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

Топология

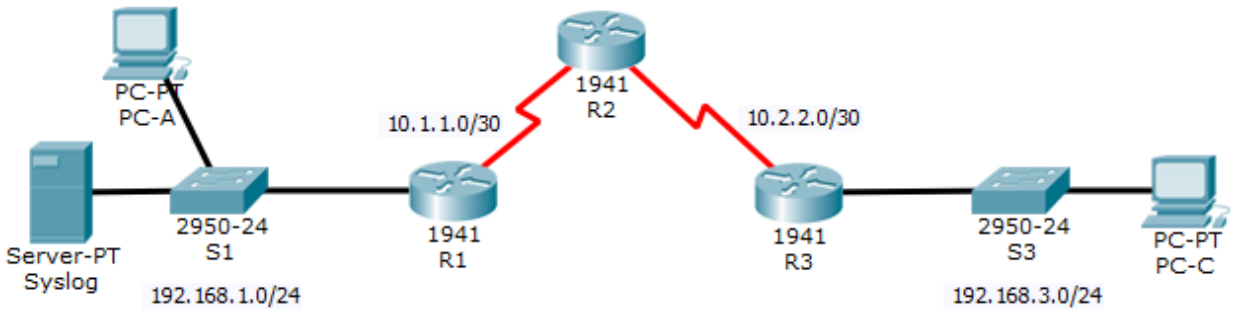

Таблица адресации

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 IOS IPS.
- Настройка ведения журнала.
- Изменение сигнатуры IPS.
- Проверка IPS.

Исходные данные/сценарий

Ваша задача – включить систему 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. При использовании сервиса Syslog для мониторинга сети очень важно, чтобы в сообщениях syslog отображались правильные дата и время. 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.

- Пароль привилегированного доступа: **ciscoenpa55**
- Пароль консоли: **ciscoconpa55**
- Имя пользователя и пароль SSH: **SSHadmin/ciscosshpa55**
- OSPF 101

Часть 1: Включение IOS IPS

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 с конечным пользователем.

d. Сохраните текущую конфигурацию и перезагрузите маршрутизатор, чтобы включить лицензию.

e. Убедитесь, что пакет Security Technology включен, с помощью команды **show version**.

Шаг 2: Проверка связи по сети.

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

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

Шаг 3: Создание каталога конфигурации IOS IPS во флеш-памяти.

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

Шаг 4: Настройка каталога для хранения сигнатур IPS.

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

Шаг 5: Создание правила IPS.

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

Шаг 6: Включение ведения журнала.

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.

a. Если сервис Syslog не включен, включите его.

b. При необходимости сбросьте часы с помощью команды **clock set** в привилегированном режиме.

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.

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

Шаг 7: Настройка системы IPS в IOS на использование 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** с помощью команды **retired false**.

Шаг 8: Применение к интерфейсу правила IPS.

Примените к интерфейсу правило IPS с помощью команды **ip ips name** *direction* в режиме настройки интерфейса. Примените правило для исходящего трафика (outbound) на интерфейсе G0/1 маршрутизатора R1. После включения IPS некоторые журнальные сообщения будут отправлены на линию консоли, указывая на выполнение инициализации механизмов 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: Изменение для сигнатуры действия при наступлении события (параметр event-action).

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

Шаг 2: Проверка IPS с помощью команд show.

Используйте команду **show ip ips all** для просмотра сводки состояний конфигураций IPS.

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

_____

Шаг 3: Проверка правильности работы IPS.

a. Попробуйте отправить эхо-запрос с компьютера **PC-C** на **PC-A**. Эхо-запрос выполнен успешно? Поясните ответ.

_____

_____

b. Попробуйте отправить эхо-запрос с компьютера **PC-A** на **PC-C**. Эхо-запрос выполнен успешно? Поясните ответ.

_____

_____

Шаг 4: Просмотр сообщений Syslog.

a. Выберите сервер **Syslog**.

b. Перейдите на вкладку **Services**.

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

Шаг 5: Проверка результатов.

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

