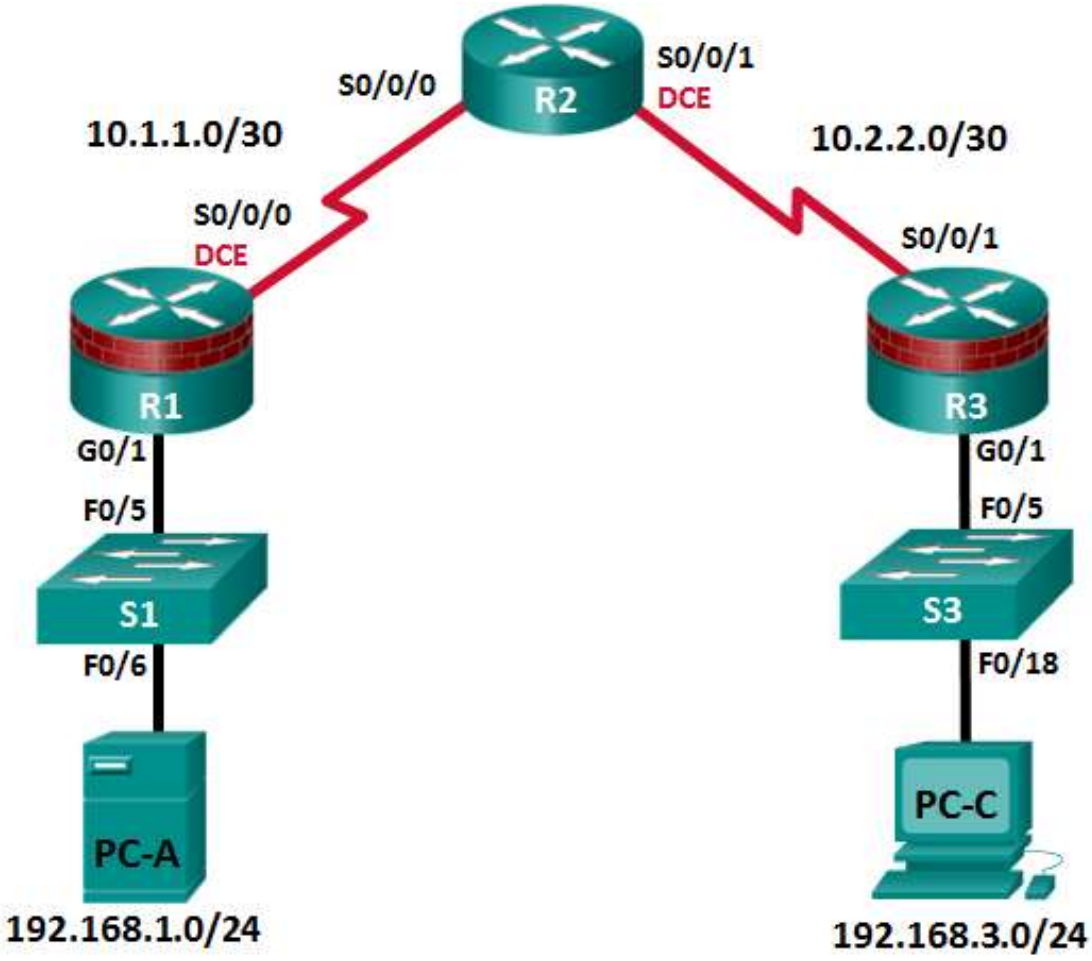
CCNA Security

Лабораторная работа. Защита маршрутизатора для административного доступа

Топология



Примечание. В устройствах ISR G1 используются интерфейсы FastEthernet вместо GigabitEthernet.

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

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 основных параметров устройства

- Подключение сетевых кабелей, как показано на топологической схеме
- Настройка базовых параметров IP-адресации для маршрутизаторов и компьютеров
- Настройка OSPF-маршрутизации
- Настройка хост-компьютеров
- Проверка связи между хостами и маршрутизаторами

Часть 2. Контроль административного доступа для маршрутизаторов

- Настройка и шифрование всех паролей
- Настройка предупреждающего баннера при входе в систему
- Настройка расширенных функций безопасности
- Настройка SSH-сервера на маршрутизаторе
- Настройка SSH-клиента и проверка связи
- Настройка SCP-сервера на маршрутизаторе

Часть 3. Настройка административных ролей

- Создание нескольких представлений ролей и предоставление им различных привилегий
- Проверка и сравнение представлений

Часть 4. Настройка отчетов о защите и управлении Cisco IOS

- Защита файлов образа и конфигурации Cisco IOS
- Настройка функции SNMPv3 Security с помощью ACL
- Настройка маршрутизатора в качестве источника синхронизированного времени для других устройств по протоколу NTP
- Настройка поддержки Syslog на маршрутизаторе
- Установка и активация сервера Syslog на компьютере
- Внесение изменений на маршрутизаторе и отслеживание результатов в системном журнале на компьютере

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

Часть 5. Защита плоскости управления

- Настройка OSPF-аутентификации с помощью SHA256
- Проверка OSPF-аутентификации

Часть 6. Настройка автоматизированных функций безопасности

- Блокировка маршрутизатора с помощью AutoSecure и проверка конфигурации
- Сравнение применения AutoSecure и защиты маршрутизатора вручную с помощью командной строки

Исходные данные/сценарий

Маршрутизатор – это один из важнейших компонентов любой сети. Он контролирует передачу данных внутрь сети и из нее, а также между устройствами в самой сети. Особенно важной задачей является защита сетевых маршрутизаторов, так как сбои в работе устройств маршрутизации могут привести к недоступности отдельных участков или сети в целом. Осуществление контроля доступа к маршрутизаторам и отчетности – крайне важные задачи для обеспечения безопасности сети, которые должны быть составной частью всесторонней политики безопасности.

В данной лабораторной работе вы построите сеть из нескольких маршрутизаторов и настроите маршрутизаторы и хосты. Используя различные инструменты командной строки, обеспечьте безопасность локального и удаленного доступа к маршрутизаторам, проанализируйте потенциальные уязвимости и предпримите меры по их устранению. Активируйте функцию отчетности для отслеживания изменений конфигурации маршрутизатора.

В данной лабораторной работе используются команды и выходные данные маршрутизатора Cisco 1941 с ПО Cisco IOS версии 15.4(3)M2 (с лицензией Security Technology Package). 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, доступные команды и выходные данные могут отличаться от указанных в данной работе.

Примечание. Перед тем как начать работу, убедитесь, что конфигурации маршрутизаторов и коммутаторов были сброшены и не имеют настроек запуска.

Необходимые ресурсы

- 3 маршрутизатора (Cisco 1941 с образом Cisco IOS Release 15.4(3)M2 и лицензией Security Technology Package)
- 2 коммутатора (Cisco 2960 или аналогичный) (необязательно)
- 2 ПК (ОС Windows 7 или 8.1, SSH-клиент, Syslog-сервер Kiwi или Tftpd32)
- Последовательные кабели и кабели Ethernet, как показано на топологической схеме
- Консольные кабели для настройки сетевых устройств Cisco

Часть 1: Настройка основных параметров устройства

В части 1 определите топологию сети и настройте базовые параметры, такие как IP-адреса интерфейсов.

Шаг 1: Подключите сетевые кабели.

Присоедините устройства, как показано на топологической схеме, и проложите кабели, как требуется.

Шаг 2: Настройте основные параметры для каждого маршрутизатора.

a. Задайте имена хостов согласно топологической схеме.

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

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

c. Настройте тактовую частоту маршрутизаторов с помощью DCE-кабеля, подключенного к последовательному интерфейсу каждого из них. В качестве примера показан маршрутизатор R1.

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

d. Чтобы маршрутизатор не пытался неправильно интерпретировать введенные команды как имена узлов, отключите функцию DNS-поиска. В качестве примера показан маршрутизатор R1.

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

Шаг 3: Настройте OSPF-маршрутизацию на маршрутизаторах.

a. Воспользуйтесь командой **router ospf** в режиме глобальной настройки, чтобы включить OSPF на маршрутизаторе R1.

```
R1(config)# router ospf 1
```

b. Настройте операторы **network** для сетей на маршрутизаторе R1. Используйте идентификатор зоны 0.

```
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 10.1.1.0 0.0.0.3 area 0
```

c. Настройте OSPF на маршрутизаторах R2 и R3.

d. Введите команду **passive-interface**, чтобы переключить интерфейс G0/1 маршрутизаторов R1 и R3 в пассивный режим.

```
R1(config)# router ospf 1
R1(config-router)# passive-interface g0/1
R3(config)# router ospf 1
R3(config-router)# passive-interface g0/1
```

Шаг 4: Проверьте соседние устройства по протоколу OSPF и информацию о маршрутизации.

a. Введите команду **show ip ospf neighbor** и убедитесь, что каждый маршрутизатор выводит список других маршрутизаторов в сети как соседей.

```
R1# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.2.2.2          0   FULL/  -        00:00:31    10.1.1.2        Serial0/0/0
```

b. Введите команду **show ip route** и убедитесь, что все сети отображаются в таблице маршрутизации на всех маршрутизаторах.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override
```

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

```
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.1/32 is directly connected, Serial0/0/0
O        10.2.2.0/30 [110/128] via 10.1.1.2, 00:03:03, Serial0/0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/1
L        192.168.1.1/32 is directly connected, GigabitEthernet0/1
O     192.168.3.0/24 [110/129] via 10.1.1.2, 00:02:36, Serial0/0/0
```

Шаг 5: Настройте параметры IP для хоста.

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

Шаг 6: Проверьте связь между компьютерами PC-A и PC-C.

a. Отправьте запрос ping с маршрутизатора R1 на R3.

   Если запрос ping выполняется с ошибкой, проверьте основные настройки устройств перед тем, как продолжить.

b. Отправьте ping-запрос 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 ping-запрос успешно передается с компьютера PC-A на PC-C, это означает, что OSPF-маршрутизация настроена верно и работает исправно. Если ping-запрос завершается ошибкой, но интерфейсы устройств включены и IP-адреса заданы верно, воспользуйтесь командами **show run, show ip ospf neighbor** и **show ip route**, чтобы выявить проблемы, связанные с протоколом маршрутизации.

Шаг 7: Сохраните основную текущую конфигурацию для каждого маршрутизатора.

Сохраните основную текущую конфигурацию для маршрутизаторов в виде текстовых файлов на своем ПК. Эти текстовые файлы могут быть использованы для последующего восстановления настроек в лабораторной работе.

Часть 2: Контроль административного доступа для маршрутизаторов

В части 2 вы выполните следующие задачи:

- настроите и зашифруете все пароли;
- настроите предупреждающий баннер при входе в систему;
- настроите расширенные функции безопасности;
- настроите расширенные параметры безопасности виртуального входа в систему;
- настроите SSH-сервер на маршрутизаторе R1;
- изучите клиентское ПО эмуляции терминала и настроите SSH-клиент;
- настроите SCP-сервер на маршрутизаторе R1.

Примечание. Выполните все задачи на маршрутизаторах R1 и R3. Здесь показаны процедуры и выходные данные для маршрутизатора R1.

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

Задача 1: Настройка и шифрование паролей на маршрутизаторах R1 и R3

Шаг 1: Установите минимальную длину пароля для всех маршрутизаторов.

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

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

Шаг 2: Настройте пароль привилегированного доступа.

Настройте шифрованный пароль привилегированного доступа на обоих маршрутизаторах. Используйте алгоритм хеширования type 9 (SCRYPT).

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

Каким образом настройка пароля привилегированного доступа поможет защитить маршрутизатор от несанкционированного доступа вследствие атаки?

_____

_____

_____

_____

_____

_____

Шаг 3: Настройте основную консоль, вспомогательный порт и линии виртуального доступа.

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. Настройте пароль консоли и активируйте вход в систему для маршрутизаторов. 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)# password ciscocon
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
R1(config-line)# logging synchronous
```

   Когда вы настроили пароль для линии консоли, какое сообщение было отображено?

   _____

   _____

b. Настройте новый пароль **ciscoconpass** для консоли.

c. Настройте пароль порта AUX для маршрутизатора R1.

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

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

d. Подключитесь по протоколу Telnet с маршрутизатора R2 к маршрутизатору R1.

```
R2> telnet 10.1.1.1
```

Вам удалось войти в систему? Поясните ответ.

_____

_____

Какие сообщения были отображены?

_____

_____

e. Настройте пароль на линиях vty для маршрутизатора R1.

```
R1(config)# line vty 0 4
R1(config-line)# password ciscovtypass
R1(config-line)# exec-timeout 5 0
R1(config-line)# transport input telnet
R1(config-line)# login
```

Примечание. Теперь для линий vty по умолчанию установлен параметр **transport input none**.

Снова подключитесь по протоколу Telnet с маршрутизатора R2 к маршрутизатору R1. Вам удалось выполнить вход в этот раз?

_____

f. Войдите в привилегированный режим и введите команду **show run**. Можете ли вы прочитать пароль привилегированного доступа? Поясните ответ.

_____

_____

Можете ли вы прочитать пароли для консоли, aux и vty? Поясните ответ.

_____

_____

g. Повторите ту же часть настройки из шагов 3a–3g на маршрутизаторе R3.

Шаг 4: Зашифруйте простые текстовые пароли.

a. Используя команду **service password-encryption**, зашифруйте пароли для консоли, aux и vty.

```
R1(config)# service password-encryption
```

b. Введите команду **show run**. Можете ли вы прочитать пароли для консоли, aux и vty? Поясните ответ.

_____

_____

На каком уровне (номер) шифруется пароль привилегированного доступа по умолчанию? _____

На каком уровне (номер) шифруются другие пароли? _____

Какой уровень шифрования наиболее сложен для взлома и почему?

_____

_____

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

Задача 2: Настройка предупреждающего баннера при входе в систему на маршрутизаторах R1 и R3

Шаг 1: Настройте предупреждающее сообщение, отображаемое до входа в систему.

a. Настройте предупреждение для неавторизованных пользователей в виде баннера с ежедневным сообщением (MOTD) с помощью команды **banner motd**. При подключении пользователя к одному из маршрутизаторов до запроса на ввод авторизационных данных отображается баннер MOTD. В данном примере в начале и конце сообщения используется знак доллара ($).

```
R1(config)# banner motd $Unauthorized access strictly prohibited!$
R1(config)# exit
```

b. Введите команду **show run**. Во что преобразуется знак $ на выходе?

_____

_____

Задача 3: Настройка расширенных функций безопасности на маршрутизаторах R1 и R3

Шаг 1: Изучите опции команды username.

Введите следующую команду в режиме глобальной настройки:

```
R1(config)# username user01 algorithm-type ?
```

Какие опции доступны?

_____

_____

_____

Шаг 2: Создайте новую учетную запись пользователя с секретным паролем.

a. Создайте новую учетную запись пользователя с паролем, зашифрованным с помощью алгоритма хеширования SCRYPT.

```
R1(config)# username user01 algorithm-type scrypt secret user01pass
```

b. Выйдите из режима глобальной настройки и сохраните конфигурацию.

c. Отобразите текущую конфигурацию. Какой метод хеширования используется для пароля?

_____

_____

Шаг 3: Проверьте новую учетную запись путем входа в систему по ней через консоль.

a. Настройте линию консоли таким образом, чтобы использовать учетные записи, определенные локально.

```
R1(config)# line console 0
R1(config-line)# login local
R1(config-line)# end
R1# exit
```

b. Перейдите к начальному экрану маршрутизатора, на котором отображается следующее: R1 con0 is now available, Press RETURN to get started.

c. Войдите в систему, используя заданные ранее имя пользователя **user01** и пароль **user01pass**.

Чем отличается вход в систему через консоль сейчас и ранее?

_____

_____

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

d. После входа введите команду **show run.** Вам удалось отправить команду? Поясните ответ.

_____

_____

e. Войдите в привилегированный режим, используя команду **enable**. У вас был запрошен пароль? Поясните ответ.

_____

_____

Шаг 4: Проверьте новую учетную запись путем входа в рамках сеанса Telnet.

a. Установите сеанс Telnet с маршрутизатором R1 с компьютера PC-A. По умолчанию Telnet в Windows 7 отключен. Если необходимо, поищите в Интернете способ активации Telnet в Windows 7.

```
PC-A> telnet 192.168.1.1
```

Система запросила у вас учетные данные? Поясните ответ.

_____

_____

b. Настройте линии vty таким образом, чтобы использовать учетные записи, определенные локально.

```
R1(config)# line vty 0 4
R1(config-line)# login local
```

c. Установите сеанс Telnet с маршрутизатором R1 с компьютера PC-A снова.

```
PC-A> telnet 192.168.1.1
```

Система запросила у вас учетные данные? Поясните ответ.

_____

_____

d. Войдите в систему как пользователь **user01** с паролем **user01pass**.

e. Во время сеанса Telnet с маршрутизатором R1 войдите в привилегированный режим по команде **enable**.

Какой пароль вы использовали?

_____

f. Для дополнительной безопасности настройте порт AUX на использование локально определенных учетных записей для входа.

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

g. Завершите сеанс Telnet с помощью команды **exit**.

Задача 4: Настройка SSH-сервера на маршрутизаторах R1 и R3

В этой задаче с помощью интерфейса командной строки (CLI) настройте безопасное управление маршрутизатором по протоколу SSH вместо Telnet. Протокол Secure Shell (SSH) – это сетевой протокол, позволяющий устанавливать безопасное подключение с эмуляцией терминала к маршрутизатору или иному сетевому устройству. Протокол SSH шифрует всю информацию, которая передается по сетевому каналу, и выполняет аутентификацию удаленного компьютера. Протокол SSH все чаще заменяет Telnet – именно его выбирают сетевые специалисты в качестве средства удаленного входа в систему.

Примечание. Чтобы маршрутизатор мог использовать протокол SSH, в нем необходимо настроить локальную аутентификацию (через сервисы AAA или имя пользователя) либо аутентификацию по паролю. В этой задаче вы настроите имя пользователя SSH и локальную аутентификацию.

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

Шаг 1: Настройте доменное имя.

Войдите в режим глобальной настройки и задайте доменное имя.

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

Шаг 2: Настройте привилегированного пользователя для входа через SSH-клиент.

a. Используйте команду **username**, чтобы создать ID пользователя с наиболее высоким уровнем привилегий и секретным паролем.

```
R1(config)# username admin privilege 15 algorithm-type scrypt secret cisco12345
```

Примечание. По умолчанию, имена пользователей нечувствительны к регистру. Научиться делать имена пользователей чувствительными к регистру вы сможете в главе 3.

b. Перейдите к начальному экрану входа в маршрутизатор. Войдите в систему под именем пользователя admin и соответствующим паролем. Какой запрос был выдан маршрутизатором после ввода пароля?

_____

_____

Шаг 3: Настройте входящие линии vty.

Задайте уровень привилегий **15**, чтобы пользователь с наивысшим уровнем привилегий (15) при доступе к линиям vty автоматически переходил в привилегированный режим. Остальные пользователи по умолчанию будут переходить в пользовательский режим. Используйте учетные записи локальных пользователей для обязательного входа в систему, а также проверки и приема только SSH-подключений.

```
R1(config)# line vty 0 4
R1(config-line)# privilege level 15
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
```

Примечание. Команда **login local** должна была быть настроена на предыдущем шаге. Данная команда включена в этом разделе, чтобы у вас были все команды, если вы делаете это впервые.

Примечание. Если к команде **transport input** добавить ключевое слово **telnet**, то пользователи смогут входить в систему с помощью как Telnet, так и SSH. Однако маршрутизатор при этом будет менее защищенным. Если указано только SSH, то на хосте, с которого выполняется подключение, должен быть установлен SSH-клиент.

Шаг 4: Удалите существующие пары ключей на маршрутизаторе.

```
R1(config)# crypto key zeroize rsa
```

Примечание. Если ключи отсутствуют, вы можете получить следующее сообщение: `% No Signature RSA Keys found in configuration`.

Шаг 5: Сгенерируйте пару ключей шифрования RSA для маршрутизатора.

Маршрутизатор использует пару ключей RSA для аутентификации и шифрования передаваемых SSH-данных.

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

a. Задайте количество битов модуля для RSA-ключей, равное **1024**. Значение по умолчанию – 512, диапазон допустимых значений – от 360 до 2048.

```
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.ccnasecurity.com.

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#
*Dec 16 21:24:16.175: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

b. Введите команду **ip ssh version 2** для принудительного использования SSH версии 2.

```
R1(config)# ip ssh version 2
R1(config)# exit
```

Примечание. Подробнее методы шифрования рассмотрены в главе 7.

Шаг 6: Проверьте конфигурацию SSH.

a. Используйте команду **show ip ssh** для просмотра текущих настроек.

```
R1# show ip ssh
```

b. Заполните следующую информацию на основе выходных данных для команды **show ip ssh**.

Активная версия SSH: _____

Время ожидания аутентификации: _____

Повторные попытки аутентификации: _____

Шаг 7: Настройте время ожидания SSH и параметры аутентификации.

Значения времени ожидания и параметров аутентификации SSH по умолчанию можно изменить на более ограничительные с помощью следующих команд.

```
R1(config)# ip ssh time-out 90
R1(config)# ip ssh authentication-retries 2
```

Шаг 8: Сохраните running-config в startup-config.

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

Задача 5: Обзор клиентского ПО эмуляции терминала и настройка SSH-клиента

Шаг 1: Изучите клиентское ПО эмуляции терминала.

Воспользуйтесь поиском в Интернете, чтобы найти бесплатный клиент эмуляции терминала, например TeraTerm или PuTTy. Какие у них есть особенности?

_____

_____

_____

_____

_____

_____

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

Шаг 2: Установите SSH-клиент на компьютеры PC-A и PC-C.

a. Если SSH-клиент еще не установлен, скачайте TeraTerm или PuTTY.

b. Сохраните приложение на рабочий стол.

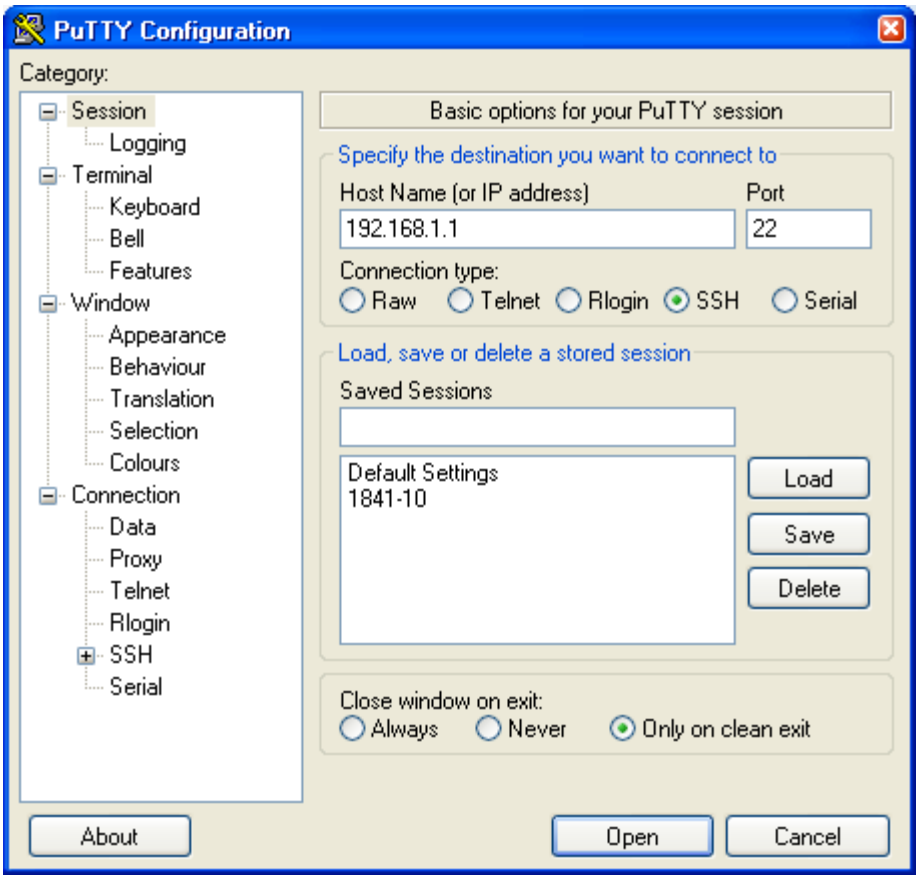
Примечание. Данная процедура описана для PuTTY и относится к компьютеру PC-A.

Шаг 3: Проверьте связь с маршрутизатором R1 с компьютера PC-A по протоколу SSH.

a. Запустите PuTTY, дважды щелкнув значок putty.exe.

b. Для интерфейса F0/1 маршрутизатора R1 введите IP-адрес **192.168.1.1** в поле **Host Name (or IP address)**.

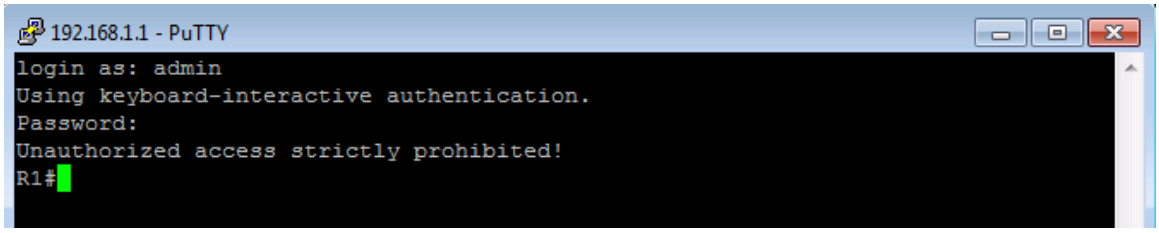
c. Убедитесь, что выбран переключатель **SSH**.



d. Нажмите **Open**.

e. В окне PuTTY Security Alert нажмите **Yes**.

f. В окне PuTTY введите имя пользователя **admin** и пароль **cisco12345**.



© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

g. В строке привилегированного режима для маршрутизатора R1 введите команду **show users**.

```
R1# show users
```

Какие пользователи сейчас подключены к маршрутизатору R1?

_____

_____

_____

h. Закройте окно сеанса PuTTY SSH.

i. Попытайтесь установить сеанс Telnet со своим маршрутизатором через PC-A. Вам удалось установить сеанс Telnet? Поясните ответ.

_____

_____

j. Установите сеанс SSH в PuTTY с маршрутизатором с компьютера PC-A. Введите имя пользователя **user01** и пароль **user01pass** в окне PuTTY, чтобы попытаться подключиться с уровнем привилегий ниже 15.

Если вам удалось войти в систему, какой запрос был выведен?

_____

_____

k. Используйте команду **enable**, чтобы войти в привилегированный режим, и введите пароль привилегированного доступа **cisco12345**.

Задача 6: Настройка SCP-сервера на маршрутизаторе R1

Теперь, когда на маршрутизаторе настроен протокол SSH, настройте маршрутизатор R1 как сервер SCP (secure copy).

Шаг 1: Настройте параметры аутентификации и авторизации AAA по умолчанию на маршрутизаторе R1.

Настройте параметры аутентификации и авторизации AAA по умолчанию на маршрутизаторе R1, чтобы использовать локальную базу данных для входа.

Примечание. Для использования SCP пользователю необходимы права доступа с уровнем привилегий 15.

a. Включите AAA на маршрутизаторе.

```
R1(config)# aaa new-model
```

b. Введите команду **aaa authentication**, чтобы использовать локальную базу данных как метод аутентификации при входе в систему по умолчанию.

```
R1(config)# aaa authentication login default local
```

c. Введите команду **aaa authorization**, чтобы использовать локальную базу данных как метод авторизации команд по умолчанию.

```
R1(config)# aaa authorization exec default local
```

d. Включите SCP-сервер на маршрутизаторе R1.

```
R1(config)# ip scp server enable
```

Примечание. Подробнее метод AAA рассмотрен в главе 3.

Шаг 2: Скопируйте текущую конфигурацию во флеш-память маршрутизатора R1.

SCP-сервер позволяет копировать файлы в память маршрутизатора или из нее. На данном этапе вы создадите копию текущей конфигурации (running-config) во флеш-памяти маршрутизатора R1. Затем вы используете SCP, чтобы скопировать этот файл на маршрутизатор R3.

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

a. Сохраните текущую конфигурацию в файле во флеш-памяти маршрутизатора R1 под именем R1-Config.

```
R1# copy running-config R1-Config
```

b. Убедитесь, что файл R1-Config находится во флеш-памяти.

```
R1# show flash
-#- --length-- -----date/time------ path
1     75551300 Feb 16 2015 15:19:22 +00:00 c1900-universalk9-mz.SPA.154-3.M2.bin
2         1643 Feb 17 2015 23:30:58 +00:00 R1-Config

181047296 bytes available (75563008 bytes used)
```

Шаг 3: Используйте команду SCP на маршрутизаторе R3, чтобы извлечь файл конфигурации из маршрутизатора R1.

a. Используйте SCP, чтобы скопировать файл конфигурации, который вы создали на шаге 2a, на маршрутизатор R3.

```
R3# copy scp: flash:
Address or name of remote host []? 10.1.1.1
Source username [R3]? admin
Source filename []? R1-Config
Destination filename [R1-Config]? [Enter]
Password: cisco12345
!
2007 bytes copied in 9.056 secs (222 bytes/sec)
```

b. Убедитесь, что файл был скопирован во флеш-память маршрутизатора R3.

```
R3# show flash
-#- --length-- -----date/time------ path
1     75551300 Feb 16 2015 15:21:38 +00:00 c1900-universalk9-mz.SPA.154-3.M2.bin
2         1338 Feb 16 2015 23:46:10 +00:00 pre_autosec.cfg
3         2007 Feb 17 2015 23:42:00 +00:00 R1-Config

181043200 bytes available (75567104 bytes used)
```

c. Введите команду **more** для просмотра содержимого файла R1-Config.

```
R3# more R1-Config
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
<Output omitted>
!
end
R3#
```

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

Шаг 4: Сохраните конфигурацию.

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

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

Часть 3: Настройка административных ролей

В части 3 данной лабораторной работы вы выполните следующие задачи:

- создадите административные роли или представления на маршрутизаторах R1 и R3;
- предоставите каждому представлению разные привилегии;
- проверите и сопоставите представления.

Функция доступа через CLI на основе ролей позволяет администратору определять представления. Эти представления представляют собой наборы операционных команд и функций конфигурирования, предоставляющие выборочный или частичный доступ к командам режимов Cisco IOS EXEC и конфигурирования (config). Представления позволяют ограничить для пользователей доступ к Cisco IOS CLI и информации о конфигурации. С помощью представлений можно определять, какие команды будут приниматься и какая информация о конфигурации будет отображаться.

Примечание. Выполните все задачи на маршрутизаторах R1 и R3. Здесь показаны процедуры и выходные данные для маршрутизатора R1.

Задача 1: Включение корневого представления на маршрутизаторах R1 и R3

Если администратор хочет настроить в системе другое представление, система должна находиться в корневом представлении. Когда система находится в корневом представлении, у пользователя есть те же права доступа, что и у пользователя с привилегиями уровня 15. Кроме того, такой пользователь может настраивать новые представления, добавлять в них команды, а также удалять их. При нахождении в представлении интерфейса командной строки (CLI) у вас есть доступ только к тем командам, которые были добавлены в него пользователем в корневом представлении.

Шаг 1: Включите AAA на маршрутизаторе R1.

Чтобы определить представления, убедитесь, что AAA было включено с помощью команды **aaa new-model** в части 2.

Шаг 2: Включите корневое представление.

Используйте команду **enable view**, чтобы включить корневое представление. Используйте пароль привилегированного доступа **(enable secret) cisco12345**. Если для маршрутизатора нет пароля привилегированного доступа, создайте его сейчас.

```
R1# enable view
Password: cisco12345
R1#
```

Задача 2: Создание новых представлений для ролей Admin1, Admin2 и Tech на маршрутизаторах R1 и R3

Шаг 1: Создайте представление admin1, установите пароль и назначьте привилегии.

a. Пользователь admin1 является пользователем следующего уровня после корневого, у которого есть доступ к этому маршрутизатору. У него есть наиболее широкие полномочия. Пользователь admin1 может использовать команды **show**, **config** и **debug**. Используйте следующую команду для создания представления admin1, находясь в корневом представлении.

```
R1(config)# parser view admin1
R1(config-view)#
```

Примечание. Чтобы удалить представление, используйте команду **no parser view** *viewname*.

b. Назначьте зашифрованный пароль для представления admin1.

```
R1(config-view)# secret admin1pass
R1(config-view)#
```

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

c. Рассмотрите команды, которые можно настроить в представлении admin1. Используйте команду **commands ?** для просмотра доступных команд. Ниже приведен неполный список доступных команд.

```
R1(config-view)# commands ?
  RITE-profile           Router IP traffic export profile command mode
  RMI Node Config        Resource Policy Node Config mode
  RMI Resource Group     Resource Group Config mode
  RMI Resource Manager   Resource Manager Config mode
  RMI Resource Policy    Resource Policy Config mode
  SASL-profile           SASL profile configuration mode
  aaa-attr-list          AAA attribute list config mode
  aaa-user               AAA user definition
  accept-dialin          VPDN group accept dialin configuration mode
  accept-dialout         VPDN group accept dialout configuration mode
  address-family         Address Family configuration mode
<output omitted>
```

d. Добавьте все команды **config**, **show** и **debug** в представление admin1, затем выйдите из режима настройки представления.

```
R1(config-view)# commands exec include all show
R1(config-view)# commands exec include all config terminal
R1(config-view)# commands exec include all debug
R1(config-view)# end
```

e. Проверьте представление admin1.

```
R1# enable view admin1
Password: admin1pass

R1# show parser view
Current view is 'admin1'
```

f. Изучите команды, доступные в представлении admin1.

```
R1# ?
Exec commands:
  <0-0>/<0-4>  Enter card slot/sublot number
  configure    Enter configuration mode
  debug        Debugging functions (see also 'undebug')
  do-exec      Mode-independent "do-exec" prefix support
  enable       Turn on privileged commands
  exit         Exit from the EXEC
  show           Show running system
```

Примечание. Команд EXEC может быть больше, чем показано. Это зависит от используемого устройства или образа IOS.

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

g. Изучите команды **show,** , доступные в представлении admin1.

```
R1# show ?
  aaa                       Show AAA values
  access-expression         List access expression
  access-lists              List access lists
  acircuit                  Access circuit info
  adjacency                 Adjacent nodes
  aliases                   Display alias commands
  alignment                 Show alignment information
  appfw                     Application Firewall information
  archive                   Archive functions
  arp                       ARP table
<output omitted>
```

Шаг 2: Создайте представление admin2, установите пароль и назначьте привилегии.

a. В данном учебном курсе пользователь admin2 является младшим администратором, который может просматривать все конфигурации, но ему не разрешено настраивать маршрутизаторы или использовать команды отладки.

b. Используйте команду **enable view**, чтобы активировать корневое представление, и введите пароль привилегированного доступа **cisco12345**.

```
R1# enable view
Password: cisco12345
```

c. Используйте следующую команду для создания представления admin2.

```
R1(config)# parser view admin2
R1(config-view)#
```

d. Назначьте пароль для представления admin2.

```
R1(config-view)# secret admin2pass
R1(config-view)#
```

e. Добавьте все команды **show** в представление, затем выйдите из режима настройки представления.

```
R1(config-view)# commands exec include all show
R1(config-view)# end
```

f. Проверьте представление admin2.

```
R1# enable view admin2
Password: admin2pass

R1# show parser view
Current view is 'admin2'
```

g. Изучите команды, доступные в представлении admin2.

```
R1# ?
Exec commands:
  <0-0>/<0-4>  Enter card slot/sublot number
  do-exec      Mode-independent "do-exec" prefix support
  enable       Turn on privileged commands
  exit         Exit from the EXEC
  show         Show running system information
```

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

Примечание. Команд EXEC может быть больше, чем показано. Это зависит от используемого устройства или образа IOS.

Что отсутствует в списке команд для admin2 из того, что есть в списке команд для admin1?

_____

Шаг 3: Создайте представление tech, установите пароль и назначьте привилегии.

a. Как правило, пользователь tech занимается установкой оборудования и прокладкой кабелей у конечного пользователя. Пользователи категории tech могут использовать только выбранные команды **show**.

b. Используйте команду **enable view**, чтобы активировать корневое представление, и введите пароль привилегированного доступа **cisco12345**.

```
R1# enable view
Password: cisco12345
```

c. Используйте следующую команду для создания представления tech.

```
R1(config)# parser view tech
R1(config-view)#
```

d. Назначьте пароль для представления tech.

```
R1(config-view)# secret techpasswd
R1(config-view)#
```

e. Добавьте нижеприведенные команды **show** в представление, затем выйдите из режима настройки представления.

```
R1(config-view)# commands exec include show version
R1(config-view)# commands exec include show interfaces
R1(config-view)# commands exec include show ip interface brief
R1(config-view)# commands exec include show parser view
R1(config-view)# end
```

f. Проверьте представление tech.

```
R1# enable view tech
Password: techpasswd

R1# show parser view
Current view is 'tech'
```

g. Изучите команды, доступные в представлении tech.

```
R1# ?
Exec commands:
  <0-0>/<0-4>  Enter card slot/sublot number
  do-exec      Mode-independent "do-exec" prefix support
  enable       Turn on privileged commands
  exit         Exit from the EXEC
  show         Show running system information
```

Примечание. Команд EXEC может быть больше, чем показано. Это зависит от используемого устройства или образа IOS.

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

h. Изучите команды **show**, доступные в представлении tech.

```
R1# show ?
  banner      Display banner information
  flash0:     display information about flash0: file system
  flash1:     display information about flash1: file system
  flash:      display information about flash: file system
  interfaces  Interface status and configuration
  ip          IP information
  parser      Display parser information
  usbflash0:  display information about usbflash0: file system
  version     System hardware and software status
```

Примечание. Команд EXEC может быть больше, чем показано. Это зависит от используемого устройства или образа IOS.

i. Введите команду **show ip interface brief**. Вам удалось сделать это, будучи пользователем tech? Поясните ответ.

_____

_____

j. Введите команду **show ip route**. Вам удалось сделать это, будучи пользователем tech?

_____

_____

k. Вернитесь в корневое представление с помощью команды **enable view**.

```
R1# enable view
Password: cisco12345
```

l. Введите команду **show run**, чтобы просмотреть представления, которые вы создали. Почему в списке для представления tech, помимо **show ip interface** и **show ip interface brief**, приведены команды **show** и **show ip**?

_____

_____

Шаг 4: Сохраните конфигурацию на маршрутизаторах R1 и R3.

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

Часть 4: Настройка отчетов о надежности и управлении Cisco IOS

В части 4 данной лабораторной работы вы выполните следующие задачи:

- защитите файлы образа и конфигурации Cisco IOS;
- настроите функцию безопасности SNMPv3 с помощью ACL;
- настроите маршрутизатор в качестве источника синхронизированного времени для других устройств с помощью NTP;
- настроите поддержку Syslog на маршрутизаторе;
- установите сервер Syslog на компьютере и активируете его;
- настроите уровень журнальных прерываний на маршрутизаторе;
- внесете изменения на маршрутизаторе и отследите результаты syslog на ПК.

Примечание. Выполните все задачи на маршрутизаторах R1 и R3. Здесь показаны процедуры и выходные данные для маршрутизатора R1.

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

Задача 1: Защита файлов образа и конфигурации Cisco IOS на маршрутизаторах R1 и R3

Функция Cisco IOS Resilient Configuration позволяет защитить текущий образ на маршрутизаторе и хранить рабочую копию конфигурации. Таким образом, можно защитить эти файлы от попыток злоумышленников стереть содержимое из постоянного хранилища (NVRAM и флеш-памяти). Данная функция защищает наименьший рабочий набор файлов для сохранения размера постоянного хранилища. Для защиты основного файла образа Cisco IOS дополнительного пространства памяти не требуется. В данной задаче вы должны будете настроить функцию Cisco IOS Resilient Configuration.

Примечание. Функция Cisco IOS Resilient Configuration недоступна на маршрутизаторах Cisco модели 1921.

Примечание. Выходные данные команд в данной задаче приведены только для примера. Ваши выходные данные будут другими.

Шаг 1: Отобразите список файлов во флеш-памяти для маршрутизатора R1.

Команда **show flash:** выводит содержимое подпапок. Команда **dir** выводит только содержимое текущей папки.

```
R1# show flash:
-#- --length-- -----date/time------ path
1     75551300 Feb 5 2015 16:53:34 +00:00 c1900-universalk9-mz.SPA.154-3.M2.bin
2            0 Jan 6 2009 01:28:44 +00:00 ipsdir
3       334531 Jan 6 2009 01:35:40 +00:00 ipsdir/R1-sigdef-default.xml
4          461 Jan 6 2009 01:37:42 +00:00 ipsdir/R1-sigdef-delta.xml
5         8509 Jan 6 2009 01:33:42 +00:00 ipsdir/R1-sigdef-typedef.xml
6        38523 Jan 6 2009 01:33:46 +00:00 ipsdir/R1-sigdef-category.xml
7          304 Jan 6 2009 01:31:48 +00:00 ipsdir/R1-seap-delta.xml
8          491 Jan 6 2009 01:31:48 +00:00 ipsdir/R1-seap-typedef.xml
9         1410 Oct 26 2014 04:44:08 +00:00 pre_autosec.cfg

76265535 bytes available (180221889 bytes used)

R1# dir
Directory of flash:/

    1  -rw-      75551300 Feb 5 2015 16:53:34 +00:00 c1900-universalk9-mz.SPA.154-3.M2.bin
    2  drw-           0   Jan 6 2009 01:28:44 +00:00  ipsdir
    9  -rw-        1410  Oct 26 2014 04:44:08 +00:00  pre_autosec.cfg

256487424 bytes total (180221889 bytes free)
```

Шаг 2: Защитите файл образа Cisco IOS и заархивируйте копию текущей конфигурации.

a. Команда **secure boot-image** обеспечивает защиту образа Cisco IOS, позволяя не указывать файл в выходных данных для команд **dir** и **show**. Данный файл нельзя просматривать, копировать, изменять или удалять с помощью команд привилегированного режима. (Его можно просматривать в режиме ROMMON.) При первом включении рабочий образ защищен.

```
R1(config)# secure boot-image
.Feb 11 25:40:13.170: %IOS_RESILIENCE-5-IMAGE_RESIL_ACTIVE: Successfully secured running image
```

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

b. Команда **secure boot-config** делает снимок состояния текущей конфигурации маршрутизатора и надежно архивирует его в постоянной памяти (флеш-память).

```
R1(config)# secure boot-config
.Feb 11 25:42:18.691: %IOS_RESILIENCE-5-CONFIG_RESIL_ACTIVE: Successfully secured config archive
[flash:.runcfg-20150211-224218.ar]
```

Шаг 3: Проверьте защищенность образа и конфигурации.

Для отображения имени архивированного файла вы можете использовать только команду **show secure bootset**. Отобразите состояние защиты конфигурации и имя первичного загрузочного файла.

```
R1# show secure bootset
IOS resilience router id FTX1111W0QF

IOS image resilience version 15.4 activated at 25:40:13 UTC Wed Feb 11 2015
Secure archive flash: c1900-universalk9-mz.SPA.154-3.M2.bin type is image (elf)
[]
  file size is 75551300 bytes, run size is 75730352 bytes
  Runnable image, entry point 0x8000F000, run from ram

IOS configuration resilience version 15.4 activated at 25:42:18 UTC Wed Feb 11 2015
Secure archive flash:.runcfg-20150211-224218.ar type is config
configuration archive size 3293 bytes
```

Какое имя у файла архива текущей конфигурации и на чем оно основано?

_____

_____

Шаг 4: Отобразите список файлов во флеш-памяти для маршрутизатора R1.

a. Отобразите содержимое флеш-памяти с помощью команды **show flash**.

```
R1# show flash:
-#- --length-- -----date/time------ path
2            0 Jan 6 2009 01:28:44 +00:00 ipsdir
3       334531 Jan 6 2009 01:35:40 +00:00 ipsdir/R1-sigdef-default.xml
4          461 Jan 6 2009 01:37:42 +00:00 ipsdir/R1-sigdef-delta.xml
5         8509 Jan 6 2009 01:33:42 +00:00 ipsdir/R1-sigdef-typedef.xml
6        38523 Jan 6 2009 01:33:46 +00:00 ipsdir/R1-sigdef-category.xml
7          304 Jan 6 2009 01:31:48 +00:00 ipsdir/R1-seap-delta.xml
8          491 Jan 6 2009 01:31:48 +00:00 ipsdir/R1-seap-typedef.xml
9         1410 Oct 26 2014 04:44:08 +00:00 pre_autosec.cfg

76265535 bytes available (180221889 bytes used)
```

Присутствует ли в списке образ Cisco IOS или файл архива текущей конфигурации?

_____

b. Как узнать, что образ Cisco IOS все еще есть в нем?

_____

_____

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

Шаг 5: Отключите функцию IOS Resilient Configuration.

a. Отключите функцию IOS Resilient Configuration для образа Cisco IOS.

```
R1# config t
R1(config)# no secure boot-image
.Feb 11 25:48:23.009: %IOS_RESILIENCE-5-IMAGE_RESIL_INACTIVE: Disabled secure image
archival
```

b. Отключите функцию IOS Resilient Configuration для файла текущей конфигурации.

```
R1(config)# no secure boot-config
.Feb 11 25:48:47.972: %IOS_RESILIENCE-5-CONFIG_RESIL_INACTIVE: Disabled secure config
archival [removed flash:.runcfg-20150211-224218.ar]
```

Шаг 6: Проверьте видимость образа Cisco IOS во флеш-памяти.

Используйте команду **show flash:** для показа файлов в памяти.

```
R1# show flash:
-#- --length-- -----date/time------ path
1     75551300 Feb 5 2015 16:53:34 +00:00 c1900-universalk9-mz.SPA.154-3.M2.bin
2            0 Jan 6 2009 01:28:44 +00:00 ipsdir
3       334531 Jan 6 2009 01:35:40 +00:00 ipsdir/R1-sigdef-default.xml
4          461 Jan 6 2009 01:37:42 +00:00 ipsdir/R1-sigdef-delta.xml
5         8509 Jan 6 2009 01:33:42 +00:00 ipsdir/R1-sigdef-typedef.xml
6        38523 Jan 6 2009 01:33:46 +00:00 ipsdir/R1-sigdef-category.xml
7          304 Jan 6 2009 01:31:48 +00:00 ipsdir/R1-seap-delta.xml
8          491 Jan 6 2009 01:31:48 +00:00 ipsdir/R1-seap-typedef.xml
9         1410 Oct 26 2014 04:44:08 +00:00 pre_autosec.cfg


76265535 bytes available (180221889 bytes used)
```

Шаг 7: Сохраните конфигурацию на обоих маршрутизаторах.

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

Задача 2: Настройка функции SNMPv3 Security с помощью ACL

Протокол Simple Network Management Protocol (SNMP) позволяет администраторам отслеживать работу сети, управлять сетевыми устройствами и диагностировать проблемы в сети. Протокол SNMPv3 предоставляет безопасный доступ путем аутентификации и шифрования управляющих пакетов SNMP по всей сети.
Вы произведете настройку протокола SNMPv3 с использованием ACL на маршрутизаторе R1.

Шаг 1: Настройте список ACL на маршрутизаторе R1, который ограничит доступ к протоколу SNMP в локальной сети 192.168.1.0.

a. Создайте стандартный список доступа с именем **PERMIT-SNMP**.

```
R1(config)# ip access-list standard PERMIT-SNMP
```

b. Добавьте оператор разрешения (permit), разрешающий только пакеты в локальной сети маршрутизатора R1.

```
R1(config-std-nacl)# permit 192.168.1.0 0.0.0.255
R1(config-std-nacl)# exit
```

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

Шаг 2: Настройте представление SNMP.

Настройте представление SNMP под названием **SNMP-RO**, чтобы оно включало в себя семейство ISO MIB.

```
R1(config)# snmp-server view SNMP-RO iso included
```

Шаг 3: Настройте группу SNMP.

Назовите группу **SNMP-G1** и настройте ее на использование протокола SNMPv3, а также запрос аутентификации и шифрование через ключевое слово **priv**. Свяжите представление, которое вы создали на шаге 2, с группой, предоставляя ему доступ только для чтения с помощью параметра **read**. Наконец, укажите, что список ACL **PERMIT-SNMP**, настроенный на шаге 1, будет ограничивать доступ по протоколу SNMP к локальной сети.

```
R1(config)# snmp-server group SNMP-G1 v3 priv read SNMP-RO access PERMIT-SNMP
```

Шаг 4: Настройте пользователя SNMP.

Настройте пользователя **SNMP-Admin** и свяжите пользователя с группой **SNMP-G1**, которую вы настроили на шаге 3. Установите метод аутентификации **SHA** и пароль аутентификации **Authpass**. Используйте метод шифрования AES-128 с паролем **Encrypass**.

```
R1(config)# snmp-server user SNMP-Admin SNMP-G1 v3 auth sha Authpass priv aes 128
Encrypass
R1(config)# end
```

Шаг 5: Проверьте конфигурацию SNMP.

a. Воспользуйтесь командой show **snmp group** в привилегированном режиме для просмотра конфигурации группы SNMP. Убедитесь, что ваша группа настроена правильно.

Примечание. Если вам необходимо внести изменения в группу, используйте команду **no snmp group**, чтобы убрать группу из конфигурации, а затем добавьте ее с правильными параметрами.

```
R1# show snmp group
groupname: ILMI                           security model:v1
contextname: <no context specified>       storage-type: permanent
readview : *ilmi                          writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: ILMI                           security model:v2c
contextname: <no context specified>       storage-type: permanent
readview : *ilmi                          writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: SNMP-G1                        security model:v3 priv
contextname: <no context specified>       storage-type: nonvolatile
readview : SNMP-RO                        writeview: <no writeview specified>
notifyview: <no notifyview specified>
row status: active    access-list: PERMIT-SNMP
```

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

b. Используйте команду **show snmp user** для просмотра информации о пользователе SNMP.

Примечание. Команда **snmp-server user** не отображается в конфигурации по соображениям безопасности. Однако если вам необходимо внести изменения в профиль пользователя SNMP, вы можете ввести команду **no snmp-server user**, чтобы удалить пользователя из конфигурации, а затем добавить его обратно с новыми параметрами.

```
R1# show snmp user

User name: SNMP-Admin
Engine ID: 80000009030030F70DA30DA0
storage-type: nonvolatile      active
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: SNMP-G1
```

Задача 3: Настройка источника синхронизированного времени с помощью NTP

Маршрутизатор R2 будет главным источником синхронизации времени для маршрутизаторов R1 и R3.

Примечание. Маршрутизатор R2 может также быть главным источником синхронизации времени для коммутаторов S1 и S3, однако для данной лабораторной работы настраивать их не нужно.

Шаг 1: Настройте главный NTP-узел с помощью команд Cisco IOS.

Маршрутизатор R2 является главным NTP-сервером в данной лабораторной работе. Все остальные маршрутизаторы и коммутаторы настраивают время на его основе, как напрямую, так и косвенно. По этой причине необходимо убедиться, что на маршрутизаторе R2 установлено правильное время в соответствии со Всемирным координированным временем.

a. Используйте команду **show clock** для показа текущего времени, заданного в маршрутизаторе.

```
R2# show clock
*19:48:38.858 UTC Wed Feb 18 2015
```

b. Чтобы задать время на маршрутизаторе, используйте команду в формате **clock set** *time*.

```
R2# clock set 20:12:00 Dec 17 2014
R2#
*Dec 17 20:12:18.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 01:20:26
UTC Mon Dec 15 2014 to 20:12:00 UTC Wed Dec 17 2014, configured from console by admin
on console.
```

c. Настройте аутентификацию NTP, задав номер ключа аутентификации, тип хеширования и пароль, которые будут использоваться для аутентификации. Пароль чувствителен к регистру.

```
R2# config t
R2(config)# ntp authentication-key 1 md5 NTPpassword
```

d. Настройте доверенный ключ, который будет использоваться для аутентификации на маршрутизаторе R2.

```
R2(config)# ntp trusted-key 1
```

e. Включите функцию аутентификации NTP на маршрутизаторе R2.

```
R2(config)# ntp authenticate
```

f. Настройте маршрутизатор R2 как главный NTP-узел, используя команду в формате **ntp master** *stratum-number* в режиме глобальной настройки. Номер слоя указывает на расстояние от источника. В данной лабораторной работе используйте номер слоя **3** на маршрутизаторе R2. Когда устройство узнает время из источника NTP, его номер слоя становится на 1 больше, чем номер слоя его источника.

```
R2(config)# ntp master 3
```

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

Шаг 2: Настройте маршрутизаторы R1 и R3 в качестве клиентов NTP с использованием командной строки.

a. Настройте аутентификацию NTP, задав номер ключа аутентификации, тип хеширования и пароль, которые будут использоваться для аутентификации.

```
R1# config t
R1(config)# ntp authentication-key 1 md5 NTPpassword
```

b. Настройте доверенный ключ, который будет использоваться для аутентификации. Данная команда обеспечивает защиту от случайной синхронизации устройства с недоверенным источником времени.

```
R1(config)# ntp trusted-key 1
```

c. Включите функцию аутентификации NTP.

```
R1(config)# ntp authenticate
```

d. Маршрутизаторы R1 и R3 станут NTP-клиентами маршрутизатора R2. Используйте команду в формате **ntp-сервер** *hostname*. В качестве имени хоста также может применяться IP-адрес. Команда **ntp update-calendar** периодически обновляет календарь в соответствии со временем NTP.

```
R1(config)# ntp server 10.1.1.2
R1(config)# ntp update-calendar
```

e. Убедитесь, что маршрутизатор R1 установил ассоциацию с маршрутизатором R2, с помощью команды **show ntp associations**. Вы также можете использовать более подробную версию команды, добавив аргумент **detail**. Для формирования ассоциации с протоколом NTP может понадобиться некоторое время.

```
R1# show ntp associations

address         ref clock       st   when   poll reach   delay   offset    disp
~10.1.1.2       127.127.1.1      3     14     64     3    0.000   -280073   3939.7
*sys.peer, # selected, +candidate, -outlyer, x falseticker, ~ configured
```

f. Введите команду **debug ntp all** для просмотра NTP-активности на маршрутизаторе R1 по мере его синхронизации с маршрутизатором R2.

```
R1# debug ntp all
NTP events debugging is on
NTP core messages debugging is on
NTP clock adjustments debugging is on
NTP reference clocks debugging is on
NTP packets debugging is on

Dec 17 20.12:18.554: NTP message sent to 10.1.1.2, from interface 'Serial0/0/0' (10.1.1.1).
Dec 17 20.12:18.574: NTP message received from 10.1.1.2 on interface 'Serial0/0/0' (10.1.1.1).
Dec 17 20:12:18.574: NTP Core(DEBUG): ntp_receive: message received
Dec 17 20:12:18.574: NTP Core(DEBUG): ntp_receive: peer is 0x645A3120, next action is 1.
Dec 17 20:12:18.574: NTP Core(DEBUG): receive: packet given to process_packet
Dec 17 20:12:18.578: NTP Core(INFO): system event 'event_peer/strat_chg' (0x04)
status 'sync_alarm, sync_ntp, 5 events, event_clock_reset' (0xC655)
Dec 17 20:12:18.578: NTP Core(INFO): synchronized to 10.1.1.2, stratum 3
Dec 17 20:12:18.578: NTP Core(INFO): system event 'event_sync_chg' (0x03) status
 'leap_none, sync_ntp, 6 events, event_peer/strat_chg' (0x664)
Dec 17 20:12:18.578: NTP Core(NOTICE): Clock is synchronized.
Dec 17 20:12:18.578: NTP Core(INFO): system event 'event_peer/strat_chg' (0x04)
status 'leap_none, sync_ntp, 7 events, event_sync_chg' (0x673)
Dec 17 20:12:23.554: NTP: Calendar updated.
```

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

g. Введите команду **undebug all** или **no debug ntp all**, чтобы выключить процесс отладки.

```
R1# undebug all
```

h. Проверьте время на маршрутизаторе R1 после того, как будет создана ассоциация с маршрутизатором R2.

```
R1# show clock
*20:12:24.859 UTC Wed Dec 17 2014
```

Задача 4: Настройка поддержки syslog на маршрутизаторе R1 и компьютере PC-A

Шаг 1: Установите сервер syslog.

Программа Tftpd32 включает в себя TFTP-сервер, TFTP-клиент, а также сервер и средство просмотра системного журнала. Служба системного журнала Kiwi представляет собой выделенный сервер syslog. В данной лабораторной работе можно использовать любую из этих программ. Обе доступны в виде бесплатной версии и работают в Microsoft Windows.

Если на данный момент на хосте не установлен syslog-сервер, скачайте последнюю версию программы Tftpd32 по ссылке http://tftpd32.jounin.net либо Kiwi по ссылке http://www.kiwisyslog.com и установите ее на свою машину. Если он уже установлен, перейдите к шагу 2.

Примечание. В данной лабораторной работе для показа функционала syslog-сервера используется приложение Ttftpd32.

Шаг 2: Настройте маршрутизатор R1 для регистрации в журнале сообщений на сервере syslog с помощью командной строки.

a. Проверьте, есть ли у вас возможность подключения между маршрутизатором R1 и компьютером PC-A, отправив запрос ping на IP-адрес 192.168.1.1 интерфейса G0/1 маршрутизатора R1. Если это сделать не удается, устраните проблему перед тем, как продолжить.

b. Протокол NTP был настроен в задаче 2 для синхронизации времени в сети. Очень важно, чтобы в сообщениях syslog отображались правильные дата и время, когда syslog используется для мониторинга сети. Если правильные время и дата сообщений неизвестны, то определить, вследствие чего возникло то или иное сообщение о событии, станет затруднительно.

Убедитесь, что на маршрутизаторе включена служба временных меток для ведения журналов, с помощью команды **show run**. Используйте следующую команду, если служба временных меток не включена.

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

c. Настройте службу syslog на маршрутизаторе для отправки сообщений системного журнала на сервер syslog.

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

Шаг 3: Настройте уровень критичности журнальных прерываний на маршрутизаторе R1.

Для журнальных прерываний можно установить поддержку функции ведения журналов. Прерывание – это порог, при достижении которого появляется журнальное сообщение. Уровень журнальных сообщений можно настроить так, чтобы администратор мог определить типы сообщений, которые должны отправляться на сервер syslog. Маршрутизаторы поддерживают различные уровни ведения журналов. Таких уровней восемь: от 0 (авария), который указывает на нестабильность системы, до 7 (отладка), при котором отправляются сообщения, содержащие информацию о маршрутизаторе.

Примечание. Для системного журнала уровень по умолчанию – 6 (информационные сообщения). Консоль и мониторинг по умолчанию имеют уровень 7 (отладка).

a. С помощью команды **logging trap** определите доступные параметры команды и различные уровни прерываний.

```
R1(config)# logging trap ?
<0-7>          Logging severity level
alerts         Immediate action needed           (severity=1)
critical       Critical conditions               (severity=2)
debugging      Debugging messages                (severity=7)
```

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

```
emergencies     System is unusable               (severity=0)
errors          Error conditions                 (severity=3)
informational   Informational messages           (severity=6)
notifications   Normal but significant conditions (severity=5)
warnings        Warning conditions               (severity=4)
<cr>
```

b. Определите уровень серьезности сообщений, отправляемых на сервер syslog. Чтобы настроить уровни серьезности, используйте ключевые слова или номера уровней серьезности (0–7).

Уровень серьезности	Ключевое слово	Значение
0	emergencies	Система неработоспособна
1	alerts	Требуется немедленное действие
2	critical	Критическое состояние
3	errors	Состояние ошибки
4	warnings	Состояние предупреждения
5	notifications	Нормальное, но значащее состояние
6	informational	Информационные сообщения
7	debugging	Сообщения об отладке

Примечание. Уровень серьезности включает в себя указанный уровень, а также все, что имеет более низкий уровень серьезности. Например, если задать уровень 4 или использовать ключевое слово **warnings**, то будут собираться сообщения с уровнем серьезности 4, 3, 2, 1 и 0.

c. Используя команду **logging trap**, установите уровень серьезности для маршрутизатора R1.

```
R1(config)# logging trap warnings
```

d. В чем заключается проблема установки слишком высокого или слишком низкого уровня серьезности?

_____

_____

e. При вводе команды **logging trap critical** сообщения каких уровней серьезности будут записаны в журнал?

_____

_____

Шаг 4: Отобразите текущее состояние ведения журнала на маршрутизаторе R1.

Используйте команду **show logging** для просмотра текущего типа и уровня ведения журнала.

```
R1# show logging
Syslog logging: enabled (0 messages dropped, 3 messages rate-limited, 0 flushes, 0 overruns, xml
disabled, filtering disabled)

No Active Message Discriminator.



No Inactive Message Discriminator.


    Console logging: level debugging, 72 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
```

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

```
    Buffer logging:  level debugging, 72 messages logged, xml disabled,
                     filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

    Trap logging: level warnings, 54 message lines logged
        Logging to 192.168.1.13  (udp port 514, audit disabled,
              link up),
              3 message lines logged,
              0 message lines rate-limited,
              0 message lines dropped-by-MD,
              xml disabled, sequence number disabled
              filtering disabled
        Logging to 192.168.1.3  (udp port 514, audit disabled,
              link up),
              3 message lines logged,
              0 message lines rate-limited,
              0 message lines dropped-by-MD,
              xml disabled, sequence number disabled
              filtering disabled
        Logging Source-Interface:       VRF Name:
<output omitted>
```

Какой уровень ведения журнала включен для консоли?

_____

На каком уровне включено ведение журнала прерываний?

_____

Какой IP-адрес у сервера syslog?

_____

Какой порт использует сервер syslog?

_____

Часть 5: Защита плоскости управления

В части 5 этой лабораторной работы вы выполните следующие задания:

- настройка аутентификации по протоколу маршрутизации OSPF с использованием алгоритма хеширования SHA256;
- проверка работы аутентификации по протоколу маршрутизации OSPF.

Задача 1: Настройка аутентификации по протоколу маршрутизации OSPF с использованием алгоритма хеширования SHA256

Шаг 1: Настройте цепочку ключей на всех трех маршрутизаторах.

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

a. Задайте имя и номер цепочки ключей.

```
R1(config)# key chain NetAcad
R1(config-keychain)# key 1
```

b. Назначьте строку ключа аутентификации.

```
R1(config-keychain-key)# key-string CCNASkeystring
```

c. Настройте используемый алгоритм шифрования. Используйте алгоритм шифрования SHA256.

```
R1(config-keychain-key)#cryptographic-algorithm hmac-sha-256
```

Шаг 2: Настройте использование аутентификации OSPF на последовательных интерфейсах.

a. Используйте команду **ip ospf authentication,** чтобы назначить цепочку ключей последовательным интерфейсам маршрутизаторов R1 и R3.

```
R1(config)# interface s0/0/0
R1(config-if)# ip ospf authentication key-chain NetAcad
R1(config)#
Feb 17 21:24:45.309: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.2 on Serial0/0/0 from FULL to DOWN,
Neighbor Down: Dead timer expired


R3(config)# interface s0/0/1
R3(config-if)# ip ospf authentication key-chain NetAcad
R3(config)#
*Feb 17 21:23:14.078: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.2 on Serial0/0/1 from FULL to DOWN,
Neighbor Down: Dead timer expired
```

b. Используйте команду **ip ospf authentication**, чтобы назначить цепочку ключей обоим последовательным интерфейсам на маршрутизаторе R2.

```
R2(config)# interface s0/0/0
R2(config-if)# ip ospf authentication key-chain NetAcad
R2(config)# interface serial 0/0/1
R2(config-if)# ip ospf authentication key-chain NetAcad
R2(config-if)#
Feb 17 21:36:25.114: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from LOADING
to FULL, Loading Done
Feb 17 21:36:30.686: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1 from LOADING
to FULL, Loading Done
```

Шаг 3: Проверьте правильность маршрутизации и аутентификации по протоколу OSPF.

a. Введите команду **ip ospf interface** и убедитесь, назначен ли ключ аутентификации последовательным интерфейсам на всех маршрутизаторах.

```
R1# show ip ospf interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Internet Address 10.1.1.1/30, Area 0, Attached via Network Statement
  Process ID 1, Router ID 192.168.1.1, Network Type POINT_TO_POINT, Cost: 64
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           64        no          no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:02
  Supports Link-local Signaling (LLS)
```

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

```
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.2.2.2
  Suppress hello for 0 neighbor(s)
  Cryptographic authentication enabled
    Sending SA: Key 1, Algorithm HMAC-SHA-256 - key chain NetAcad
R1#
```

b. Введите команду **show ip ospf neighbor** и убедитесь, что каждый маршрутизатор выводит список других маршрутизаторов в сети как соседей.

```
R2# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.3.1       0   FULL/  -        00:00:39    10.2.2.1        Serial0/0/1
192.168.1.1       0   FULL/  -        00:00:37    10.1.1.1        Serial0/0/0
R2#
```

c. Введите команду **show ip route** и убедитесь, что все сети отображаются в таблице маршрутизации на всех маршрутизаторах.

```
R3# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O        10.1.1.0/30 [110/1562] via 10.2.2.2, 00:01:56, Serial0/0/1
C        10.2.2.0/30 is directly connected, Serial0/0/1
L        10.2.2.1/32 is directly connected, Serial0/0/1
O     192.168.1.0/24 [110/1563] via 10.2.2.2, 00:01:46, Serial0/0/1
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, GigabitEthernet0/1
L        192.168.3.1/32 is directly connected, GigabitEthernet0/1
```

d. Используйте команду **ping** для проверки связи между компьютерами PC-A и PC-C.

Если запрос ping завершается ошибкой, проведите диагностику перед тем, как продолжить.

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

Часть 6: Настройка автоматизированных функций безопасности

В части 6 этой лабораторной работы вы выполните следующие задания:

- защита маршрутизатора R3 с помощью AutoSecure;
- проверка конфигурации безопасности маршрутизатора через интерфейс командной строки CLI.

Задача 1: Защита маршрутизатора R3 с помощью AutoSecure

С помощью одной команды в режиме командной строки функция AutoSecure позволяет отключать общие сервисы IP, которые могут быть использованы для сетевых атак. Она также позволяет включать сервисы IP и функции, которые могут помочь в защите сети от атак. AutoSecure упрощает настройку безопасности маршрутизатора и делает конфигурацию маршрутизатора надежнее.

Шаг 1: Используйте функцию AutoSecure системы Cisco IOS.

a. Войдите в привилегированный режим, используя команду **enable**.

b. Введите команду **auto secure** на маршрутизаторе R3, чтобы его заблокировать. Маршрутизатор R2 представляет собой маршрутизатор поставщика ISP, поэтому имейте в виду, что при запросах AutoSecure интерфейс S0/0/1 маршрутизатора R3 подключается к Интернету. Ответьте на вопросы AutoSecure, как показано в выходных данных ниже. Ответы выделены полужирным шрифтом.

```
R3# auto secure
                --- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***

AutoSecure will modify the configuration of your device.
All configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
Autosecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]: yes
Enter the number of interfaces facing the internet [1]: [Enter]

Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0         unassigned      YES manual administratively down down
GigabitEthernet0/1         192.168.3.1     YES manual up                    up
Serial0/0/0                unassigned      YES NVRAM  administratively down down
Serial0/0/1                10.2.2.1        YES manual up                    up
Enter the interface name that is facing the internet: Serial0/0/1

Securing Management plane services...
```

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

```
Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp

Here is a sample Security Banner to be shown
at every access to device. Modify it to suit your
enterprise requirements.

Authorized Access only
  This system is the property of So-&-So-Enterprise.
  UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
  You must have explicit permission to access this
  device. All activities performed on this device
  are logged. Any violations of access policy will result
  in disciplinary action.

Enter the security banner {Put the banner between
k and k, where k is any character}:
#  Unauthorized Access Prohibited #
Enter the new enable password: cisco67890
Confirm the enable password: cisco67890
Configuring AAA local authentication
Configuring console, Aux and vty lines for
local authentication, exec-timeout, transport
Securing device against Login Attacks
Configure the following parameters

Blocking Period when Login Attack detected: 60

Maximum Login failures with the device: 2

Maximum time period for crossing the failed login attempts: 30

Configure SSH server? [yes]: [Enter]

Configuring interface specific AutoSecure services
Disabling the following ip services on all interfaces:
```

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

```
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
Disabling mop on Ethernet interfaces

Securing Forwarding plane services...

Enabling unicast rpf on all interfaces connected
to internet

Configure CBAC Firewall feature? [yes/no]: no

This is the configuration generated:

no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
banner motd ^C  Unaauthorized Access Prohibited ^C
security authentication failure rate 10 log
enable password 7 121A0C0411045A53727274
aaa new-model
aaa authentication login local_auth local
line console 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line aux 0
 login authentication local_auth
 exec-timeout 10 0
 transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet
line tty 1 2
 login authentication local_auth
 exec-timeout 15 0
```

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

```
login block-for 60 attempts 2 within 30
crypto key generate rsa general-keys modulus 1024
ip ssh time-out 60
ip ssh authentication-retries 2
line vty 0 4
 transport input ssh telnet
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
interface Embedded-Service-Engine0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface GigabitEthernet0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface GigabitEthernet0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface Serial0/0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface Serial0/0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
access-list 100 permit udp any any eq bootpc
interface Serial0/0/1
 ip verify unicast source reachable-via rx allow-default 100
```

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

```
!
end


Apply this configuration to running-config? [yes]: [Enter]

Applying the config generated to running-config
% You already have RSA keys defined named R3.ccnasecurity.com.
% They will be replaced.

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

*Feb 18 20:29:18.159: %SSH-5-DISABLED: SSH 2.0 has been disabled
R3#
000066: *Feb 18 20:29:21.023 UTC: %AUTOSEC-1-MODIFIED: AutoSecure configuration has been Modified
on this device
R3#
```

Примечание. Задаваемые вопросы и выходные данные могут варьироваться в зависимости от особенностей образа IOS и устройства.

Шаг 2: Установите SSH-соединение между компьютером PC-C и маршрутизатором R3.

a. Запустите PuTTy или другой SSH-клиент и войдите в систему под именем **admin** и с паролем **cisco12345**, созданными при запуске AutoSecure. Введите **192.168.3.1** в качестве IP-адреса интерфейса G0/1 маршрутизатора R3.

b. Так как на маршрутизаторе R3 протокол SSH был настроен с помощью AutoSecure, вы получите предупреждение о безопасности от PuTTY. Несмотря на это, нажмите **Yes**, чтобы подключиться.

c. Войдите в привилегированный режим и проверьте конфигурацию маршрутизатора R3 с помощью команды **show run**.

d. Введите команду **show flash**. Здесь есть файл, который может относиться к AutoSecure? Если да, то как он называется и когда был создан?

_____

_____

e. Введите команду **more flash:pre_autosec.cfg**. Что содержит этот файл и каково его предназначение?

_____

_____

f. Каким образом можно восстановить этот файл, если AutoSecure не произвел необходимых результатов?

_____

_____

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

Шаг 3: Сравните конфигурацию маршрутизатора R3, сгенерированную функцией AutoSecure, с конфигурацией маршрутизатора R1, настроенной вручную.

a. Какие изменения настроек безопасности были произведены функцией AutoSecure на маршрутизаторе R3, которые не были произведены в предыдущих разделах лабораторной работы на маршрутизаторе R1?

b. Какие изменения настроек безопасности были произведены в предыдущих разделах лабораторной работы, которые не были произведены функцией AutoSecure?

c. Укажите по крайней мере пять ненужных сервисов, которые были заблокированы функцией AutoSecure, и хотя бы три меры безопасности, примененные к каждому из интерфейсов.

Примечание. Некоторые из перечисленных сервисов, будучи отключенными на выходе AutoSecure, могут не появляться в выходных данных команды **show running-config**, так как они были отключены по умолчанию для данного маршрутизатора и версии Cisco IOS.

Среди отключенных сервисов:

Для каждого интерфейса были отключены следующие параметры:

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

Шаг 4: Проверьте связь.

Отправьте ping-запрос с компьютера PC-A в локальной сети маршрутизатора R1 на компьютер PC-C в локальной сети маршрутизатора R3. Если ping-запрос с компьютера PC-A на PC-C завершается ошибкой, проведите диагностику перед тем, как продолжить.

Вопросы для повторения

1. Объясните, чем важны защита доступа к маршрутизатору и мониторинг сетевых устройств.

   _____

   _____

   _____

   _____

   _____

   _____

2. Какие преимущества протокол SSH имеет перед Telnet?

   _____

   _____

3. Насколько масштабируемой является процедура назначения имен пользователей и использования локальной базы данных для аутентификации?

   _____

   _____

   _____

   _____

   _____

   _____

4. Почему использование централизованных серверов журналов лучше, чем маршрутизаторов, ведущих журнал только локально?

   _____

   _____

   _____

   _____

   _____

   _____

5. Каковы преимущества использования функции AutoSecure?

   _____

   _____

   _____

   _____

   _____

   _____

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

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.

© 2020 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.