МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,

СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»

(СПбГУТ)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Факультет инфокоммуникационных сетей и систем

Кафедра защищенных систем связи

Дисциплина Безопасность компьютерных сетей

ЛАБОРАТОРНАЯ РАБОТА №8 – Часть 1

Packet Tracer - Configure IOS Intrusion Prevention System (IPS) Using CLI

11.03.02 Инфокоммуникационные технологии и системы связи

Студенты:

Громов А. А., ИКТЗ-83 \_\_\_\_\_\_\_\_\_

*(Ф.И.О., № группы) (подпись)*

Жиляков Г. В., ИКТЗ-83 \_\_\_\_\_\_\_\_\_

*(Ф.И.О., № группы) (подпись)*

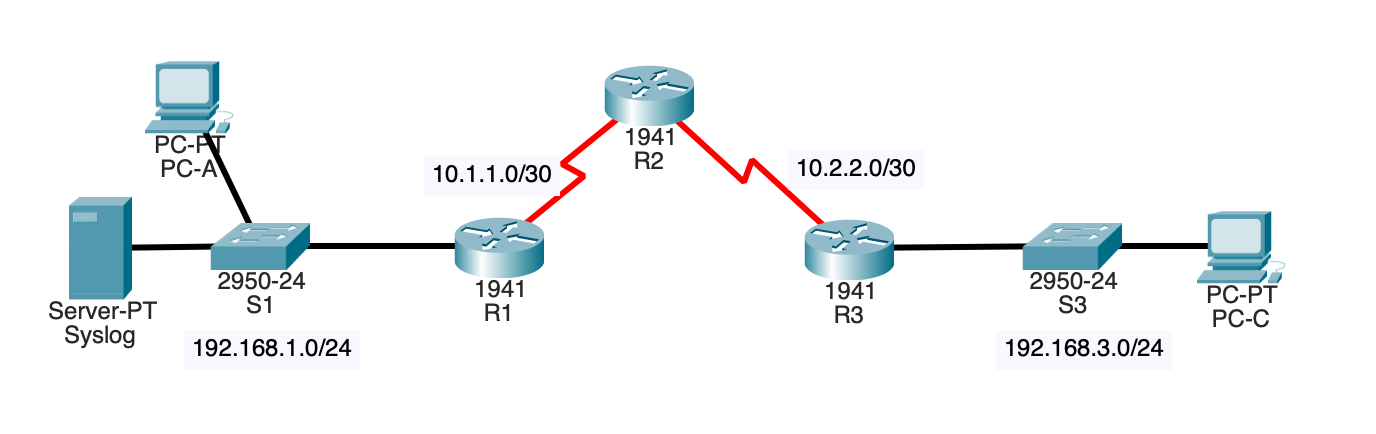
Миколаени М. С., ИКТЗ-83 \_\_\_\_\_\_\_\_\_

*(Ф.И.О., № группы) (подпись)*

Проверил:

К.т.н., доцент каф. ЗСС, Кушнир Д. В.

# Топология:

****

**Packet Tracer. Настройка системы предотвращения вторжений (IPS) в IOS с помощью интерфейса командной строки**

**Таблица адресации**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **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 F0/1 |
| S0/0/0 | 10.1.1.1 | 255.255.255.252 | Н/П | Н/П |
| R2 | S0/0/0 (DCE) | 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 | G0/1 | 192.168.3.1 | 255.255.255.0 | Н/П | S3 F0/1 |
| S0/0/0 | 10.2.2.1 | 255.255.255.252 | Н/П | Н/П |
| Syslog | NIC | 192.168.1.50 | 255.255.255.0 | 192.168.1.1 | S1 F0/2 |
| PC-A | NIC | 192.168.1.2 | 255.255.255.0 | 192.168.1.1 | S1 F0/3 |
| PC-C | NIC | 192.168.3.2 | 255.255.255.0 | 192.168.3.1 | S3 F0/2 |

**Задачи**

·         Включение системы IPS в IOS.

·         Настройка ведения журнала.

·         Изменение сигнатуры IPS.

·         Проверка IPS.

**Исходные данные/ сценарий**

Ваша задача – включение системы IPS на маршрутизаторе R1 для проверки трафика, поступающего в сеть 192.168.1.0.

Сервер Syslog используется для ведения журнала сообщений IPS. Вы должны настроить маршрутизатор для идентификации сервера Syslog, который будет получать сообщения журнала. Очень важно, чтобы в сообщениях Syslog отображались правильные дата и время, когда сервис Syslog используется для мониторинга сети. Настройте часы и сервис временных меток для ведения журналов на маршрутизаторах. Наконец, включите систему IPS для выдачи оповещения и отбрасывания пакетов ICMP Echo Reply во внутриканальном режиме.

Сервер и компьютеры были предварительно настроены. На маршрутизаторах также были предварительно настроены следующие параметры.

o    Пароль привилегированного доступа: **ciscoenpa55**

o    Пароль консоли: **ciscoconpa55**

o    Имя пользователя и пароль SSH: **SSHadmin**/**ciscosshpa55**

o    OSPF 101

**Ход работы:**

**Часть 1. Включение системы IPS в IOS**

**Примечание**. В Packet Tracer файлы сигнатур уже импортированы на маршрутизаторы. Это XML-файлы по умолчанию, хранящиеся во флеш-памяти. По этой причине не нужно настраивать открытый криптографический ключ и вручную импортировать файлы сигнатур.

**Шаг 1. Включение пакета Security Technology**

a.     На маршрутизаторе **R1** введите команду **show version** для просмотра сведений о лицензии Technology Package.

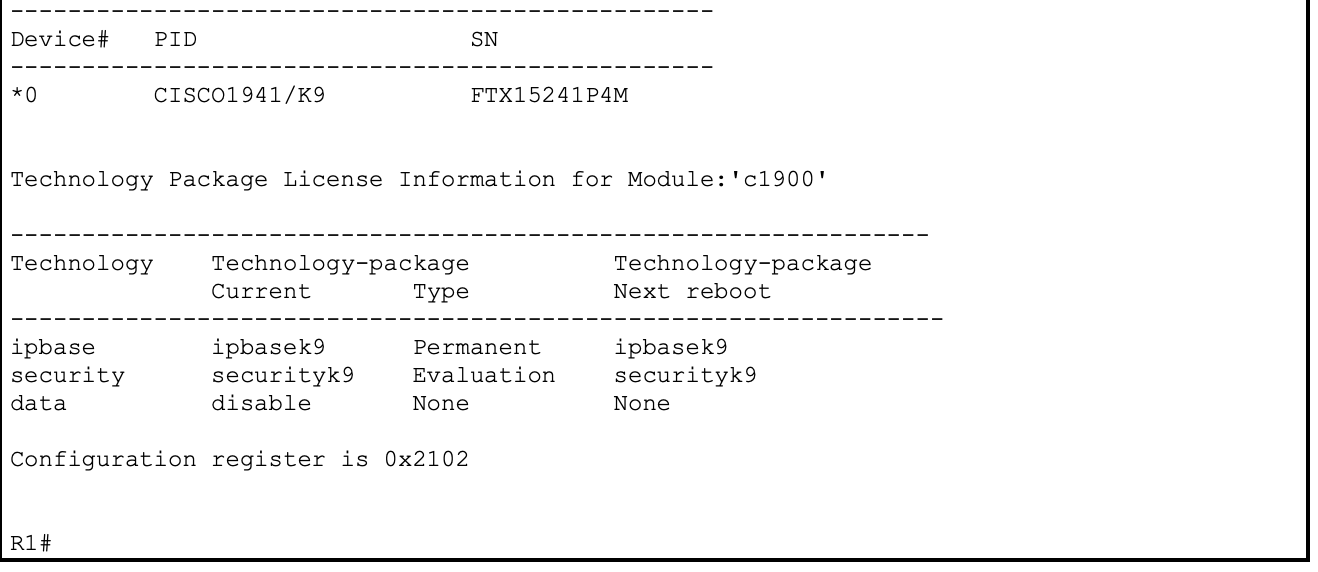
b.     Если пакет Security Technology не активирован, сделайте это с помощью следующей команды.

R1(config)# **license boot module c1900 technology-package securityk9**

c.     Примите условия лицензионного соглашения c конечным пользователем.

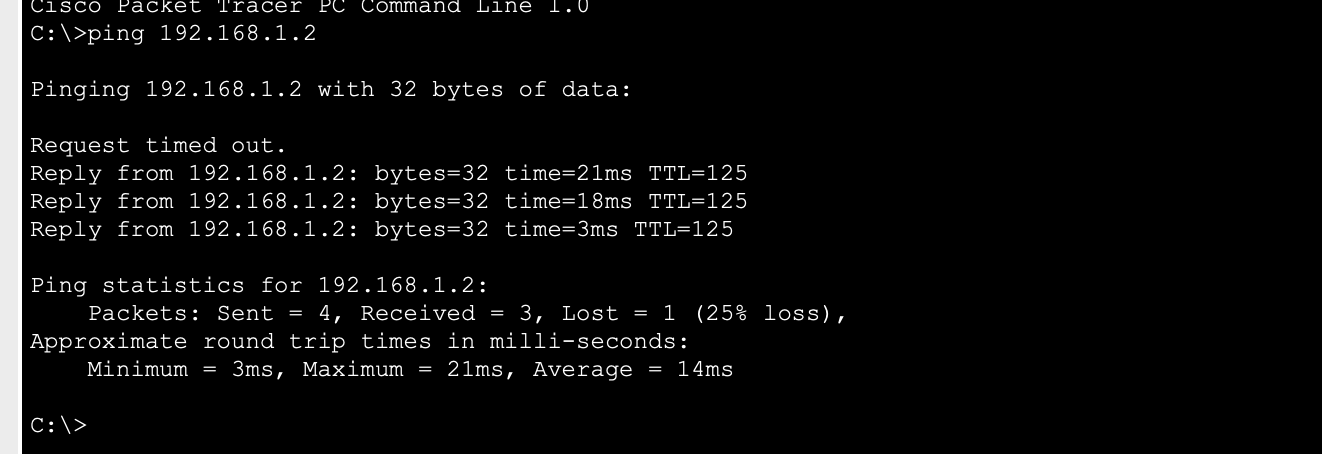
d.     Сохраните текущую конфигурацию и перезагрузите маршрутизатор, чтобы активировать лицензию Security Technology.

e.     Убедитесь, что пакет Security Technology активирован, c помощью команды **show version**.

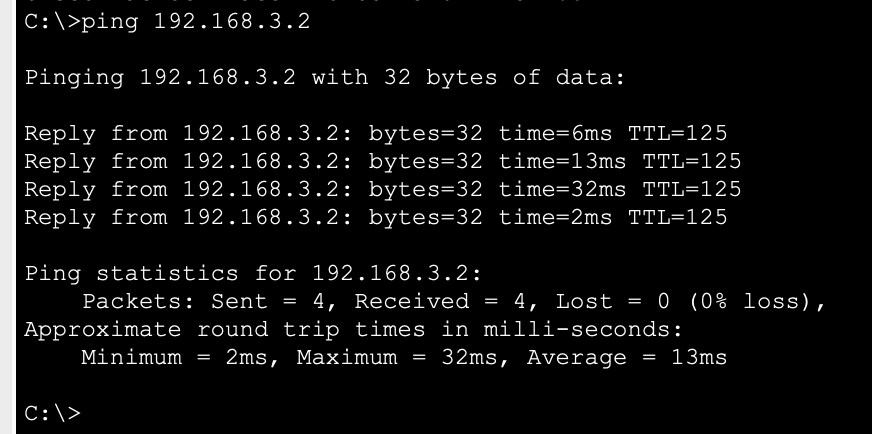


**Шаг 2. Проверка связи по сети**

1. Отправьте эхо-запрос c компьютера **PC-C** на компьютер **PC-A**. Эхо-запрос должен быть выполнен успешно.



1. Отправьте эхо-запрос c компьютера **PC-A** на компьютер **PC-C**. Эхо-запрос должен быть выполнен успешно.



**Шаг 3. Создайте каталог конфигураций IPS в IOS во флеш-памяти.**

На маршрутизаторе **R1** создайте каталог во флеш-памяти c помощью команды **mkdir** . Присвойте каталогу имя **ipsdir**.

**Шаг 4. Настройте каталог для хранения сигнатур IPS.**

На маршрутизаторе **R1** задайте только что созданный каталог в качестве места хранения сигнатур IPS.

Команда - ip ips config location flash:ipsdir

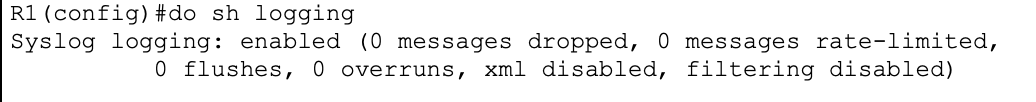
**Шаг 5. Создайте правило IPS.**

На маршрутизаторе **R1** создайте имя правила IPS c помощью команды **ip ips name***name* в режиме глобальной настройки. Присвойте правилу IPS имя **iosips**.

**Шаг 6. Включите ведение журналов.**

Система IPS в IOS поддерживает использование Syslog для отправки уведомлений о событиях. Функция уведомлений Syslog включена по умолчанию. Если консоль ведения журналов включена, будут отображаться сообщения Syslog, касающиеся IPS.

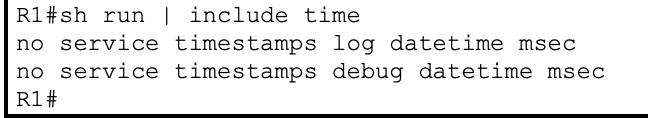
1. Если сервис Syslog не включен, включите его.



logging on

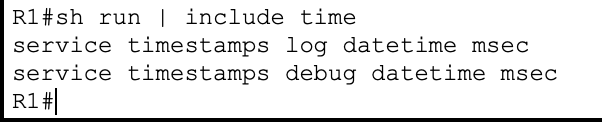
b.     При необходимости сбросьте часы c помощью команды **clock set** привилегированного режима.

c.     Убедитесь, что на маршрутизаторе включен сервис временных меток для ведения журналов, с помощью команды **show run**. Если сервис временных меток не включен, включите его.



service timestamps debug datetime msec

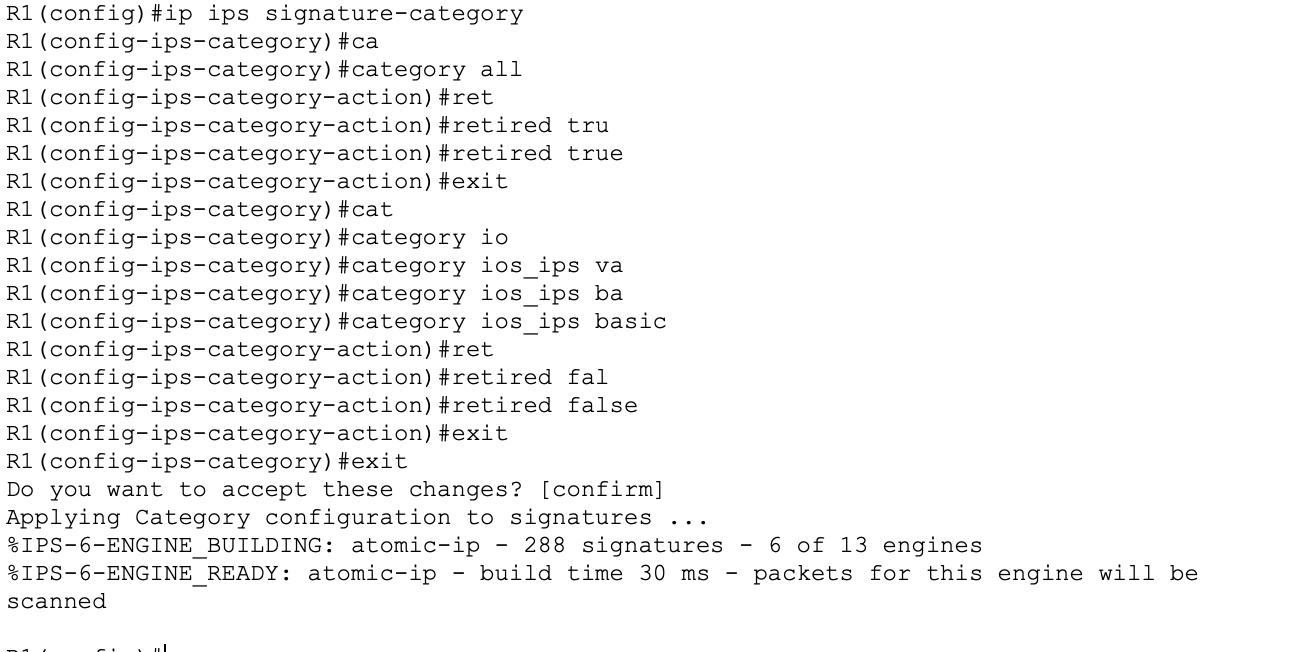
service timestamps log datetime msec



d.     Отправьте сообщения журналов на сервер Syslog по IP-адресу 192.168.1.50.

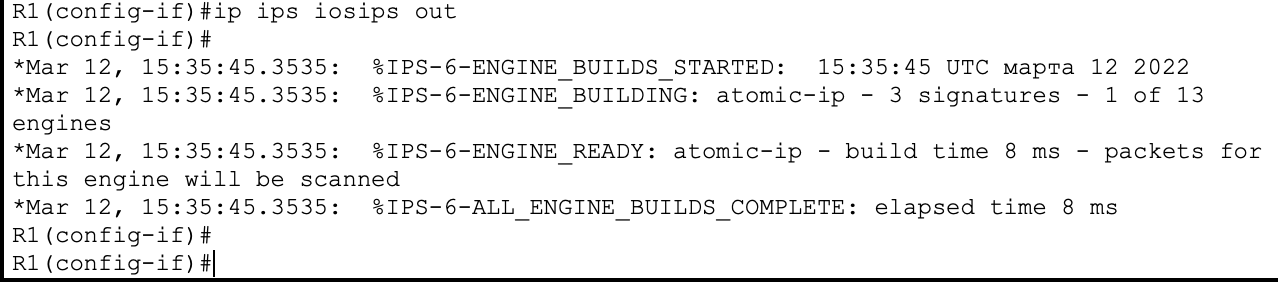
**Шаг 7. Настройте систему IPS в IOS для использования категорий сигнатур.**

Выведите из использования категорию сигнатур **all** с помощью команды **retired true** (все сигнатуры в выпуске сигнатур). Верните в использование категорию **IOS\_IPS Basic** c помощью команды **retired false** .



**Шаг 8. Примените к интерфейсу правило IPS.**

Примените к интерфейсу правило IPS c помощью команды **ip ips name***direction* в режиме настройки интерфейса. Примените правило к исходящему трафику (outbound) на интерфейсе G0/1 маршрутизатора **R1**. После включения IPS некоторые сообщения журнала будут отправлены на линию консоли, указывая, что выполняется инициализация модулей IPS.

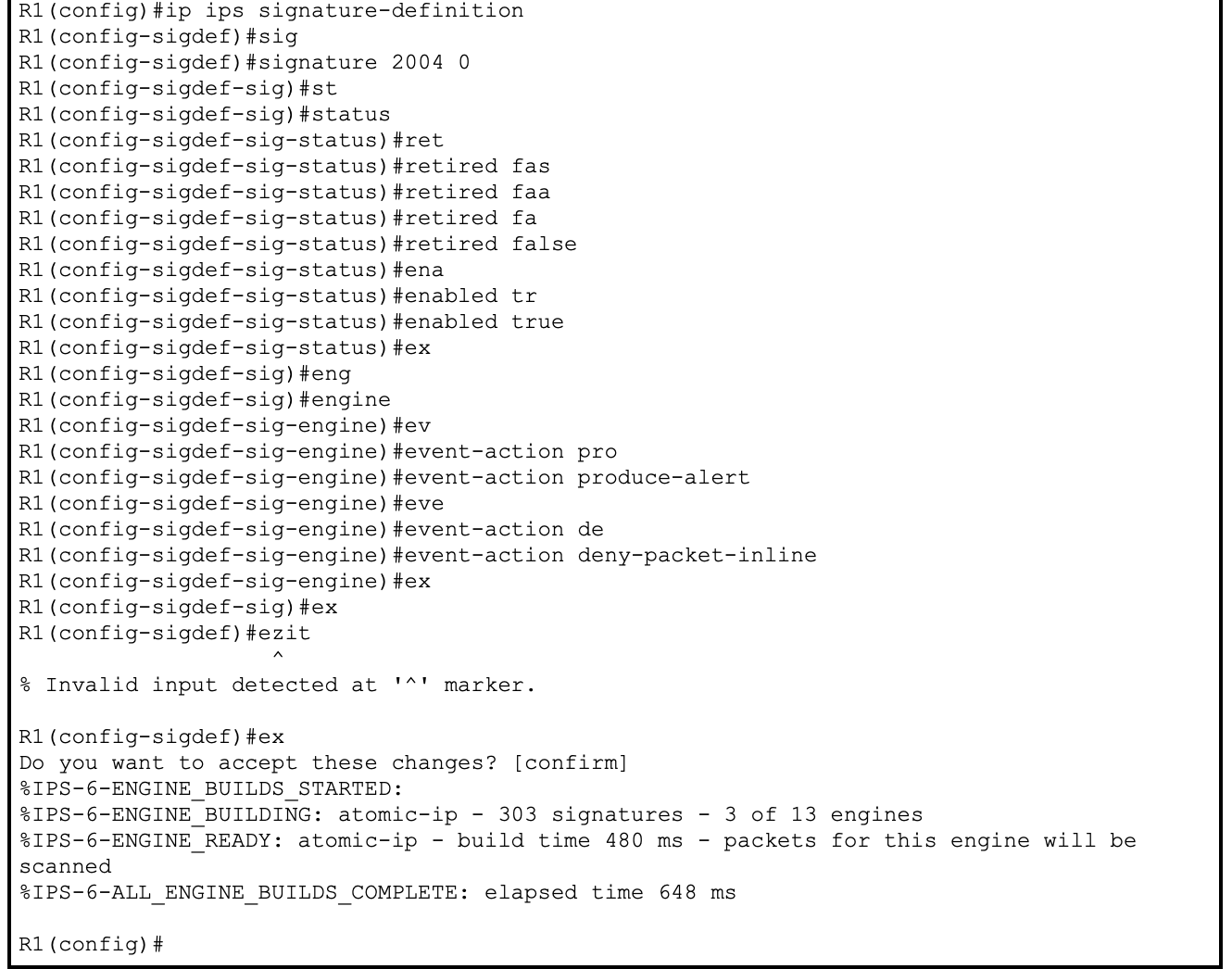


**Примечание**. Направление **in** означает, что система IPS проверяет только трафик, входящий на интерфейс. Аналогичным образом, направление **out** означает, что система IPS проверяет только трафик, исходящий из интерфейса.

**Часть 2. Изменение сигнатуры**

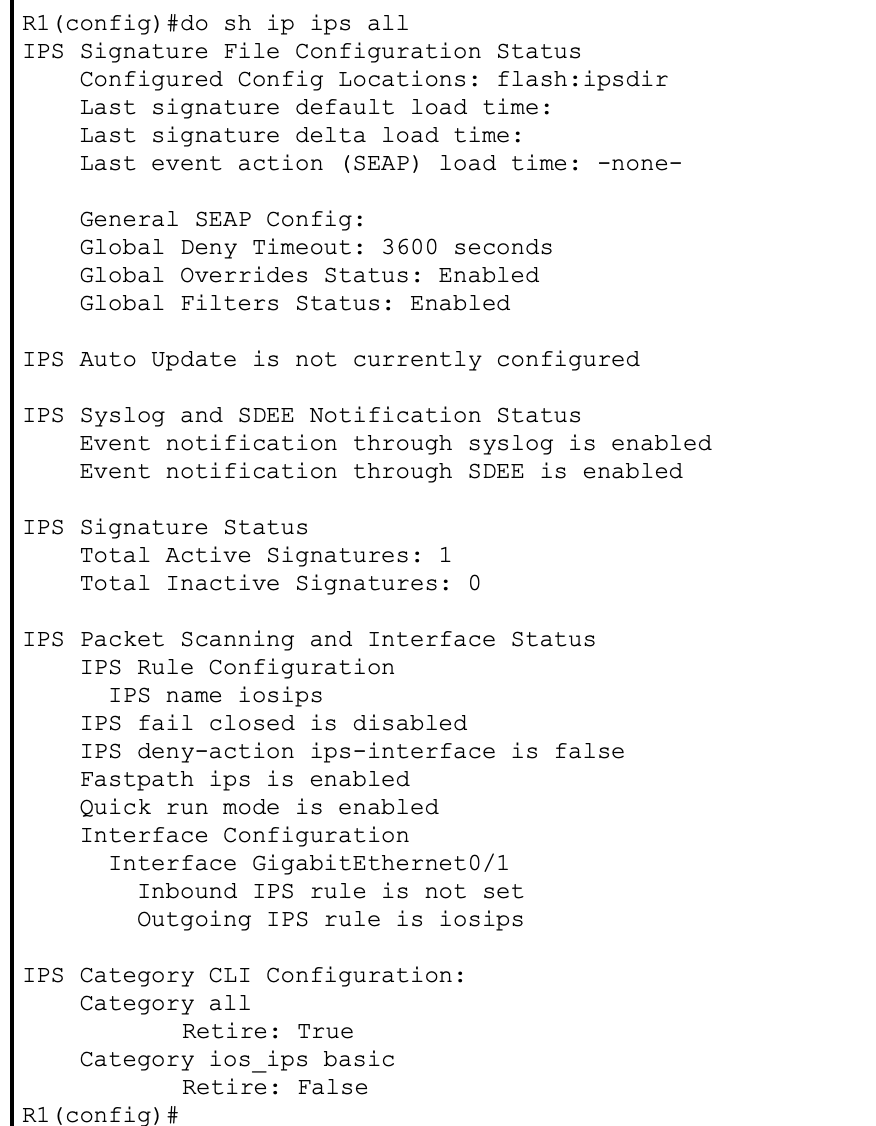
**Шаг 1. Измените для сигнатуры действие при наступлении события (параметр event-action).**

Верните в использование сигнатуру эхо-запроса (сигнатуру 2004, идентификатор subsig 0), включите ее и измените действие сигнатуры на оповещение и отбрасывание.



**Шаг 2. Проверьте IPS с помощью команд show.**

Используя команду **show ip ips all**, просмотрите сводку состояния конфигураций IPS.

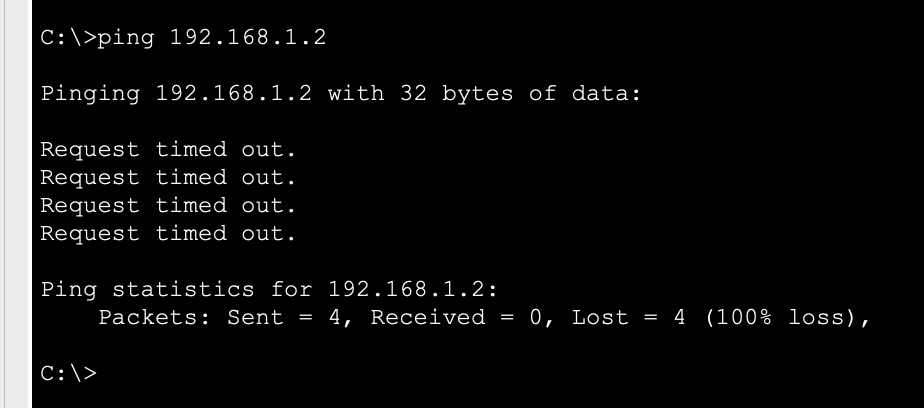


К каким интерфейсам в каком направлении применяется правило **iosips** ?

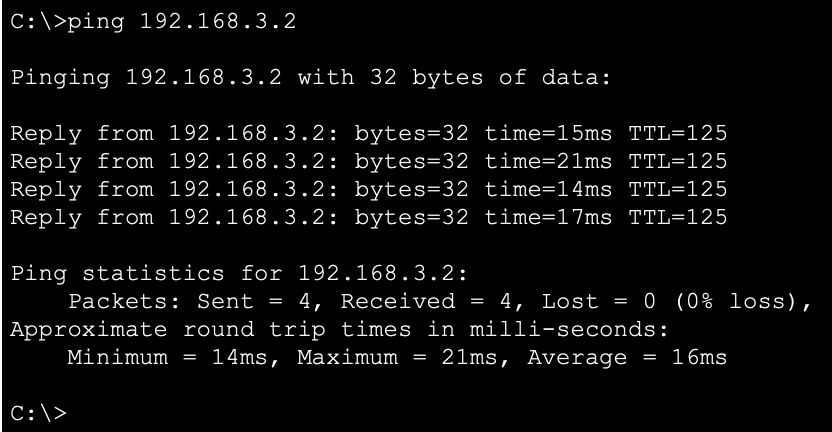
G0/1 out

**Шаг 3. Проверьте правильность работы IPS.**

1. Попробуйте отправить эхо-запрос c компьютера **PC-C** на **PC-A**. Эхо-запросы выполнены успешно? Поясните ответ.



1. Попробуйте отправить эхо-запрос c компьютера **PC-A** на **PC-C**. Эхо-запросы выполнены успешно? Поясните ответ.

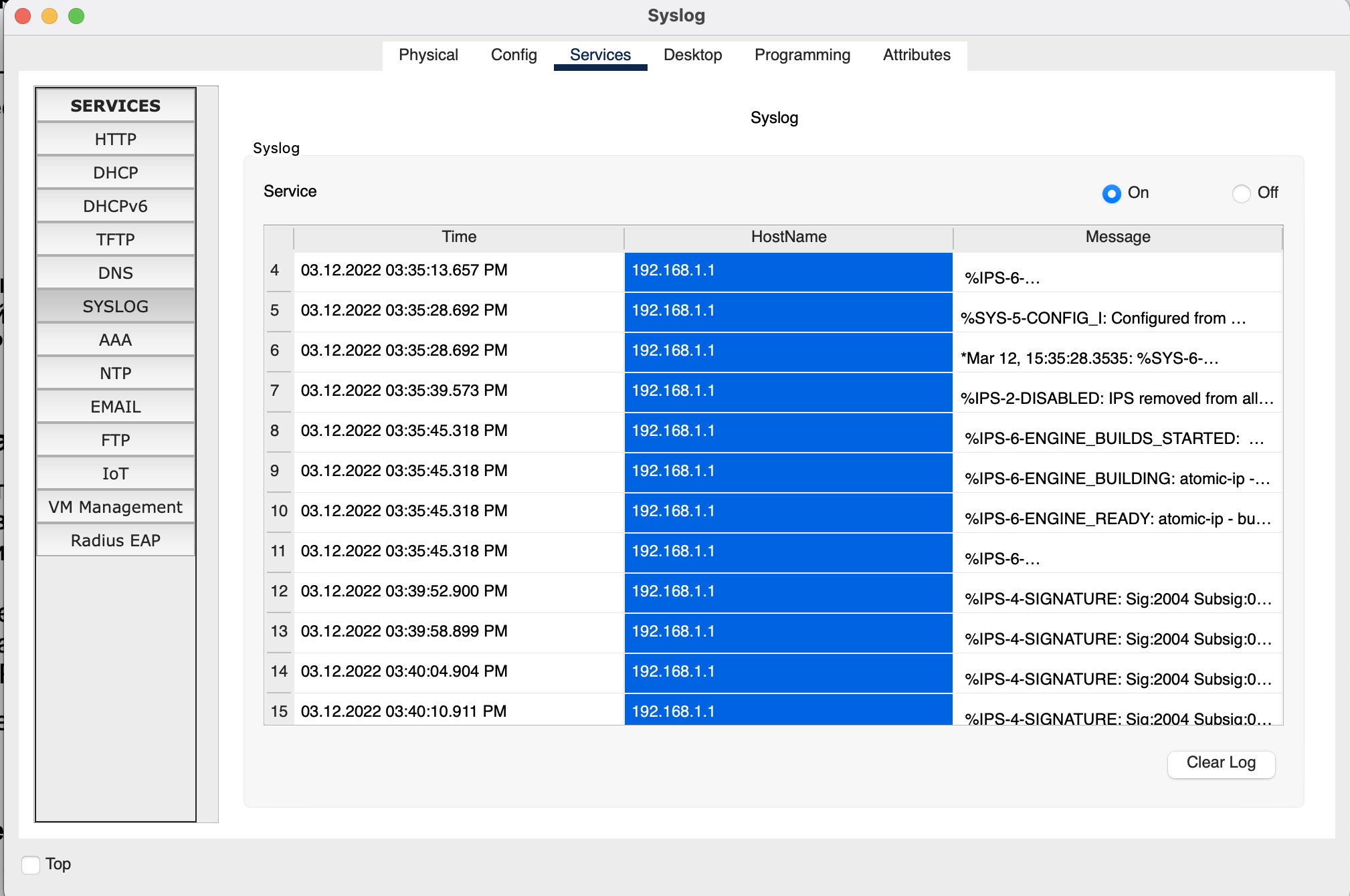


**Шаг 4. Просмотрите сообщения Syslog.**

a.     Выберите сервер **Syslog**.

b.     Перейдите на вкладку **Services**.

c.     В левом меню навигации выберите **SYSLOG** для просмотра файла журнала.

****

**Шаг 5. Проверьте результаты.**

Вы полностью выполнили задание. Нажмите **Check Results** (Проверить результаты) для просмотра отзыва и проверки завершенных обязательных компонентов.

