CCNA Security

Лабораторная работа. Настройка системы предотвращения вторжений (IPS)

Топология

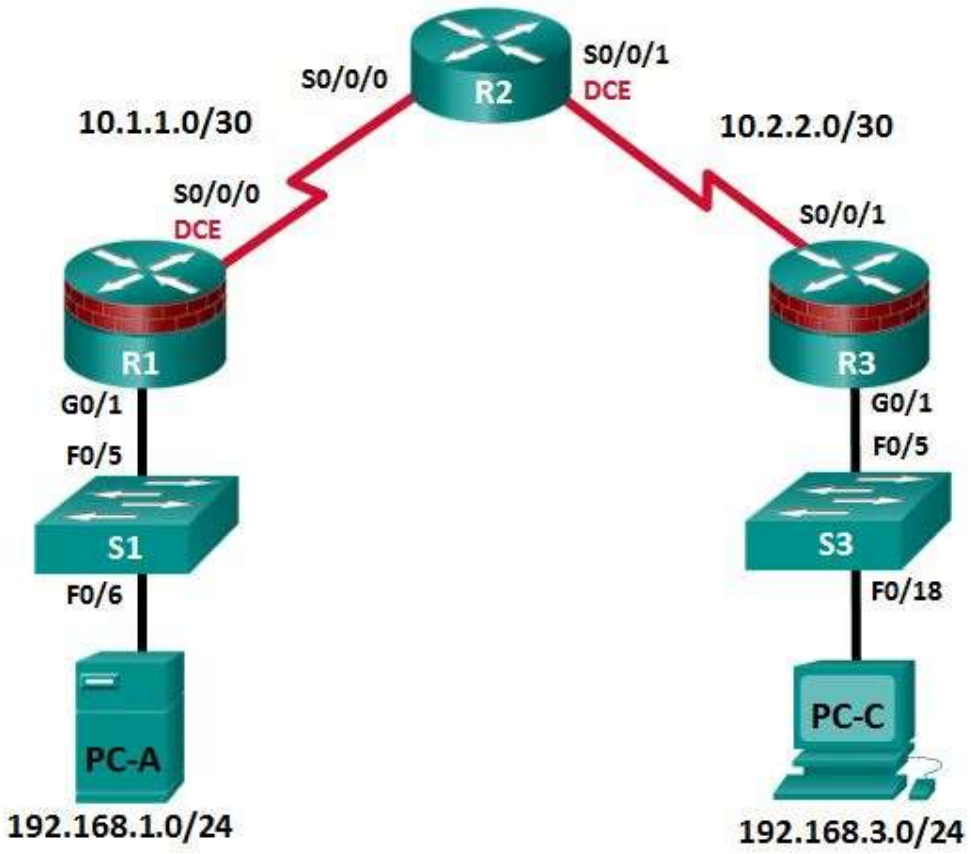


Таблица IP-адресов

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	G0/1	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-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Задачи

Часть 1. Настройка базовых параметров маршрутизатора

- Настройте имена хостов, IP-адреса интерфейсов и пароли для доступа.
- Настройте статическую маршрутизацию.

Часть 2. Настройка IOS IPS с помощью CLI

- Настройте IOS IPS с помощью CLI.
- Измените сигнатуры IPS.
- Рассмотрите итоговую конфигурацию IPS.
- Проверьте работоспособность IPS.
- Запишите сообщения журнала IPS на сервер syslog.

Часть 3. Имитация атаки

- Используйте инструмент сканирования для моделирования атаки.

Исходные данные/сценарий

В данной лабораторной работе необходимо настроить Cisco IOS IPS, которая является частью набора функционала межсетевого экрана Cisco IOS. Система предотвращения вторжений (IPS) изучает конкретные шаблоны атак и оповещает или противостоит подобным атакам, когда они случаются. Одной лишь системы IPS недостаточно для того, чтобы превратить маршрутизатор в надежный межсетевой экран для Интернета, но совместно с другими средствами безопасности организовать эффективную защиту можно.

Необходимо настроить IPS с помощью Cisco IOS CLI, а затем проверить работоспособность IPS. Вы загрузите пакет сигнатур IPS с сервера TFTP и сконфигурируете открытый криптографический ключ с помощью Cisco IOS.

Примечание. В данной лабораторной работе используются команды и выходные данные для маршрутизатора Cisco 1941 с ПО Cisco IOS версии 15.4(3)M2. 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. Доступные команды и выходные данные зависят от используемых моделей маршрутизаторов и версии Cisco IOS. Таким образом, они могут отличаться от того, что представлено 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)
- 2 коммутатора (Cisco 2960 или аналогичный)
- 2 ПК (Windows Vista или 7), сервер Tftpd32, Nmap/Zenmap, последняя версия Java, Internet Explorer и Flash Player)
- Последовательные кабели и кабели Ethernet, как показано на топологической схеме
- Консольные кабели для настройки сетевых устройств Cisco
- Пакет сигнатур IPS и файлы открытых криптографических ключей на компьютерах PC-A и PC-C (предоставляются инструктором)

Часть 1: Настройка базовых параметров маршрутизатора

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

Примечание. Выполните шаги, указанные в части 1, на всех трех маршрутизаторах. Ниже указана процедура только для маршрутизатора R1.

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 интерфейсов, как показано в таблице IP-адресов.

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

```
R1(config)# interface S0/0/0
R1(config-if)# clock rate 64000
```

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

```
R1(config)# no ip domain-lookup
```

Шаг 3: Настройте статическую маршрутизацию на маршрутизаторах.

a. Настройте статический маршрут по умолчанию от маршрутизатора R1 к R2 и от маршрутизатора R3 к R2, используя адрес IPv4 следующего узла.

b. Настройте статический маршрут от маршрутизатора R2 к LAN R1 (192.168.1.0) и статический маршрут от маршрутизатора R2 к LAN R3 (192.168.3.0) с помощью подходящих адресов IPv4 следующего узла.

Шаг 4: Настройте параметры IP для хостов.

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

Шаг 5: Проверьте базовую связь по сети.

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

Если запрос завершается с ошибкой, измените значения основных параметров устройства перед тем, как продолжить работу.

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

Если запрос завершается с ошибкой, измените значения основных параметров устройства перед тем, как продолжить работу.

Примечание. Если эхо-запрос с компьютера PC-A на компьютер PC-C выполнен успешно, это означает, что протокол статической маршрутизации настроен правильно и работает корректно. Если эхо-запрос был выполнен с ошибкой, но интерфейсы устройств активны и IP-адреса заданы верно, воспользуйтесь командами **show run** и **show ip route**, чтобы определить проблемы, связанные с протоколом маршрутизации.

Шаг 6: 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 надежным шифрованием.

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

Шаг 7: Сохраните основную текущую конфигурацию для каждого маршрутизатора.

Сохраните текущую конфигурацию в конфигурацию запуска в привилегированном режиме.

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


Часть 2: Настройка IPS с помощью Cisco IOS CLI

В части 2 данной лабораторной работы вы настроите IPS на маршрутизаторе R1 с помощью Cisco IOS CLI. Затем вы проверите итоговую конфигурацию.

Задача 1: Проверка доступа к сети LAN маршрутизатора R1 из R2

В этой задаче вы убедитесь, что без настройки IPS внешний маршрутизатор R2 может отправить эхо-запрос на интерфейс S0/0/0 маршрутизатора R1 и компьютер PC-A во внутренней сети LAN маршрутизатора R1.

Шаг 1: Отправьте эхо-запрос с маршрутизатора R2 на R1.

С маршрутизатора R2 отправьте эхо-запрос на интерфейс S0/0/0 маршрутизатора R1 по IP-адресу 10.1.1.1.

```
R2# ping 10.1.1.1
```

Если запрос завершается с ошибкой, измените значения основных параметров устройства перед тем, как продолжить работу.

Шаг 2: Отправьте эхо-запрос с маршрутизатора R2 на компьютер PC-A в локальной сети маршрутизатора R1.

Отправьте эхо-запрос с маршрутизатора R2 на компьютер PC-A в локальной сети маршрутизатора R1 по IP-адресу 192.168.1.3.

```
R2# ping 192.168.1.3
```

Если запрос завершается с ошибкой, измените значения основных параметров устройства перед тем, как продолжить работу.

Шаг 3: Отобразите текущую конфигурацию маршрутизатора R1 до настройки IPS.

Введите команду **show run** для проверки текущей базовой конфигурации маршрутизатора R1.

Есть ли какие-то команды безопасности, относящиеся к IPS?

_____

_____

_____

Задача 2: Подготовка маршрутизатора и сервера TFTP

Шаг 1: Убедитесь в наличии файлов Cisco IOS IPS.

Для настройки Cisco IPS 5.x необходимо, чтобы на компьютере PC-A были доступны файл пакета сигнатур IOS IPS и файл открытых криптографических ключей. Если данных файлов нет на компьютере, обратитесь к инструктору. Файлы можно скачать с сайта www.cisco.com, используя действительную учетную запись пользователя после успешной авторизации.

a. Убедитесь, что файл IOS-S*xxx*-CLI.pkg находится в папке TFTP. Это пакет сигнатур. Буквами *xxx* в имени файла обозначается номер версии, который зависит от загруженного файла.

b. Убедитесь, что имеется файл realm-cisco.pub.key.txt, запомните его расположение на компьютере PC-A. Это открытый криптографический ключ, используемый в IOS IPS.

Шаг 2: Проверьте или создайте каталог IPS во флеш-памяти маршрутизатора R1.

a. На данном шаге вы проверите наличие каталога или создадите каталог во флеш-памяти маршрутизатора, в котором будут храниться требуемые файлы сигнатур и конфигурации.

Примечание. Вы также можете использовать USB-накопитель, подключенный к USB-порту маршрутизатора, для хранения файлов сигнатур и конфигураций. USB-накопитель должен быть постоянно подключен к указанному порту маршрутизатора, если он используется в качестве хранилища для конфигурации IOS IPS. IOS IPS также поддерживает любую файловую систему Cisco IOS в качестве места хранения конфигурации с соответствующим доступом на запись.

b. Из командной строки маршрутизатора R1 отобразите содержимое флеш-памяти с помощью команды **show flash** и проверьте наличие каталога **ipsdir**.

```
R1# show flash
```

c. Если каталог **ipsdir** отсутствует, создайте его в привилегированном режиме.

```
R1# mkdir ipsdir
Create directory filename [ipsdir]? <Enter>
Created dir flash:ipsdir
```

d. Если каталог уже существует, появится следующее сообщение:

```
%Error Creating dir flash:ipsdir (Can't create a file that exists)
```

Используйте команду **delete** для удаления содержимого каталога **ipsdir.**

```
R1# delete flash:ipsdir/*
Delete filename [/ipsdir/*]?
Delete flash:/ipsdir/R1-sigdef-default.xml? [confirm]
Delete flash:/ipsdir/R1-sigdef-delta.xml? [confirm]
Delete flash:/ipsdir/R1-sigdef-typedef.xml? [confirm]
Delete flash:/ipsdir/R1-sigdef-category.xml? [confirm]
Delete flash:/ipsdir/R1-seap-delta.xml? [confirm]
Delete flash:/ipsdir/R1-seap-typedef.xml? [confirm]
```

Примечание. Используйте данную команду с осторожностью. Если каталог **ipsdir** пуст, появится следующее сообщение:

```
R1# delete flash:ipsdir/*
Delete filename [/ipsdir/*]?
No such file
```

e. С помощью CLI маршрутизатора R1 убедитесь, что каталог существует. Используйте команду **dir flash:** или **dir flash:ipsdir.**

```
R1# dir flash:
Directory of flash:/

    1  -rw-    75551300  Feb 16 2015 01:53:10 +00:00  c1900-universalk9-mz.SPA.154-3.M2.bin
    2  drw-           0  Mar 8  2015 12:38:14 +00:00  ipsdir
```

или

```
R1# dir flash:ipsdir

Directory of flash:/ipsdir/

No files in directory
```

Примечание. Каталог существует, но в нем на данный момент отсутствуют файлы.

Задача 3: Настройка криптографического ключа IPS

Криптографический ключ проверяет цифровую подпись для главного файла сигнатур (sigdef-default.xml). Содержимое подписывается с помощью закрытого ключа Cisco, чтобы гарантировать подлинность и целостность при каждом выпуске.

Шаг 1: Скопируйте файл криптографических ключей на маршрутизатор R1.

В режиме глобальной настройки выберите и скопируйте файл криптографического ключа с именем **realm-cisco.pub.key.txt**.

```
crypto key pubkey-chain rsa
 named-key realm-cisco.pub signature
  key-string
   30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
   00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
   17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
   B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
   5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
   FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
   50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
   006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
   2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
   F3020301 0001
  quit
```

Шаг 2: Примените содержимое текстового файла на маршрутизаторе.

a. В привилегированном режиме на маршрутизаторе R1 войдите в режим глобальной настройки с помощью команды **conf t.**

b. Вставьте содержимое криптографического ключа в запросе режима глобальной настройки.

```
R1(config)#
R1(config)# crypto key pubkey-chain rsa
R1(config-pubkey-chain)# named-key realm-cisco.pub signature
R1(config-pubkey-key)# key-string
Enter a public key as a hexidecimal number ....

R1(config-pubkey)#$2A864886 F70D0101 01050003 82010F00 3082010A 02820101
R1(config-pubkey)#$D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
R1(config-pubkey)#$912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
R1(config-pubkey)#$085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
R1(config-pubkey)#$0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
R1(config-pubkey)#$994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
R1(config-pubkey)#$5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
R1(config-pubkey)#$A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
R1(config-pubkey)#$80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
R1(config-pubkey)#   F3020301 0001
R1(config-pubkey)#  quit
R1(config-pubkey-key)#
```

c. Выйдите из режима глобальной настройки и введите команду **show run,** чтобы убедиться, что криптографический ключ настроен.

Задача 4: Настройка IPS

Шаг 1: Создайте правило IPS.

a. На маршрутизаторе R1 создайте имя правила IPS с помощью команды **ip ips name name** в режиме глобальной настройки. Присвойте правилу IPS имя **iosips**. Оно будет использовано в дальнейшем на интерфейсе для включения IPS.

```
R1(config)# ip ips name iosips
```

b. Вы можете по выбору указать либо расширенный, либо стандартный список контроля доступа (ACL) для фильтрации трафика, который будет сканироваться правилом с этим именем. Весь трафик, разрешенный списком ACL, будет инспектироваться системой IPS. Трафик, отклоняемый списком ACL, системой IPS инспектироваться не будет.

c. Чтобы посмотреть варианты указания списка ACL с помощью имени правила, используйте команду **ip ips name** и функцию справки CLI (?).

```
R1(config)# ip ips name ips list ?
  <1-199>  Numbered access list
  WORD     Named access list
```

Шаг 2: Укажите местоположение хранилища сигнатур IPS во флеш-памяти маршрутизатора.

Файлы IPS будут храниться в каталоге **ipsdir**, созданном в задаче 2, часть 2. Укажите его местоположение с помощью команды **ip ips config location.**

```
R1(config)# ip ips config location flash:ipsdir
```

Шаг 3: Включите уведомление о событиях IPS SDEE.

Сервер Cisco Security Device Event Exchange (SDEE) построен на основе протокола Simple Object Access Protocol (SOAP), спецификации формата оповещений IDS и транспортных протоколов. SDEE заменяет Cisco RDEP.

Для использования SDEE необходимо включить HTTP-сервер с помощью команды **ip http server.** Если HTTP-сервер не включен, маршрутизатор не сможет отвечать клиентам SDEE, так как он не увидит запросы. Уведомления SDEE по умолчанию отключены и должны быть явно включены.

```
R1(config)# ip http server
```

Для включения SDEE используйте следующую команду:

```
R1(config)# ip ips notify sdee
```

Шаг 4: Включите поддержку Syslog для IPS.

Система IOS IPS также поддерживает использование Syslog для отправки уведомлений. SDEE и Syslog могут использоваться независимо друг от друга или работать одновременно для отправки уведомлений о событиях IOS IPS. Функция уведомлений Syslog включена по умолчанию.

a. Если ведение журнала для консоли включено, отображаются сообщения журнала IPS Syslog. Если Syslog не включен, включите его.

```
R1(config)# ip ips notify log
```

b. С помощью команды **show clock** проверьте текущее время и дату для маршрутизатора. При необходимости сбросьте часы с помощью команды **clock set** в привилегированном режиме. В следующем примере показано, как установить время.

```
R1# clock set 01:20:00 8 march 2015
```

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.

```
R1(config)# service timestamps log datetime msec
```


d. Для отправки журнальных сообщений на сервер Syslog на компьютере PC-A используйте следующую команду:

```
R1(config)# logging 192.168.1.3
```

e. С помощью команды **show logging** определите тип и уровень ведения журнала на маршрутизаторе R1.

```
R1# show logging
```

Примечание. Проверьте наличие связи между маршрутизатором R1 и компьютером PC-A с помощью эхо-запроса с PC-A на IP-адрес **192.168.1.1** интерфейса Fa0/1 на R1. Если это сделать не удается, устраните проблему перед тем, как продолжить.

Ниже показано, как скачать один из бесплатных серверов syslog, если он не установлен на компьютере PC-A.

Шаг 5: (Необязательно) Скачайте и запустите сервер syslog.

Если сервер syslog в данный момент на компьютере PC-A отсутствует, вы можете скачать Tftpd32 с сайта http://tftpd32.jounin.net. Если сервер syslog имеется на ПК, перейдите к шагу 6.

Запустите ПО сервера syslog на компьютере PC-A, чтобы отправлять на него журнальные сообщения.

Шаг 6: Настройка IOS IPS на использование одной из предварительно заданных категорий сигнатур.

IOS IPS с сигнатурами в формате Cisco 5.x работает с категориями сигнатур так же, как это выполняют другие устройства Cisco IPS. Все сигнатуры предварительно разбиты по категориям, а сами категории имеют иерархическую структуру. Это позволяет классифицировать сигнатуры для более простой настройки и группирования.

Предупреждение. Категория сигнатур all содержит *все* сигнатуры в выпуске сигнатур. Не возвращайте в использование категорию all, так как IOS IPS не сможет одновременно компилировать и использовать все сигнатуры в выпуске. Маршрутизатору не хватит на это памяти.

Примечание. При настройке IOS IPS необходимо сначала вывести из использования все сигнатуры в категории all, а затем вернуть в использование выбранные категории сигнатур.

В следующем примере все сигнатуры категории **all** выведены из использования, а затем введена в использование категория **ios_ips basic**.

```
R1(config)# ip ips signature-category
R1(config-ips-category)# category all
R1(config-ips-category-action)# retired true
R1(config-ips-category-action)# exit
R1(config-ips-category)# category ios_ips basic
R1(config-ips-category-action)# retired false
R1(config-ips-category-action)# exit
R1(config-ips-category)# exit
Do you want to accept these changes? [confirm] <Enter>

Jan  6 01:32:37.983: Applying Category configuration to signatures ...
```

Шаг 7: Примените к интерфейсу правило IPS.

a. Примените к интерфейсу правило IPS с помощью команды **ip ips** *name direction* в режиме настройки интерфейса. Примените только что созданное правило для входящего трафика на интерфейсе S0/0/0. После включения IPS некоторые журнальные сообщения будут отправлены на линию консоли. Это означает, что в механизмах IPS выполняется инициализация.

Примечание. Направление **in** означает, что система IPS проверяет только трафик, входящий на интерфейс. Аналогичным образом, направление **out** означает только трафик, исходящий из интерфейса. Чтобы IPS проверял входящий и исходящий трафик, введите имя правила IPS отдельно для направлений in и out на интерфейсе.

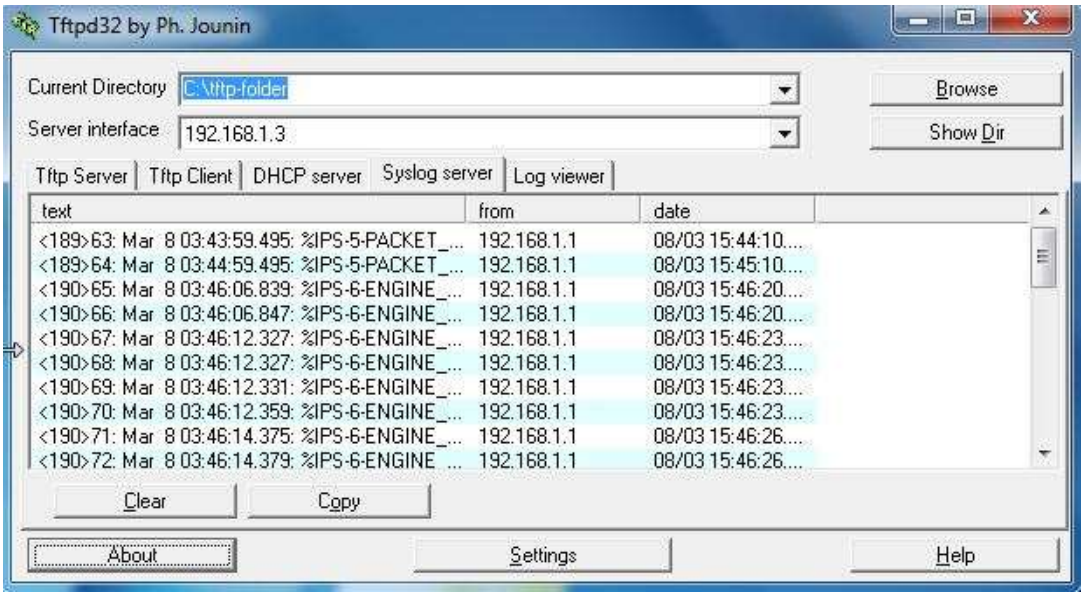

```
R1(config)# interface serial0/0/0
R1(config-if)# ip ips iosips in


Jan  6 03:03:30.495: %IPS-6-ENGINE_BUILDS_STARTED:  03:03:30 UTC Jan 6 2008
Jan  6 03:03:30.495: %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13 engines
Jan  6 03:03:30.511: %IPS-6-ENGINE_READY: atomic-ip - build time 16 ms – packets for this engine
will be scanned
Jan  6 03:03:30.511: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 16 ms
```

Это сообщение также появится на сервере syslog, если он включен. Ниже показаны сообщения сервера syslog Tftpd32.

Примечание. Это сообщение может появиться только в том случае, если на маршрутизаторе нет встроенного файла сигнатур IOS.

```
**********************************************************************
The signature package is missing or was saved by a previous version
IPS Please load a new signature package
**********************************************************************
Jan  6 01:22:17.383: %IPS-3-SIG_UPDATE_REQUIRED: IOS IPS requires a signature update package
to be loaded
```



b. Несмотря на то что интерфейс Fa0/1 маршрутизатора R1 является внутренним, настройте на нем с помощью IPS режим реагирования на внутренние атаки. Примените правило IPS к интерфейсу Fa0/1 маршрутизатора R1 для входящего направления.

```
R1(config)# interface g0/1
R1(config-if)# ip ips iosips in
```

Шаг 8: Сохраните текущую конфигурацию.

Войдите в привилегированный режим и сохраните текущую конфигурацию в файл startup-config.

```
R1# copy run start
```


Задача 5: Загрузка пакета сигнатур IOS IPS на маршрутизатор

Самым распространенным способом загрузки пакета сигнатур IOS IPS на маршрутизатор является применение TFTP. Альтернативные варианты загрузки пакета сигнатур IOS IPS см. в описании шага 4. Эти варианты включают в себя применение FTP или USB-накопителя.

Шаг 1: (Необязательно) Скачайте сервер TFTP.

В данной задаче используется бесплатный TFTP-сервер Tftpd32. Также имеются и другие бесплатные TFTP-серверы. Если сервер TFTP в данный момент на компьютере PC-A отсутствует, вы можете скачать последнюю версию Tftpd32 с сайта http://tftpd32.jounin.net. Если он уже установлен, перейдите к шагу 2.

Примечание. В данной лабораторной работе используется TFTP-сервер Ttftpd32. В комплекте к нему также идет syslog-сервер, который запускается одновременно с сервером TFTP.

Шаг 2: Запустите TFTP-сервер на компьютере PC-A и проверьте каталог файлов IPS.

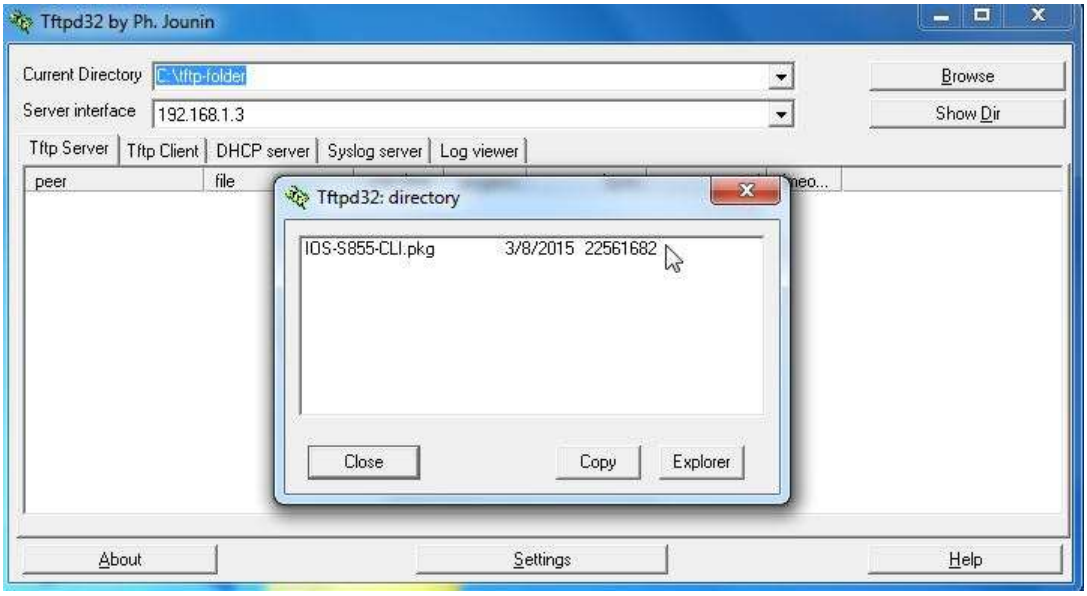
a. Используйте команду **ping** для проверки связи между маршрутизатором R1, компьютером PC-A и TFTP-сервером.

b. Проверьте, чтобы файл пакета сигнатур IPS компьютера ПК-C находился в каталоге на TFTP-сервере. Файл обычно называется IOS-S*xxx*-CLI.pkg, где *xxx* – версия файла сигнатур.

Примечание. Если этот файл отсутствует, обратитесь к инструктору перед тем, как продолжить.

c. Запустите Tftpd32 или другой TFTP-сервер, выберите для интерфейса сервера сетевой интерфейс компьютера PC-A (192.168.1.3), установите для каталога по умолчанию каталог, где содержится пакет сигнатур IPS. Ниже показан экран Tftpd32 с выбранным каталогом C:\tftp-folder\. Запишите имя файла, чтобы использовать его на следующем шаге.

Примечание. В производственной среде рекомендуется использовать файл сигнатур последней доступной версии. Однако если в данной лабораторной среде невозможно использовать маршрутизатор с требуемым размером флеш-памяти, можно использовать предыдущую версию файла сигнатур 5.x, которая требует меньшего объема памяти. В этой лабораторной работе используется файл S364, хотя доступны более новые версии. Определить самую последнюю версию для производственной среды можно с помощью CCO.



Шаг 3: Скопируйте пакет сигнатур с TFTP-сервера на маршрутизатор.

Если у вас нет сервера TFTP и вы используете маршрутизатор с USB-портом, перейдите к шагу 5 и выполните описанную в нем процедуру.

a. С помощью команды **copy tftp** получите файл сигнатур и загрузите его в конфигурацию обнаружения вторжений. В конце команды **copy** используйте ключевое слово **idconf**.

Примечание. Компилирование сигнатур начнется сразу после загрузки пакета сигнатур на маршрутизатор. При уровне ведения журнала 6 или выше вы сможете увидеть сообщения на маршрутизаторе.

```
# copy tftp://192.168.1.3/IOS-S855-CLI.pkg idconf
Loading IOS-S855-CLI.pkg from 192.168.1.3 (via GigabitEthernet0/1): !!!!!OO!!
Mar  8 03:43:59.495: %IPS-5-PACKET_UNSCANNED: atomic-ip - fail open - packets passed
unscanned!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Mar  8 03:44:59.495: %IPS-5-PACKET_UNSCANNED: atomic-ip - fail open - packets passed
unscanned!!!!!!!!!!!!!!!!
[OK - 22561682 bytes]


Mar  8 03:46:06.839: %IPS-6-ENGINE_BUILDS_STARTED:  03:46:06 UTC Mar 8 2015
Mar  8 03:46:06.847: %IPS-6-ENGINE_BUILDING: atomic-ip - 539 signatures - 1 of 13
engines
Mar  8 03:46:12.327: %IPS-6-ENGINE_READY: atomic-ip - build time 5480 ms - packets for
this engine will be scanned
Mar  8 03:46:12.327: %IPS-6-ENGINE_BUILDING: normalizer - 10 signatures - 2 of 13
engines
Mar  8 03:46:12.331: %IPS-6-ENGINE_READY: normalizer - build time 4 ms - packets for
this engine will be scanned
Mar  8 03:46:12.359: %IPS-6-ENGINE_BUILDING: service-http - 1837 signatures - 3 of 13
engines
Mar  8 03:46:14.375: %IPS-6-ENGINE_READY: service-http - build time 2016 ms - packets
for this engine will be scanned
Mar  8 03:46:14.379: %IPS-6-ENGINE_BUILDING: service-smb-advanced - 76 signatures - 4
of 13 engines
Mar  8 03:46:15.003: %IPS-6-ENGINE_READY: service-smb-advanced - build time 624 ms -
packets for this engine will be scanned
Mar  8 03:46:15.003: %IPS-6-ENGINE_BUILDING: service-msrpc - 37 signatures - 5 of 13
engines
Mar  8 03:46:15.107: %IPS-6-ENGINE_READY: service-msrpc - build time 104 ms - packets
for this engine will be scanned
Mar  8 03:46:15.111: %IPS-6-ENGINE_BUILDING: state - 39 signatures - 6 of 13 engines
Mar  8 03:46:15.203: %IPS-6-ENGINE_READY: state - build time 92 ms - packets for this
engine will be scanned
Mar  8 03:46:15.203: %IPS-6-ENGINE_BUILDING: service-ftp - 3 signatures - 7 of 13
engines
Mar  8 03:46:15.207: %IPS-6-ENGINE_READY: service-ftp - build time 4 ms - packets for
this engine will be scanned
Mar  8 03:46:15.271: %IPS-6-ENGINE_BUILDING: string-tcp - 3782 signatures - 8 of 13
engines
Mar  8 03:46:19.887: %IPS-6-ENGINE_READY: string-tcp - build time 4616 ms - packets
for this engine will be scanned
```



```
Mar  8 03:46:19.895: %IPS-6-ENGINE_BUILDING: service-rpc - 79 signatures - 9 of 13
engines
Mar  8 03:46:19.991: %IPS-6-ENGINE_READY: service-rpc - build time 96 ms - packets for
this engine will be scanned
Mar  8 03:46:19.991: %IPS-6-ENGINE_BUILDING: service-dns - 39 signatures - 10 of 13
engines
Mar  8 03:46:20.027: %IPS-6-ENGINE_READY: service-dns - build time 36 ms - packets for
this
R1#
R1# engine will be scanned
Mar  8 03:46:20.027: %IPS-6-ENGINE_BUILDING: string-udp - 80 signatures - 11 of 13
engines
Mar  8 03:46:20.087: %IPS-6-ENGINE_READY: string-udp - build time 60 ms - packets for
this engine will be scanned
Mar  8 03:46:20.099: %IPS-6-ENGINE_BUILDING: multi-string - 614 signatures - 12 of 13
engines
Mar  8 03:46:20.803: %IPS-6-ENGINE_READY: multi-string - build time 700 ms - packets
for this engine will be scanned
Mar  8 03:46:20.803: %IPS-6-ENGINE_BUILDING: string-icmp - 3 signa
R1#tures - 13 of 13 engines
Mar  8 03:46:20.803: %IPS-6-ENGINE_READY: string-icmp - build time 0 ms - packets for
this engine will be scanned
Mar  8 03:46:20.803: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 13964 ms
```

b. Используйте команду **dir flash** для просмотра содержимого каталога **ipsdir**, который вы создали ранее. В нем должно быть шесть файлов, как показано далее.

```
R1# dir flash:ipsdir
Directory of flash0:/ipsdir/

    4  -rw-         255   Mar 8 2015 02:45:40 +00:00  iosips-sig-delta.xmz
    5  -rw-       16625   Mar 8 2015 03:43:52 +00:00  iosips-sig-typedef.xmz
    6  -rw-      143832   Mar 8 2015 03:43:58 +00:00  iosips-sig-category.xmz
    7  -rw-         304   Mar 8 2015 02:45:42 +00:00  iosips-seap-delta.xmz
    8  -rw-         835   Mar 8 2015 02:45:42 +00:00  iosips-seap-typedef.xmz
    9  -rw-     1632555   Mar 8 2015 03:45:18 +00:00  iosips-sig-default.xmz
```

Шаг 4: Убедитесь, что пакет сигнатур скомпилирован корректно.

a. С помощью команды **show ip ips signature count** просмотрите количество скомпилированных пакетов сигнатур.

```
R1# show ip ips signature count

Cisco SDF release version S364.0
Trend SDF release version V0.0

Signature Micro-Engine: multi-string: Total Signatures 11
      multi-string enabled signatures: 9
      multi-string retired signatures: 11
```



```
Signature Micro-Engine: service-http: Total Signatures 662
      service-http enabled signatures: 163
      service-http retired signatures: 565
      service-http compiled signatures: 97
      service-http obsoleted signatures: 1

Signature Micro-Engine: string-tcp: Total Signatures 1148
      string-tcp enabled signatures: 622
      string-tcp retired signatures: 1031
      string-tcp compiled signatures: 117
      string-tcp obsoleted signatures: 21

<Output Omitted>

Total Signatures: 2435
   Total Enabled Signatures: 1063
   Total Retired Signatures: 2097
   Total Compiled Signatures: 338
   Total Obsoleted Signatures: 25
```

Примечание. Если во время компиляции сигнатур вы видите сообщения об ошибках, такие как %IPS-3-INVALID_DIGITAL_SIGNATURE: Invalid Digital Signature found (key not found), это означает, что открытый криптографический ключ недействителен. Вернитесь к задаче 3 «Настройка криптографического ключа IPS», чтобы перенастроить открытый криптографический ключ.

b. Используйте команду **show ip ips all**, чтобы просмотреть сводку состояния конфигурации IPS. К каким интерфейсам и в каком направлении применяется правило iosips?

_____

_____

```
R1# show ip ips all

IPS Signature File Configuration Status
    Configured Config Locations: flash:ipsdir/
    Last signature default load time: 18:47:52 UTC Jan 6 2009
    Last signature delta load time: 20:11:35 UTC Jan 6 2009
    Last event action (SEAP) load time: -none-

    General SEAP Config:
    Global Deny Timeout: 3600 seconds
    Global Overrides Status: Enabled
    Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status
    Event notification through syslog is enabled
    Event notification through SDEE is enabled

IPS Signature Status
    Total Active Signatures: 339
    Total Inactive Signatures: 2096
```



```
IPS Packet Scanning and Interface Status
    IPS Rule Configuration
      IPS name iosips
    IPS fail closed is disabled
    IPS deny-action ips-interface is false
    Interface Configuration
      Interface Serial0/0/0
        Inbound IPS rule is iosips
        Outgoing IPS rule is not set
Interface FastEthernet0/1
        Inbound IPS rule is iosips
        Outgoing IPS rule is not set

IPS Category CLI Configuration:
    Category all:
        Retire: True
    Category ios_ips basic:
        Retire: False
```

Шаг 5: (Необязательно) Альтернативные методы копирования пакета сигнатур на маршрутизатор.

Если вы использовали TFTP для копирования файла и не будете использовать один из представленных альтернативных методов, ознакомьтесь с описанными здесь процедурами. Если вместо TFTP вы используете один из этих методов, вернитесь к шагу 4 и убедитесь, что пакет сигнатур загружен корректно.

Метод FTP. Несмотря на то что использование метода TFTP обычно оправдано, файл сигнатур обладает достаточно большим размером, и FTP может представлять собой другой метод копирования файла. Вы можете использовать сервер FTP для копирования файла сигнатур на маршрутизатор с помощью следующей команды:

```
copy ftp://<ftp_user:password@Server_IP_address>/<signature_package> idconf
```

В представленном примере на FTP-сервере должен быть определен пользователь **admin** с паролем **cisco.**

```
R1# copy ftp://admin:cisco@192.168.1.3/IOS-S855-CLI.pkg idconf
Loading IOS-S855-CLI.pkg !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 7608873/4096 bytes]
```

Метод USB. Если к серверу FTP или TFTP доступа нет, вы можете использовать USB-накопитель для загрузки пакета сигнатур на маршрутизатор.

a. Скопируйте пакет сигнатур на USB-накопитель.

b. Подключите USB-накопитель к одному из USB-портов маршрутизатора.

c. С помощью команды **show file systems** отобразите имя USB-накопителя. В представленных выходных данных USB-накопитель объемом 4 ГБ подключен к USB-порту маршрутизатора в качестве файловой системы usbflash0:

```
R1# show file systems
File Systems:

       Size(b)       Free(b)      Type  Flags  Prefixes
             -             -    opaque     rw   archive:
             -             -    opaque     rw   system:
             -             -    opaque     rw   tmpsys:
             -             -    opaque     rw   null:
```



```
               -            -   network     rw   tftp:
          196600       185972     nvram     rw   nvram:
*      64012288     14811136      disk     rw   flash:#
               -            -    opaque     wo   syslog:
               -            -    opaque     rw   xmodem:
               -            -    opaque     rw   ymodem:
               -            -   network     rw   rcp:
               -            -   network     rw   pram:
               -            -   network     rw   http:
               -            -   network     rw   ftp:
               -            -   network     rw   scp:
               -            -    opaque     ro   tar:
               -            -   network     rw   https:
               -            -    opaque     ro   cns:
     4001378304   3807461376  usbflash     rw   usbflash0:
```

d. Проверьте содержимое флеш-накопителя с помощью команды **dir.**

```
R1# dir usbflash0:
Directory of usbflash0:/

  1  -rw-         807   Mar 8 2015 13:20:12 +00:00  realm-cisco.pub.key
  2  -rw-    22561682   Mar 8 2015 09:57:38 +00:00  IOS-S855-CLI.pkg
```

e. Используйте команду **copy** с ключевым словом **idconf** для копирования пакета сигнатур на маршрутизатор.

```
R1# copy usbflash0:IOS-S855-CLI.pkg idconf
```

Процесс копирования по USB может занимать более минуты, и при этом не будет отображаться индикатор прогресса. По окончании процесса копирования будет отображено много вспомогательных сообщений. Они должны перестать появляться до того, как появится командная строка.

Задача 6: Проверка правила IPS и изменение сигнатуры

Для работы с сигнатурами можно использовать различные способы. Их можно вводить и выводить из использования, включать и выключать, а также изменять их характеристики и действия. В этой задаче вы сначала проверите поведение системы IOS IPS по умолчанию, отправив эхо-запрос на него из внешней среды.

Шаг 1: Отправьте эхо-запрос с маршрутизатора R2 на последовательный интерфейс 0/0/0 маршрутизатора R1.

Из CLI маршрутизатора R2 отправьте эхо-запрос на интерфейс S0/0/0 маршрутизатора R1 по IP-адресу **10.1.1.1**. Этот запрос будет выполнен успешно, так как сигнатура ICMP Echo Request 2004:0 выведена из использования.

Шаг 2: Отправьте эхо-запрос с маршрутизатора R2 на компьютер PC-A.

С CLI маршрутизатора R2 отправьте эхо-запрос на компьютер PC-A по IP-адресу **192.168.1.3**. Этот запрос также будет выполнен успешно из-за выведенной из использования сигнатуры. Таково поведение сигнатур IPS по умолчанию.

```
R2# ping 192.168.1.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```


Шаг 3: Измените сигнатуру.

Вы можете использовать Cisco IOS CLI для изменения состояния и действий сигнатуры для одной из сигнатур или целой группы сигнатур в соответствии с категориями сигнатур.

В следующем примере показано, как вернуть в использование сигнатуру эхо-запроса, включить ее, изменить действие сигнатуры на оповещение, а также отклонить и выполнить сброс для сигнатуры 2004 с идентификатором subsig 0.

```
R1(config)# ip ips signature-definition
R1(config-sigdef)# signature 2004 0
R1(config-sigdef-sig)#status
R1(config-sigdef-sig-status)# retired false
R1(config-sigdef-sig-status)# enabled true
R1(config-sigdef-sig-status)# engine
R1(config-sigdef-sig-engine)# event-action produce-alert
R1(config-sigdef-sig-engine)# event-action deny-packet-inline
R1(config-sigdef-sig-engine)# event-action reset-tcp-connection
R1(config-sigdef-sig-engine)# exit
R1(config-sigdef-sig)# exit
R1(config-sigdef)# exit
Do you want to accept these changes? [confirm] <Enter>

Mar  8 05:37:45.775: %IPS-6-ENGINE_BUILDS_STARTED:  05:37:45 UTC Mar 8 2015
Mar  8 05:37:46.099: %IPS-6-ENGINE_BUILDING: atomic-ip - 539 signatures - 1 of 13
engines
R1(config)#
Mar  8 05:37:51.219: %IPS-6-ENGINE_READY: atomic-ip - build time 5120 ms - packets for
this engine will be scanned
Mar  8 05:37:51.427: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 5652 ms
```

Шаг 4: Отправьте эхо-запрос с маршрутизатора R2 на последовательный интерфейс 0/0/0 маршрутизатора R1.

a. Запустите сервер syslog.

b. Из CLI маршрутизатора R2 отправьте эхо-запрос на интерфейс S0/0/0 маршрутизатора R1 по IP-адресу 10.1.1.1. Эхо-запросы выполнены успешно? Поясните ответ.

_____

_____

Шаг 5: Отправьте эхо-запрос с маршрутизатора R2 на компьютер PC-A.

a. С CLI маршрутизатора R2 отправьте эхо-запрос на компьютер PC-A по IP-адресу **192.168.1.3**. Эхо-запросы выполнены успешно? Поясните ответ.

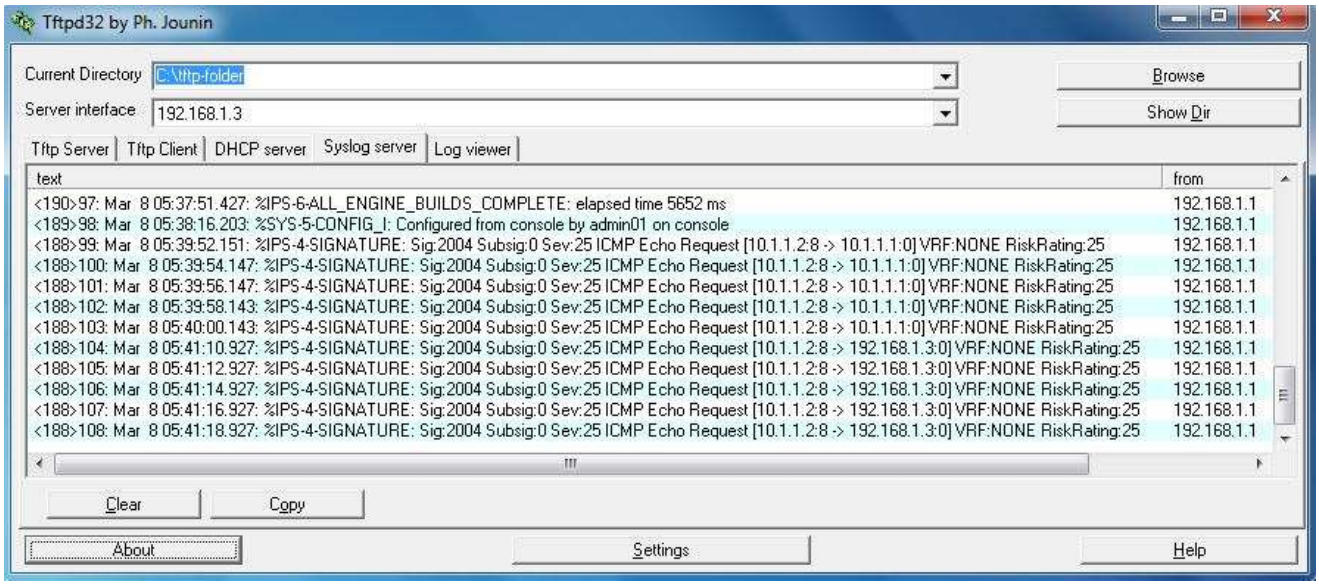
_____

_____

b. Обратите внимание на сообщения IPS из маршрутизатора R1 на экране сервера syslog ниже. Сколько сообщений было сгенерировано эхо-запросами с маршрутизатора R2 на маршрутизатор R1 и компьютер PC-A?

_____

_____



Примечание. Рейтинг риска IPS для эхо-запросов ICMP (уровень серьезности) является относительно низким – 25. Рейтинг риска может принимать значение от 0 до 100.

Часть 3: Имитация атаки

Задача 1: Проверка IPS с помощью Zenmap

Nmap/Zenmap – это инструмент сканирования сети, позволяющий обнаружить сетевые хосты и ресурсы, включая сервисы, порты, операционные системы и другую информацию цифровых отпечатков. Zenmap – это графический интерфейс для Nmap. Nmap **не должен** использоваться для сканирования сети без предварительного разрешения. Факт сканирования сети может быть воспринят как форма сетевой атаки.

Nmap/Zenmap проверит возможности IPS на маршрутизаторе R1. Вы запустите сканирующую программу на компьютере PC-A и попытаетесь просканировать открытые порты на маршрутизаторе R2 до и после применения правила IPS iosips на маршрутизаторе R1.

Шаг 1: Загрузите и установите Nmap/Zenmap.

a. Если Nmap/Zenmap не установлен на PC-A, скачайте **Nmap/Zenmap** по ссылке http://nmap.org/download.html.

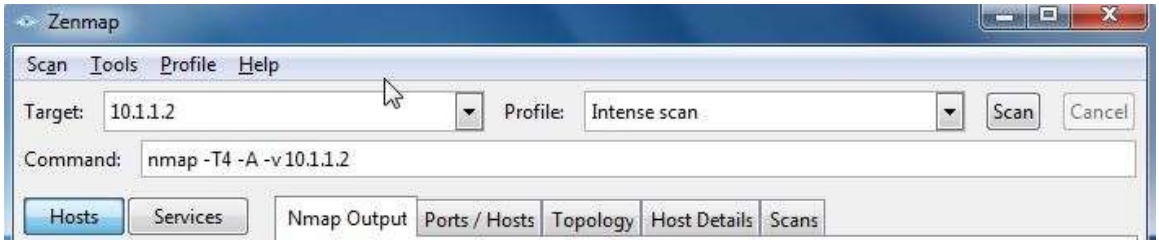
b. Найдите подходящие для вашей операционной системы двоичные файлы.

c. Установите Nmap/Zenmap.

Шаг 2: Запустите Nmap/Zenmap и настройте параметры сканирования.

a. Запустите **Zenmap** на компьютере PC-A.

b. Введите IP-адрес **10.1.1.2** в поле Target и выберите значение **Intense scan** в поле Profile. Нажмите **Scan** для начала сканирования.

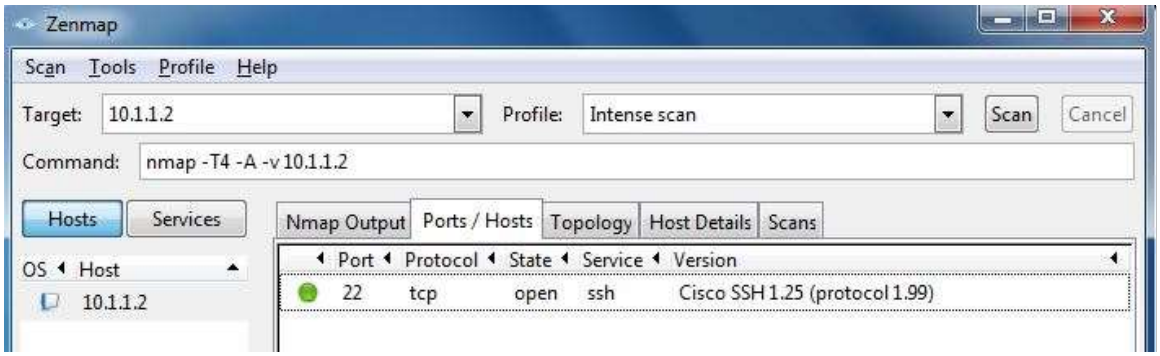


c. После завершения сканирования проверьте результаты, отображаемые на вкладке **Nmap Output.**

d. Перейдите на вкладку **Ports/Hosts.** Сколько открытых портов нашел Nmap на маршрутизаторе R2? Назовите связанные номера портов и сервисы.

_____

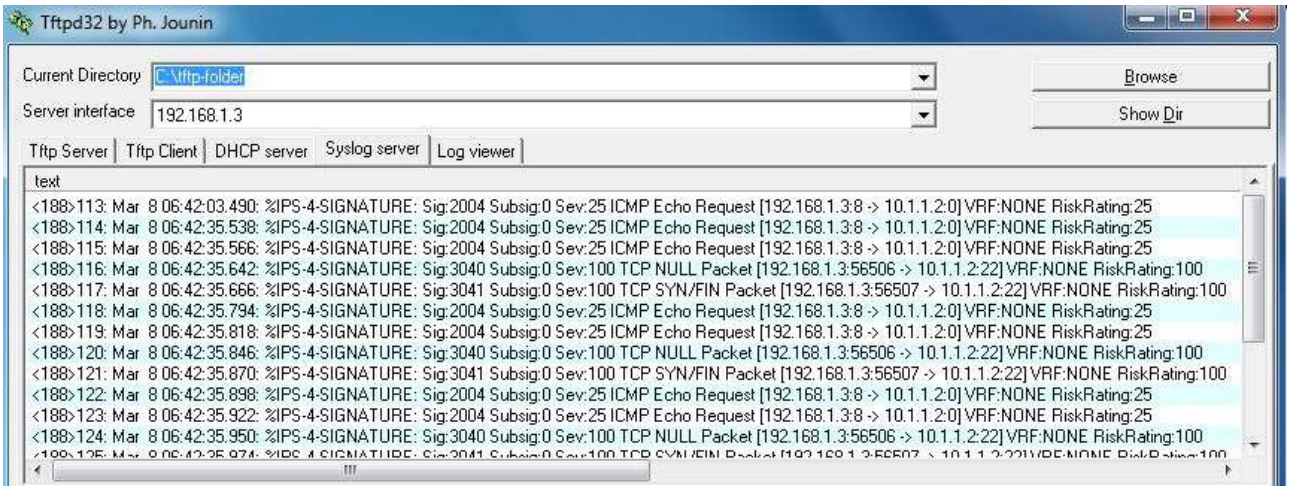
_____



e. Выйдите из Zenmap.

Задача 2: Проверка сообщений Syslog на маршрутизаторе R1

Вы должны видеть записи журнала syslog на консоли маршрутизатора R1 и на сервере syslog, если он включен. Описания должны содержать определенные строки, такие как TCP NULL Packet и TCP SYN/FIN Packet.



a. Каков рейтинг риска или уровень серьезности IPS (Sev:) для TCP NULL Packet, сигнатура 3040?

_____

b. Каков рейтинг риска или уровень серьезности IPS (Sev:) для пакета TCP SYN/FIN, сигнатура 3041?

_____

Вопросы для повторения

1. Если при использовании файлов сигнатур версии 5.x в сигнатуру вносятся изменения, будут ли они видны на маршрутизаторе в конфигурации?

_____

_____

_____

_____

_____

_____

_____

_____

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 (FA0/0)	Fast Ethernet 0/1 (Fa0/1)	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 (FA0/0)	Fast Ethernet 0/1 (Fa0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (Fa0/1)	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.

