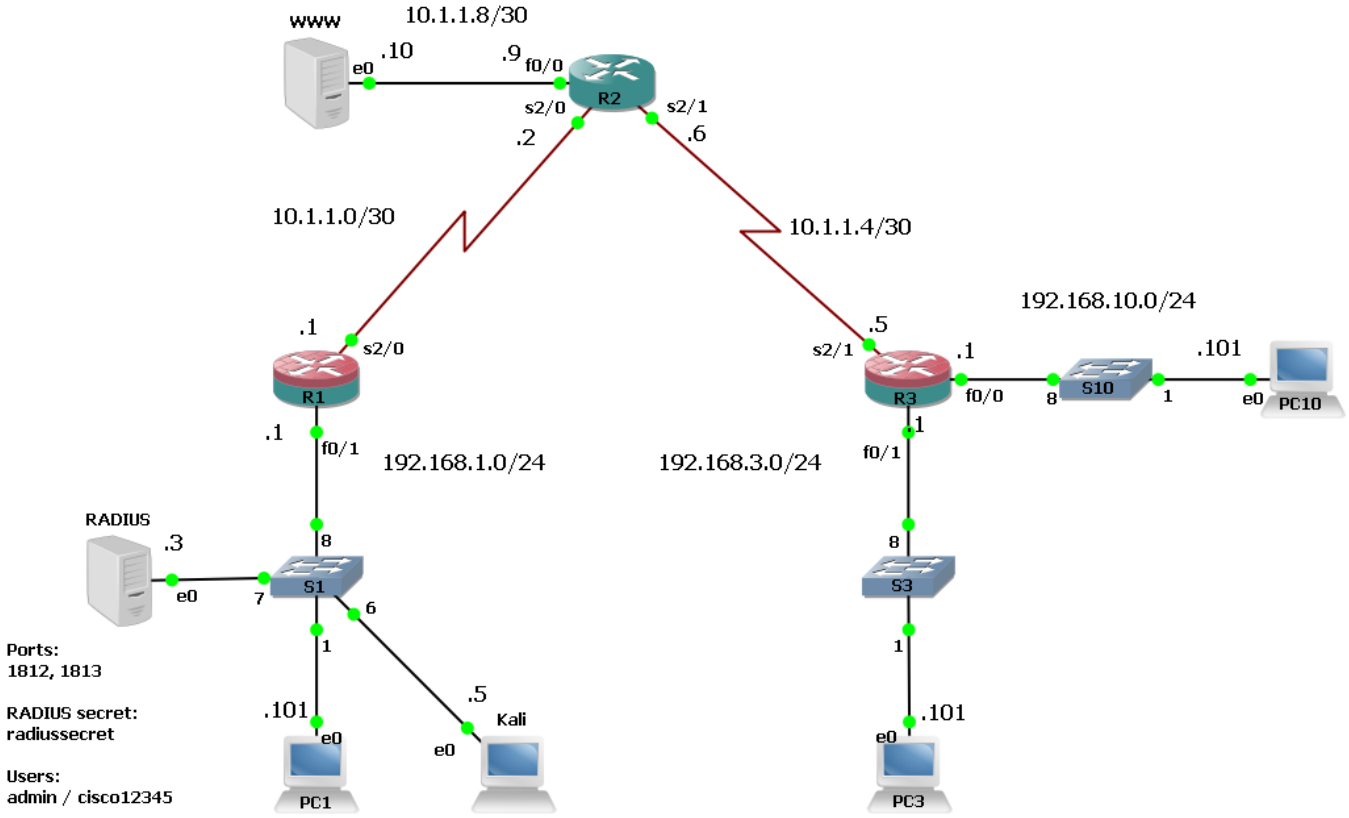
CCNA Security

Лабораторная работа 16

Настройка Zone-based Policy Firewall

Топология



Описание

В этой лабораторной работе вы внедрите функционал ZPF (Zone-based Policy Firewall) на маршрутизаторе R3.

Таблица адресации

Устройство	Интерфейс	IPv4-адрес/Маска подсети	Шлюз по умолчанию	Описание
R1	Fa0/1	192.168.1.1/24	-	LAN interface
	Se2/0	10.1.1.1/30	-	WAN interface (To R2)
R2	Se2/0	10.1.1.2/30	-	To R1
	Se2/1	10.1.1.6/30	-	To R3
	Fa0/0	10.1.1.9/30	-	To WWW server
R3	Fa0/1	192.168.3.1/24	-	LAN interface
	Fa0/0	192.168.10.1/24	-	Conference Room
	Se2/1	10.1.1.5/30	-	WAN interface (To R2)
PC1	NIC	192.168.1.101/24	192.168.1.1	-
PC2	NIC	192.168.3.101/24	192.168.3.1	-
PC10	NIC	192.168.10.101/24	192.168.10.1	-
Kali	NIC	192.168.1.5/24	192.168.1.1	-
RADIUS	NIC	192.168.1.3/24	192.168.1.1	-
WWW	NIC	10.1.1.10/24	10.1.1.9	-

Имена пользователей и пароли

	Console		VTY		Enable
Устройство	Имя пользователя	Пароль	Имя пользователя	Пароль	Пароль
R1	admin	cisco12345	admin	cisco12345	cisco12345
R2	-	-	-	-	-
R3	admin	cisco12345	admin	cisco12345	cisco12345

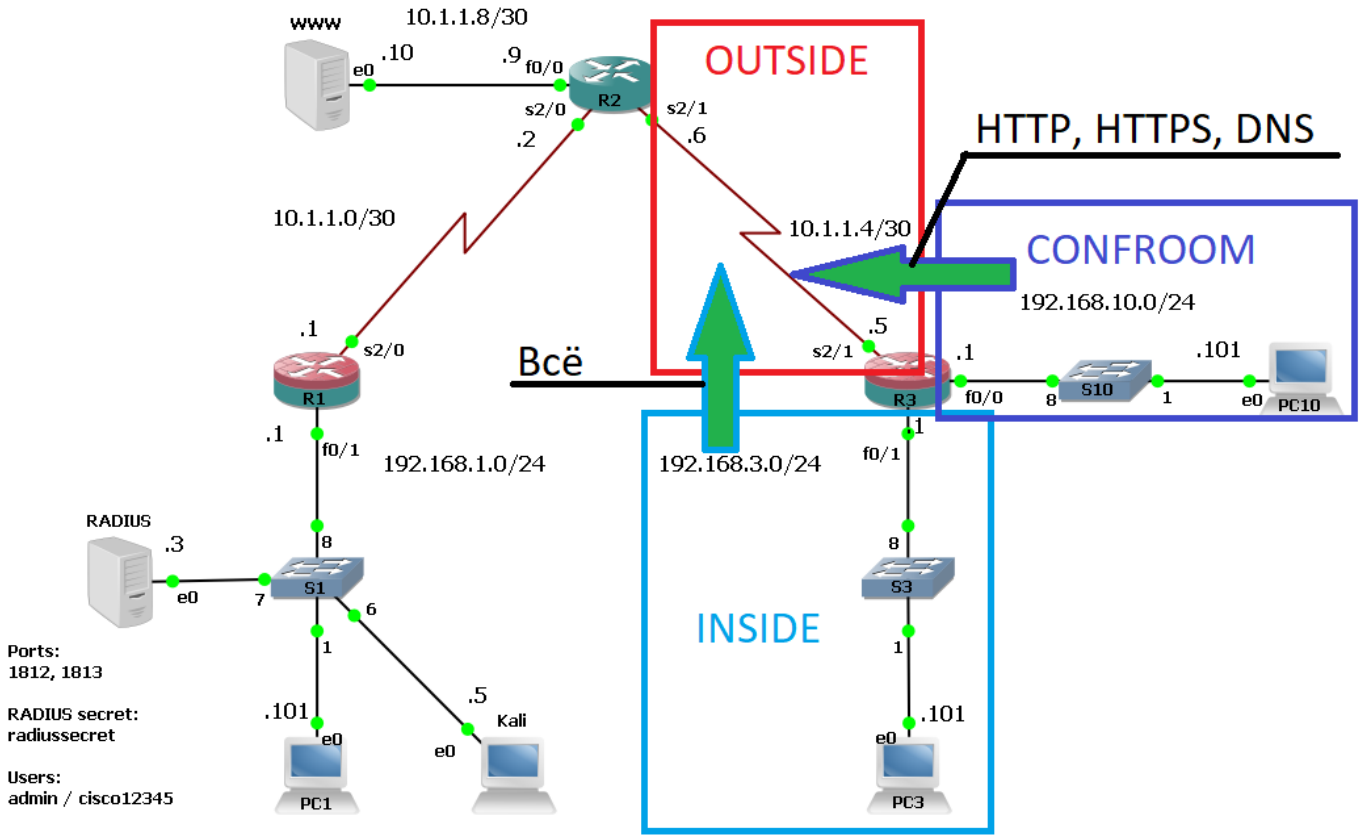
Устройство	Имя пользователя	Пароль
PC1	Student1	1
PC2	Student1	1
PC10	Student1	1
Kali	root	toor

Часть 1: Постановка задачи

1. Необходимо выполнить следующие требования:
   - В вашем филиале есть две сети: 192.168.3.0/24 и 192.168.10.0/24;
   - В сети 192.168.3.0/24 находятся рабочие станции «продвинутых» пользователей, они должны иметь полный доступ к внешним ресурсам;
   - Сеть 192.168.10.0/24 отведена под конференц-зал, в который приходят люди со стороны. Нужно разрешить доступ к внешним ресурсам только по протоколам HTTP, HTTPS, DNS на стандартные порты получателя;
   - Между сетью 192.168.3.0/24 и 192.168.10.0/24 трафик запрещён;
   - Извне необходимо разрешить только возвратный трафик.

2. На основе требований вы спланировали следующее:
   - Потребуется создать три зоны (INSIDE, CONFROOM, OUTSIDE);
   - Потребуется определить две классовые карты инспектирующего типа (class-map type inspect) для выбора интересного траффика из зоны INSIDE и CONFROOM;
   - Потребуется создать две карты политик инспектирующего типа (policy-map type inspect). Первая карта политик будет инспектировать интересный трафик, определённый в классовой карте для зоны INSIDE, вторая будет инспектировать интересный трафик, определённый в классовой карте для зоны CONFROOM;
   - Потребуется создать две пары зон. Первая пара зон будет использоваться для применения политики при движении траффика из зоны INSIDE в зону OUTSIDE, вторая пара зон будет использоваться для применения политики при движении траффика из зоны CONFROOM в зону OUTSIDE.

3. Схематичное изображение плана представлено ниже:



Часть 2: Настройка ZPF на маршрутизаторе R3

1. Перейдите в консоль маршрутизатора R3.

2. Войдите в режим конфигурирования.
```
R3# conf t
```

3. Создайте три зоны. В подрежиме конфигурирования зоны можно присвоить ей описание с помощью команды description, однако названия наших зон и так говорящие.
```
R3(config)# zone security ZONE_INSIDE
R3(config-sec-zone)# exit
R3(config)# zone security ZONE_CONFROOM
R3(config-sec-zone)# exit
R3(config)# zone security ZONE_OUTSIDE
R3(config-sec-zone)# exit
```

4. Проверьте наличие зон. Кроме трёх зон, созданных вами, также вы увидите зону self, к которой относятся адреса самого маршрутизатора. Для маршрутизатора R3 к зоне self будут относиться адреса 192.168.3.1, 192.168.10.1, 10.1.1.5.
```
R3(config)# do show zone security
zone self
  Description: System defined zone
zone ZONE_INSIDE

zone ZONE_CONFROOM

zone ZONE_OUTSIDE
```

5. Создайте классовую карту инспектирующего типа, которая будет выбирать интересный траффик из зоны ZONE_INSIDE. Вам интересен весь трафик, выразите это как «протокол TCP или протокол UDP или протокол ICMP». При создании используйте параметр match-any, в таком случае классовая карта сработает, когда выполнится хотя бы одно из входящих в неё условий. Параметр match-any равносилен объединению условий логическим союзом ИЛИ. Сами условия задайте с помощью команды match protocol.
```
R3(config)# class-map type inspect match-any CM_INSIDE_PROTOCOLS
R3(config-cmap)# match protocol tcp
R3(config-cmap)# match protocol udp
R3(config-cmap)# match protocol icmp
R3(config-cmap)# exit
```

6. Создайте классовую карту инспектирующего типа, которая будет выбирать интересный траффик из зоны CONFROOM. Помните, что условия match protocol – это всего лишь лёгкий способ записи, чтобы не использовать ACL, а не активация глубокой инспекции траффика уровня приложений.

Условие в class-map	Аналог в ACL
match protocol http	permit tcp any any eq 80
match protocol https	permit tcp any any eq 443

match protocol dns	permt udp any any eq 53 permit tcp any any eq 53

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

7. Проверьте созданные классовые карты.

```
R3(config)# do show class-map type inspect
Class Map type inspect match-any CM_CONFROOM_PROTOCOLS (id 2)
   Match protocol  http
   Match protocol  https
   Match protocol  dns

 Class Map type inspect match-any CM_INSIDE_PROTOCOLS (id 1)
   Match protocol  tcp
   Match protocol  udp
   Match protocol  icmp
```

8. Создайте карту политик инспектирующего типа, которая будет инспектировать интересный траффик, выбранный классовой картой CM_INSIDE_PROTOCOLS. Остальной траффик попадёт под класс class-default, для этого класса действие по умолчанию – drop.

```
R3(config)# policy-map type inspect PM_INSIDE_TO_OUTSIDE
R3(config-pmap)# class type inspect CM_INSIDE_PROTOCOLS
R3(config-pmap-c)# inspect
R3(config-pmap-c)# exit
R3(config-pmap)# exit
```

9. Создайте карту политик инспектирующего типа, которая будет инспектировать интересный траффик, выбранный классовой картой CM_CONFROOM_PROTOCOLS.

```
R3(config)# policy-map type inspect PM_CONFROOM_TO_OUTSIDE
R3(config-pmap)# class type inspect CM_CONFROOM_PROTOCOLS
R3(config-pmap-c)# inspect
R3(config-pmap-c)# exit
R3(config-pmap)# exit
```

10. Проверьте созданные карты политик.

```
R3(config)# do show policy-map type inspect
  Policy Map type inspect PM_CONFROOM_TO_OUTSIDE
    Class CM_CONFROOM_PROTOCOLS
      Inspect

  Policy Map type inspect PM_INSIDE_TO_OUTSIDE
    Class CM_INSIDE_PROTOCOLS
      Inspect
```

11. Создайте пару зон, определяющую движение траффика из ZONE_INSIDE в ZONE_OUTSIDE, и привяжите к ней карту политик PM_INSIDE_TO_OUTSIDE.

```
R3(config)# zone-pair security ZP_INSIDE_TO_OUTSIDE source ZONE_INSIDE destination ZONE_OUTSIDE
R3(config-sec-zone-pair)# service-policy type inspect PM_INSIDE_TO_OUTSIDE
R3(config-sec-zone-pair)# exit
```

12. Создайте пару зон, определяющую движение траффика из ZONE_CONFROOM в ZONE_OUTSIDE, и привяжите к ней карту политик PM_CONFROOM_TO_OUTSIDE.

```
R3(config)# zone-pair security ZP_CONFROOM_TO_OUTSIDE source ZONE_CONFROOM destination ZONE_OUTSIDE
R3(config-sec-zone-pair)# service-policy type inspect PM_CONFROOM_TO_OUTSIDE
R3(config-sec-zone-pair)# exit
```

13. Проверьте созданные пары зон и привязанные к ним сервисные политики.

```
R3(config)# do show zone-pair security
Zone-pair name ZP_INSIDE_TO_OUTSIDE
    Source-Zone ZONE_INSIDE  Destination-Zone ZONE_OUTSIDE
    service-policy PM_INSIDE_TO_OUTSIDE
Zone-pair name ZP_CONFROOM_TO_OUTSIDE
    Source-Zone ZONE_CONFROOM  Destination-Zone ZONE_OUTSIDE
    service-policy PM_CONFROOM_TO_OUTSIDE
```

14. Проверьте общую настройку ZPF. Представленная ниже команда удобна тем, что позволяет развернуть все составляющие сразу: zone-pair, service-policy, policy-map, class-map. Также эта команда выведет разнообразную статистику, что пригодится в будущем.

```
R3(config)# do show policy-map type inspect zone-pair

policy exists on zp ZP_INSIDE_TO_OUTSIDE
  Zone-pair: ZP_INSIDE_TO_OUTSIDE

  Service-policy inspect : PM_INSIDE_TO_OUTSIDE

    Class-map: CM_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

policy exists on zp ZP_CONFROOM_TO_OUTSIDE
  Zone-pair: ZP_CONFROOM_TO_OUTSIDE

  Service-policy inspect : PM_CONFROOM_TO_OUTSIDE

    Class-map: CM_CONFROOM_PROTOCOLS (match-any)
      Match: protocol http
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol https
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol dns
        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
```

15. Занесите интерфейсы в нужные зоны. Помните, что нельзя включить ZPF частично, потому что траффик между интерфейсом, входящим в любую зону, и интерфейсом, не входящим в любую зону, по умолчанию запрещён.

```
R3(config)# int fa0/1
R3(config-if)# zone-member security ZONE_INSIDE
R3(config-if)# exit
R3(config)# int fa0/0
R3(config-if)# zone-member security ZONE_CONFROOM
R3(config-if)# exit
R3(config)# int s2/1
R3(config-if)# zone-member security ZONE_OUTSIDE
R3(config-if)# end
```

16. Проверьте, что интерфейсы занесены в нужную зону.

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

zone ZONE_INSIDE
  Member Interfaces:
    FastEthernet0/1

zone ZONE_CONFROOM
  Member Interfaces:
    FastEthernet0/0

zone ZONE_OUTSIDE
  Member Interfaces:
    Serial2/1
```

Часть 3: Практическая проверка

1. Войдите в виртуальную машину PC3.

2. Запустите командную строку. Попробуйте связаться с сервером WWW командой ping (ping 10.1.1.10). Проверка связи будет успешна. Почему?
   - Траффик идёт из ZONE_INSIDE в ZONE_OUTSIDE;
   - Зоны разные, но есть пара зон ZP_INSIDE_TO_OUTSIDE;
   - К паре зон прилеплена карта политик PM_INSIDE_TO_OUTSIDE;
   - Карта политик ссылается на классовую карту CM_INSIDE_PROTOCOLS;
   - Классовая карта срабатывает, траффик попадает под условие match protocol icmp, для срабатывания достаточно выполнения одного условия (параметр match-any);
   - В карте политик срабатывает действие inspect – траффик разрешается, создаётся состояние, возвратный траффик автоматически разрешается.

3. Откройте браузер, попробуйте зайти на сервер WWW по протоколу http (http://10.1.1.10). Успешно откроется тестовая страница. Почему?
   - Траффик идёт из ZONE_INSIDE в ZONE_OUTSIDE;
   - Зоны разные, но есть пара зон ZP_INSIDE_TO_OUTSIDE;
   - К паре зон прилеплена карта политик PM_INSIDE_TO_OUTSIDE;
   - Карта политик ссылается на классовую карту CM_INSIDE_PROTOCOLS;
   - Классовая карта срабатывает, траффик попадает под условие match protocol tcp, для срабатывания достаточно выполнения одного условия (параметр match-any);
   - В карте политик срабатывает действие inspect – траффик разрешается, создаётся состояние, возвратный траффик автоматически разрешается.

4. Откройте браузер, попробуйте зайти на сервер WWW по протоколу http на нестандартный порт 12345 (http://10.1.1.10:12345). Успешно откроется тестовая страница. Почему? По тем же причинам, что и в шаге 3.

5. Вернитесь в командную строку. Попробуйте связаться с PC10 командой ping (ping 192.168.10.101). Проверка связи будет неуспешна. Почему?
   - Траффик идёт из ZONE_INSIDE в ZONE_CONFROOM;
   - Зоны разные, пары зон нет. Действие по умолчанию в таких случаях – drop.

6. Попробуйте связаться с маршрутизатором R3 командой ping (ping 192.168.10.1). Проверка связи будет успешна. Почему?
   - Траффик идёт из ZONE_INSIDE в self. Хотя интерфейс fa0/0 относится к ZONE_CONFROOM, адрес 192.168.10.1 принадлежит самому маршрутизатору, а стало быть относится к зоне self;
   - Зоны разные, но зона получатель – self. По умолчанию весь траффик в или из зоны self разрешён, действие по умолчанию в таких случаях – pass. Подтверждением данного факта также является сохранившееся соседство в протоколе OSPF между R2 и R3.

7. Войдите в виртуальную машину PC10.

8. Запустите командную строку. Попробуйте связаться с сервером WWW командой ping (ping 10.1.1.10). Проверка связи будет неуспешна. Почему?
   - Траффик идёт из ZONE_CONFROOM в ZONE_OUTSIDE;
   - Зоны разные, но есть пара зон ZP_CONFROOM_TO_OUTSIDE;
   - К паре зон прилеплена карта политик PM_CONFROOM_TO_OUTSIDE;
   - Карта политик ссылается на классовую карту CM_CONFROOM_PROTOCOLS;
   - Классовая карта не срабатывает, траффик не попадает ни под одно из условий;
   - В карте политик более нет отсылок к классовым картам, значит траффик попадает под класс class-default, действие по умолчанию – drop.

9. Откройте браузер, попробуйте зайти на сервер WWW по протоколу http (http://10.1.1.10). Успешно откроется тестовая страница. Почему?
   - Траффик идёт из ZONE_CONFROOM в ZONE_OUTSIDE;
   - Зоны разные, но есть пара зон ZP_CONFROOM_TO_OUTSIDE;
   - К паре зон прилеплена карта политик PM_CONFROOM_TO_OUTSIDE;
   - Карта политик ссылается на классовую карту CM_CONFROOM_PROTOCOLS;
   - Классовая карта срабатывает, траффик попадает под условие match protocol http, для срабатывания достаточно выполнения одного условия (параметр match-any);
   - В карте политик срабатывает действие inspect – траффик разрешается, создаётся состояние, возвратный траффик автоматически разрешается.

10. Откройте браузер, попробуйте зайти на сервер WWW по протоколу http на нестандартный порт 12345 (http://10.1.1.10:12345). Тестовая страница не откроется. Почему? **Попробуйте обосновать сами**.

11. Вернитесь в командную строку. Попробуйте связаться с PC3 командой ping (ping 192.168.3.101). Проверка связи будет неуспешна. Почему? **Попробуйте обосновать сами.**

12. Попробуйте связаться с маршрутизатором R3 командой ping (ping 192.168.3.1). Проверка связи будет успешна. Почему? **Попробуйте обосновать сами**.

13. Вернитесь в консоль маршрутизатора R3.

17. Проверьте счётчики ZPF. Изменились ли они с момента предыдущей проверки? Ваш вывод может отличаться.

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

  Service-policy inspect : PM_INSIDE_TO_OUTSIDE

    Class-map: CM_INSIDE_PROTOCOLS (match-any)
      Match: protocol tcp
        3 packets, 96 bytes
        30 second rate 0 bps
      Match: protocol udp
        0 packets, 0 bytes
        30 second rate 0 bps
```

```
      Match: protocol icmp
        1 packets, 40 bytes
        30 second rate 0 bps

    Inspect
        Packet inspection statistics [process switch:fast switch]
        tcp packets: [0:37]
        icmp packets: [0:8]

        Session creations since subsystem startup or last reset 4
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [2:1:1]
        Last session created 00:20:15
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 3
        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

policy exists on zp ZP_CONFROOM_TO_OUTSIDE
  Zone-pair: ZP_CONFROOM_TO_OUTSIDE

  Service-policy inspect : PM_CONFROOM_TO_OUTSIDE

     Class-map: CM_CONFROOM_PROTOCOLS (match-any)
       Match: protocol http
         2 packets, 64 bytes
         30 second rate 0 bps
       Match: protocol https
         0 packets, 0 bytes
         30 second rate 0 bps
       Match: protocol dns
         0 packets, 0 bytes
         30 second rate 0 bps

    Inspect
        Packet inspection statistics [process switch:fast switch]
        tcp packets: [0:24]

        Session creations since subsystem startup or last reset 2
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [1:1:1]
        Last session created 00:02:54
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 1
        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
    13 packets, 436 bytes
```

14. Вы можете продолжить проверку самостоятельно. Например, выполнить разные тесты с маршрутизатора R2 или попробовать просканировать сети 192.168.3.0/24 и 192.168.10.0/24 с виртуальной машины Kali.

Часть 4: Отключение ZPF

1. Чтобы функционал ZPF не мешал в следующей лабораторной работе, отключите его. Для этого достаточно вывести все интерфейсы из зон. Перейдите в консоль маршрутизатора R3.

2. Войдите в режим конфигурирования.
```
R3# conf t
```

3. Вынесите интерфейсы из зон.
```
R3(config)# int fa0/1
R3(config-if)# no zone-member security ZONE_INSIDE
R3(config-if)# exit
R3(config)# int fa0/0
R3(config-if)# no zone-member security ZONE_CONFROOM
R3(config-if)# exit
R3(config)# int s2/1
R3(config-if)# no zone-member security ZONE_OUTSIDE
R3(config-if)# end
```

4. Проверьте, что зоны пусты.
```
R3# show zone security
zone self
  Description: System defined zone

zone ZONE_INSIDE

zone ZONE_CONFROOM

zone ZONE_OUTSIDE
```