33.3
```

Эхо-запрос выполнен успешно? Поясните ответ.

_____

_____

_____

_____

_____

c. Отправьте эхо-запрос на компьютер PC-A с компьютера PC-B. На PC-B откройте командное окно и введите:

```
C:\Users\NetAcad> ping 192.168.1.3
```

d. Эхо-запрос выполнен успешно? Поясните ответ.

_____

_____

_____

_____

_____

Отправьте эхо-запрос на компьютер PC-A с компьютера PC-C. На PC-C откройте командное окно и введите:

```
C:\Users\NetAcad> ping 192.168.1.3
```

e. Эхо-запрос выполнен успешно? Поясните ответ.

_____

_____

_____

_____

_____

Шаг 2: Проверьте собственную зону.

a. Отправьте с компьютера PC-A эхо-запрос на интерфейс G0/1 маршрутизатора R3:

```
C:\Users\NetAcad> ping 192.168.3.1
```

Эхо-запрос выполнен успешно? Это правильное поведение? Поясните ответ.

_____

_____

_____

_____

b. Отправьте с компьютера PC-C эхо-запрос на интерфейс G0/1 маршрутизатора R3:

```
C:\Users\NetAcad> ping 192.168.3.1
```

Эхо-запрос выполнен успешно? Это правильное поведение? Поясните ответ.

_____

_____

_____

_____

Задача (дополнительно)

Создайте подходящую пару зон, карты классов и карты политик и настройте маршрутизатор R3 таким образом, чтобы трафик из Интернета не мог попадать в зону Self.

Приложение. Несколько интерфейсов в одной зоне (дополнительно)

Одно из преимуществ межсетевых экранов ZPF – их относительно хорошая масштабируемость по сравнению с классическими межсетевыми экранами. Если новый интерфейс с теми же требованиями безопасности добавляется в межсетевой экран, администратор может просто добавить его как член уже существующей зоны безопасности. Однако некоторые версии IOS не позволят устройствам, подключенным к разным интерфейсам в одной и той же зоне безопасности, взаимодействовать друг с другом по умолчанию. В подобной ситуации необходимо создать пару зон, использующую одну и ту же зону в качестве источника и места назначения.

Трафик между интерфейсами в одной зоне будет всегда двунаправленным, так как зона-источник и зона назначения одинаковы. Благодаря этому нет необходимости проверять трафик для того, чтобы разрешить автоматический возврат; возвратный трафик всегда будет разрешен, так как он всегда будет соответствовать определению пары зон. В данной ситуации для карты политик должно быть установлено действие **pass,** а не **inspect.** В соответствии с действием **pass** маршрутизатор не будет проверять трафик, соответствующий карте политик, а будет просто перенаправлять его в место назначения.

В контексте данной лабораторной работы, если бы на маршрутизаторе R3 был интерфейс G0/2, также назначенный зоне INSIDE, и версия IOS на маршрутизаторе не разрешала трафик между интерфейсами, направленными в одну зону, дополнительная конфигурация выглядела бы так:

Новая пара зон: **Inside to Inside** разрешает маршрутизацию трафика между внутренними доверенными интерфейсами.

Создание карты политик (обратите внимание, что явная карта классов не требуется, так как мы используем класс по умолчанию catch-all):

```
R3(config)# policy-map type inspect inside
R3(config-pmap)# class class-default
R3(config-pmap-c)# pass
```


Создание пары зон и назначение ей новой карты политик. Обратите внимание, что зона INSIDE является как источником, так и местом назначения пары зон:

```
R3(config)# zone-pair security INSIDE source INSIDE destination INSIDE
R3(config-sec-zone-pair)# service-policy type inspect inside
```

Чтобы проверить существование новой пары, используйте команду **show zone-pair security:**

```
R3# show zone-pair security
    Zone-pair name INSIDE_TO_INTERNET
        Source-Zone INSIDE Destination-Zone INTERNET
        service-policy INSIDE_TO_INTERNET
    Zone-pair name CONFROOM_TO_INTERNET
        Source-Zone CONFROOM  Destination-Zone INTERNET
        service-policy CONFROOM_TO_INTERNET
    Zone-pair name INSIDE
        Source-Zone INSIDE Destination-Zone INSIDE
        service-policy inside
```

Сводная таблица по интерфейсам маршрутизаторов

Сводная таблица по интерфейсам маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet 1**	**Интерфейс Ethernet 2**	**Последовательный интерфейс 1**	**Последовательный интерфейс 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать конфигурацию маршрутизатора, определите его тип по интерфейсам, а также по количеству имеющихся интерфейсов. Эффективно перечислить все комбинации настроек для маршрутизатора каждого класса невозможно. В данной таблице приведены идентификаторы возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов в устройстве. В эту таблицу не включены какие-либо иные типы интерфейсов, даже если в определенном маршрутизаторе они могут присутствовать. В качестве примера можно привести интерфейс ISDN BRI. В строке в скобках приведены официальные аббревиатуры, которые могут использоваться в командах Cisco IOS для представления интерфейсов.

