Тема 1 Организация безопасного удаленного доступа

Занятие 1. Защита доступа к устройствам сети

Дисциплина: Анализ информационных потребностей подразделений информационно-аналитического мониторинга

Доцент: Кирьянов Александр Владимирович
email:kiryanov_a@mirea.ru

Учебные вопросы и цели занятия:

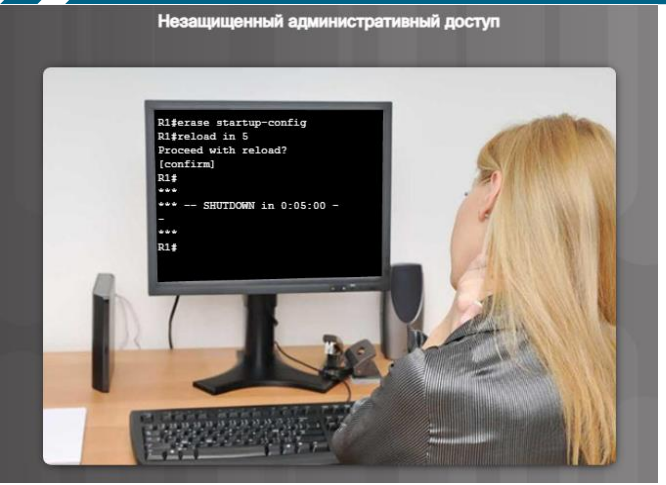
1. Защита сетевой инфраструктуры.
2. Защита сети с использованием паролей.
3. Защита сети по протоколу SSH.

Вступительная часть

Обеспечение безопасности проходящего сетевого трафика и внимательное изучение входящего трафика являются критически важными аспектами сетевой безопасности. Защита граничного маршрутизатора, который подключается к внешней сети, – это важный первый шаг в обеспечении безопасности сети.

Защищая сеть, не менее важно защищать сами устройства. Это включает использование интерфейса командной строки Cisco IOS для внедрения проверенных способов физической защиты маршрутизатора и защиты административного доступа к маршрутизатору. Некоторые из этих способов включают обеспечение безопасности административного доступа, в том числе: ведение паролей, конфигурирование расширенных функций виртуальной учетной записи и внедрение протокола Secure Shell (SSH). Так как не все ИТ-специалисты должны иметь одинаковый уровень доступа к устройствам инфраструктуры, определение административных ролей с точки зрения доступа – это еще один важный аспект защиты устройств инфраструктуры.

Первый учебный вопрос.
Защита доступа к устройствам



Защита сетевой инфраструктуры

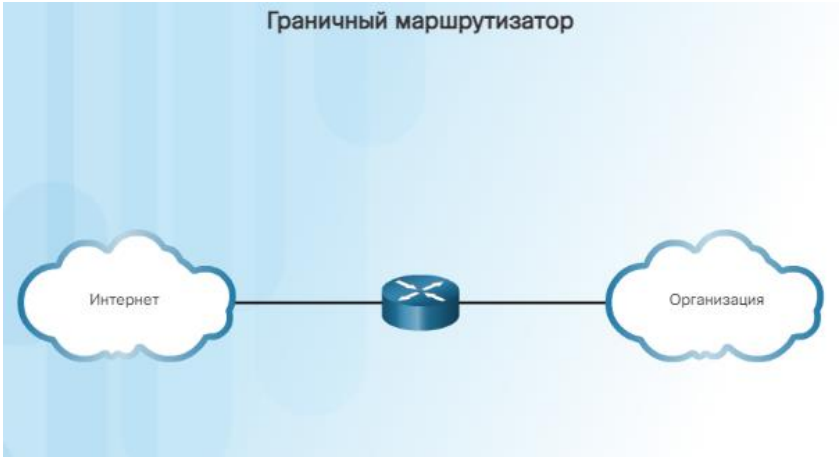
Защита сетевой инфраструктуры крайне важна для безопасности сети в целом. Сетевая инфраструктура включает маршрутизаторы, коммутаторы, серверы, оконечные устройства и другое оборудование.

Представьте невежливого сотрудника, который заглядывает через плечо сетевого администратора, когда тот выполняет вход в маршрутизатор. Злоумышленнику на удивление просто получить несанкционированный доступ.

Если злоумышленник получает доступ к маршрутизатору, то могут быть скомпрометированы безопасность и управление всей сети. Например, злоумышленник стер начальную конфигурацию и заставил маршрутизатор перезагрузиться через пять минут. Когда маршрутизатор загрузится снова, начальной конфигурации на нем уже не будет.

Для предотвращения несанкционированного доступа ко всем инфраструктурным устройствам необходимо внедрять соответствующие политики безопасности и средства управления. Маршрутизаторы являются основными целями для злоумышленников, потому что эти устройства играют роль «дорожной полиции», регулируя перемещение трафика между сетями.

Первый учебный вопрос.
Защита доступа к устройствам



Граничный маршрутизатор, показанный на рисунке, – это последний маршрутизатор между внутренней сетью и недоверенной сетью, например Интернетом. Весь интернет-трафик организации проходит через граничный маршрутизатор, который зачастую выполняет роль первой и последней линии обороны сети. Граничный маршрутизатор помогает защитить периметр сети и выполняет действия по защите на основе политик безопасности организации. Именно поэтому так важно обеспечивать защиту сетевых маршрутизаторов.

Подходы к защите граничных маршрутизаторов

Внедрение граничного маршрутизатора отличается в зависимости от размера сети и сложности требуемого дизайна сети. Маршрутизатор можно внедрять как отдельное устройство, защищающее всю внутреннюю сеть, или как устройство первой линии обороны в случае так называемого подхода «эшелонированной обороны».

Подход с использованием одного маршрутизатора

На рисунке один маршрутизатор подключает защищаемую сеть или внутреннюю локальную сеть (LAN) к Интернету. Все политики безопасности сконфигурированы на этом устройстве. Такой подход обычно применяется на небольших площадках, например в небольших офисах, домашних офисах (SOHO) или офисах филиалов. В небольших сетях требуемые функции безопасности могут быть реализованы с использованием маршрутизаторов с интеграцией сервисов (Integrated Services Routers, ISR), без снижения производительности маршрутизатора.

Первый учебный вопрос.
Защита доступа к устройствам

Маршрутизатор сначала анализирует трафик перед его передачей на специальный межсетевой экран, например на устройство Cisco ASA.

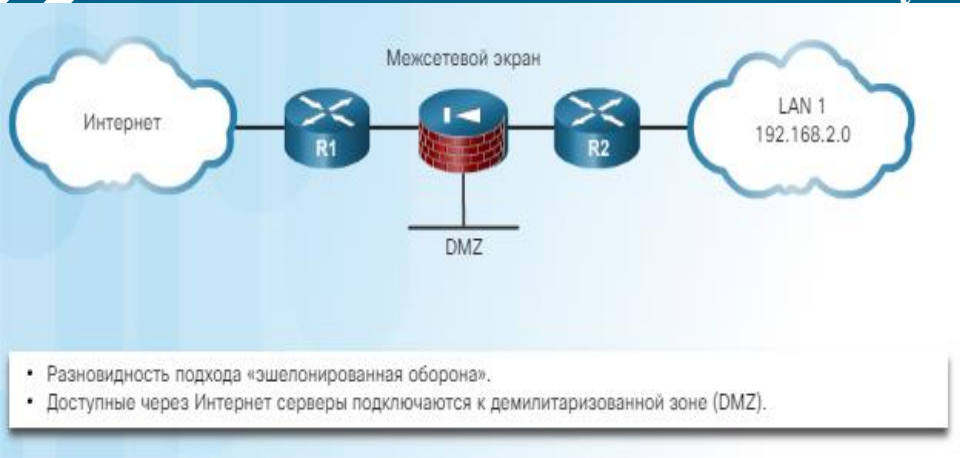
Подход «эшелонированная оборона»

Подход «эшелонированная оборона» более надежен, чем подход с использованием одного маршрутизатора. До того как трафик попадет в защищаемую локальную сеть, он должен будет пройти через несколько уровней обороны. На рисунке показано **три основных уровня обороны**: граничный маршрутизатор, межсетевой экран и внутренний маршрутизатор, который подключается к защищаемой локальной сети.

Граничный маршрутизатор выполняет роль первой линии обороны и называется также экранирующим маршрутизатором. Выполнив первоначальную фильтрацию трафика, граничный маршрутизатор передает все подключения, которые предназначены для внутренней локальной сети, на вторую линию обороны, коей служит межсетевой экран.

Обычно межсетевой экран начинает свою работу с того момента, на котором ее заканчивает граничный маршрутизатор, и выполняет дополнительную фильтрацию. Он обеспечивает дополнительный контроль доступа за счет отслеживания состояния подключения и выполняет роль контрольно-пропускного устройства. По умолчанию, межсетевой экран запрещает подключения с внешних (недоверенных) сетей к внутренней (доверенной) сети. Однако он позволяет внутренним пользователям устанавливать подключения к недоверенным сетям и разрешает проходить через него обратным ответам. Межсетевой экран может также выполнять аутентификацию пользователей (аутентификацию прокси-сервера), когда пользователи должны аутентицифироваться, чтобы получить доступ к сетевым ресурсам.

Маршрутизаторы не единственные устройства, которые можно использовать для эшелонированной обороны. Можно также развертывать и другие инструменты защиты, такие как системы предотвращения вторжений (IPS), устройства защиты веб-трафика (прокси-серверы) и устройства защиты электронной почты (фильтрации спама).

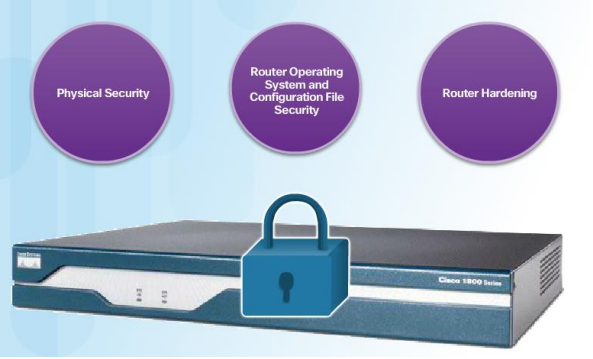


Подход DMZ

На рисунке представлен вариант эшелонированной обороны. Этот подход подразумевает наличие промежуточной зоны, которую обычно называют демилитаризованной зоной (DMZ).

DMZ может использоваться серверами, которые должны быть доступны из Интернета или каких-либо других внешних сетей. DMZ можно настроить между двумя маршрутизаторами, с внутренним маршрутизатором, подключенным к защищаемой сети, и внешним маршрутизатором, подключенным к незащищенной сети. В качестве альтернативы, DMZ может быть просто дополнительный выключенный порт одного маршрутизатора. Межсетевой экран располагается между защищенной и незащищенной сетями. Межсетевой экран настраивается таким образом, чтобы разрешать требуемые подключения, например HTTP, от внешних (недоверенных) сетей к публичным серверам в DMZ. Межсетевой экран служит основной защитой для всех устройств в DMZ.

Первый учебный вопрос.
Защита доступа к устройствам



Защита маршрутизатора периметра – это критически важный первый шаг для обеспечения безопасности сети. Как показано на рисунке, защиту маршрутизатора необходимо обеспечивать в трех областях.

Физическая безопасность

Обеспечение физической безопасности маршрутизаторов.

- Маршрутизатор и физические устройства, к которым он подключается, должны находиться в запертом помещении, доступ в которое разрешен только уполномоченному персоналу.
- В помещении не должно быть электростатических и магнитных помех, должна быть система пожаротушения и регуляторы температуры и влажности.
- Установите бесперебойный источник питания (ИБП) или дизельный резервный генератор, а также всегда имейте в наличии запасные детали.

Защита операционной системы

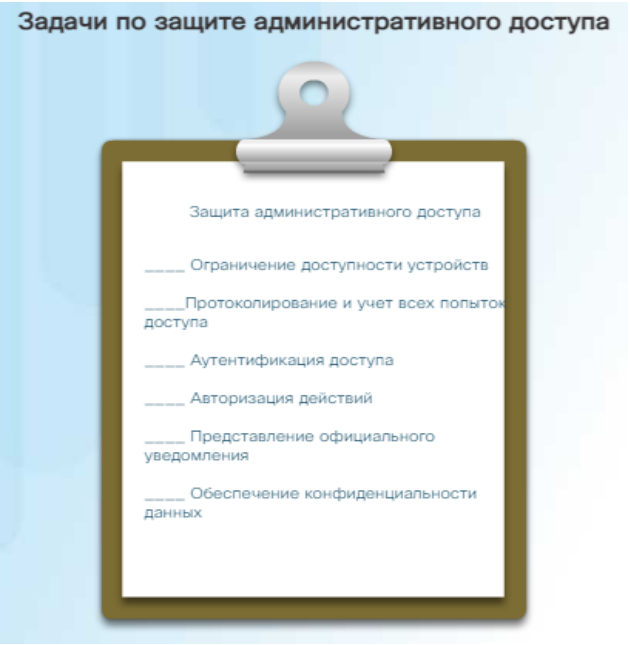
Для защиты операционных систем маршрутизаторов следует выполнить несколько действий.

- Сконфигурируйте маршрутизатор так, чтобы в нем был доступен максимальный объем памяти. Чем больше свободной памяти, тем меньше риск выхода сети из строя при воздействии атак типа «отказ в обслуживании», а также больше возможностей использования широкого ряда функций безопасности.
- Используйте самую последнюю, надежную версию операционной системы, удовлетворяющую техническим характеристикам функций маршрутизатора или сетевого устройства. Функции безопасности и шифрования в операционной системе постоянно совершенствуются и обновляются, поэтому критически важно иметь самую последнюю обновленную версию.
- Создавайте резервную копию образов ОС маршрутизатора и файлов конфигурации маршрутизатора.

Укрепление защиты маршрутизатора

- Устранение потенциального неправомерного использования незадействованных портов и сервисов.
- Обеспечьте защиту административного управления. Проверьте, что только уполномоченный персонал может иметь соответствующий доступ и что этот уровень доступа контролируется.
- Отключите неиспользуемые порты и интерфейсы. Уменьшите число способов, с помощью которых осуществляется доступ к устройству.
- Отключите ненужные сервисы.

Первый учебный вопрос.
Защита доступа к устройствам



Защита административного доступа – это чрезвычайно важная задача безопасности. Если неуполномоченный сотрудник получает административный доступ к маршрутизатору, он может изменить параметры маршрутизации, отключить функции маршрутизации или обнаружить и получить доступ к другим системам в сети.

На рисунке показано несколько важных задач по защите административного доступа к устройствам инфраструктуры:

- **Ограничение доступности устройства.** Ограничьте число доступных портов, ограничьте разрешенные коммуникации и способы доступа.
- **Фиксация и учет всех попыток доступа.** В целях аудита записывайте всех, кто и когда входит в устройство, и что он на нем делает.
- **Аутентификация доступа.** Обеспечьте предоставление доступа только уполномоченным пользователям, группам и сервисам. Ограничьте число неудачных попыток входа и время между входами.
- **Авторизация действий.** Ограничьте доступность действий и представлений только уполномоченными пользователями, группами или сервисами.
- **Предоставление официальных уведомлений.** При интерактивных сеансах отображайте официальное уведомление, разработанное в сотрудничестве с юристами компании.
- **Обеспечение конфиденциальности данных.** Защищайте локально сохраняемые конфиденциальные данные от просмотра и копирования. Не забывайте, что данные, передающиеся по коммуникационному каналу, могут быть прослушаны, перехвачены и подвержены атакам «человек посередине» (man-in-the-middle, MITM).

Первый учебный вопрос.
Защита доступа к устройствам

Безопасный локальный и удаленный доступ

Доступ к маршрутизатору в административных целях может осуществляться локально или удаленно.

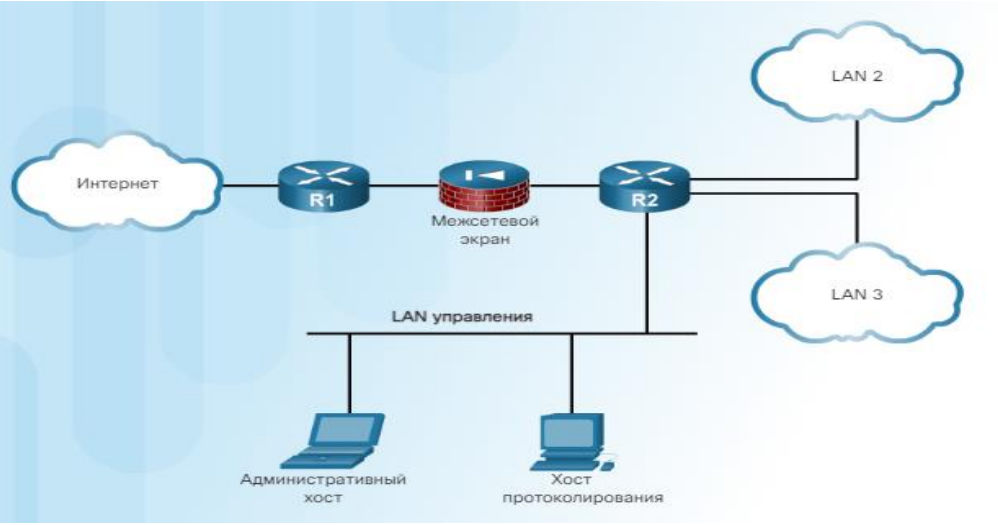
- **Локальный доступ.** Доступ ко всем устройствам сетевой инфраструктуры может выполняться локально. Для локального доступа к маршрутизатору обычно требуется прямое подключение к консольному порту на маршрутизаторе Cisco, а также использование компьютера, на котором запущено ПО эмуляции терминалов, как показано на рис. 1. Администратор должен иметь физический доступ к маршрутизатору и использовать консольный кабель для подключения к консольному порту. Локальный доступ обычно используется для первоначальной конфигурации устройства.

- **Удаленный доступ.** Администраторы могут также входить на инфраструктурные устройства удаленно, как показано на рисунках 2 и 3. Хотя для этого доступен вариант со вспомогательным (aux) портом, наиболее распространенными видами доступа являются подключения к маршрутизатору по протоколам Telnet, SSH, HTTP, HTTPS или SNMP с компьютера. Компьютер может быть как в локальной сети, так и в удаленной.

Первый учебный вопрос.
Защита доступа к устройствам

Некоторые протоколы удаленного доступа отправляют на маршрутизатор данные, включая имена пользователей и пароли, в виде простого текста. Если злоумышленник может собрать сетевой трафик, когда администратор удаленно входит на маршрутизатор, то этот злоумышленник может завладеть паролями или данными о конфигурации маршрутизатора. Поэтому предпочтительно разрешать только локальный доступ к маршрутизатору. Однако в некоторых случаях удаленный доступ может быть также необходим. При удаленном доступе к маршрутизатору необходимо соблюдать следующие меры предосторожности.

- Шифруйте весь трафик между компьютером администратора и маршрутизатором. Например, вместо Telnet используйте SSH версии 2 или вместо HTTP используйте HTTPS.
- Создайте выделенную сеть управления, как показано на рис. 4. Сеть управления должна включать только идентифицированные административные хосты и подключения к выделенному интерфейсу на маршрутизаторе.



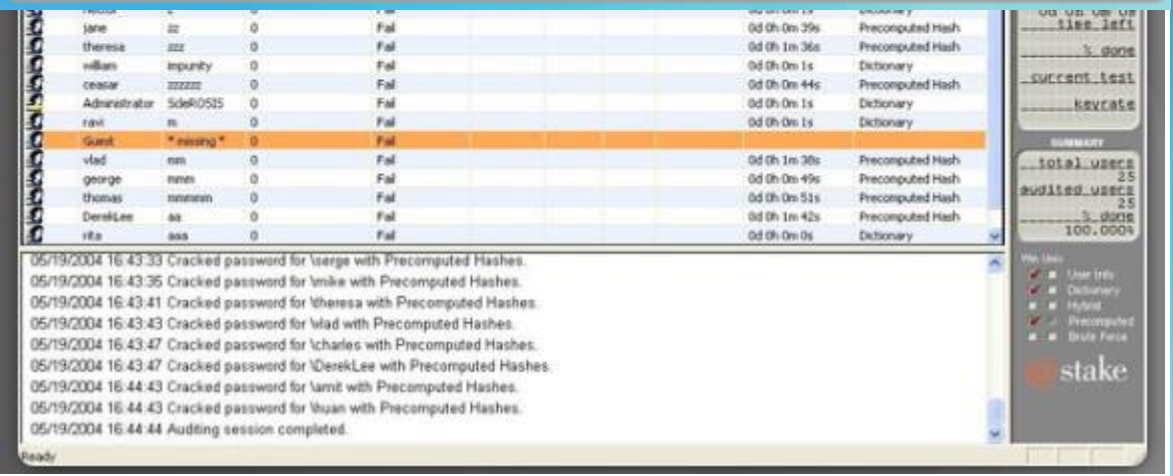
- Сконфигурируйте фильтр пакетов, чтобы доступ к маршрутизатору могли иметь только идентифицированные административные хосты и предпочтительные протоколы. Например, для инициирования подключения к маршрутизаторам к сети разрешите только SSH-запросы с IP-адреса хоста администрирования.
- Сконфигурируйте и установите VPN-подключение к локальной сети до подключения к интерфейсу управления маршрутизатором.

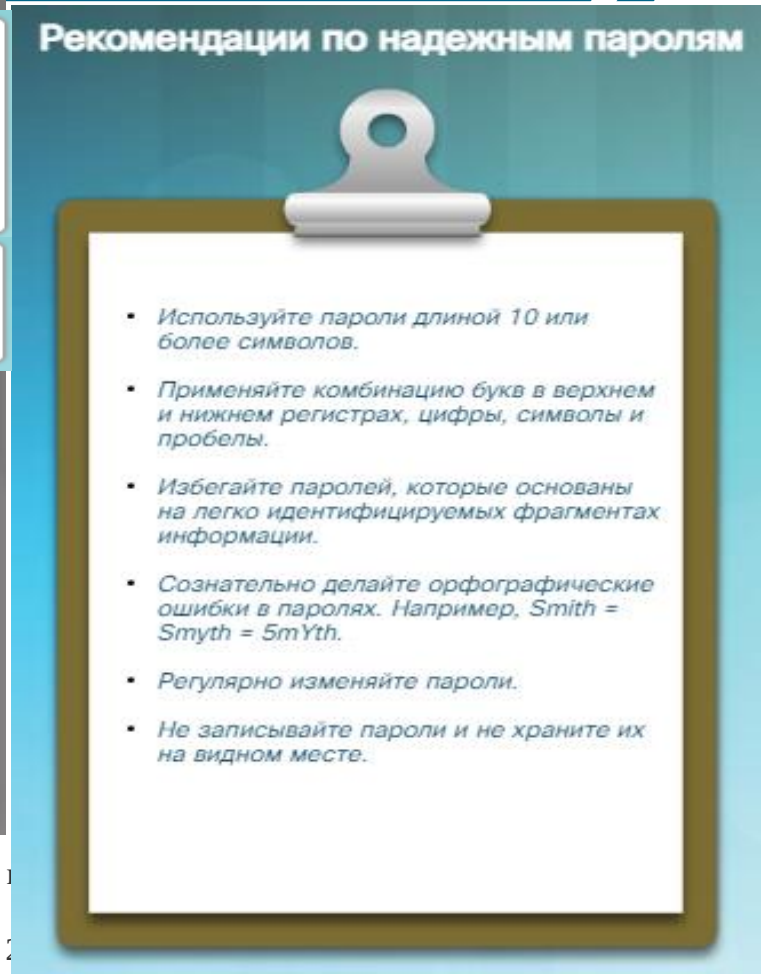
Эти меры предосторожности важно предпринимать, но они не смогут полностью защитить сеть. Также необходимо использовать и другие способы защиты. Одним из базовых и важных способов является использование надежных паролей.

Второй учебный вопрос.
Защита сети с использованием паролей

Ненадежный пароль	Почему он ненадежен?
secret	Простой словарный пароль
smith	Девичья фамилия матери
toyota	Марка автомобиля
bob1967	Имя пользователя и его день рождения
Blueleaf23	Простые слова и цифры

Надежный пароль	Почему он надежен?
b67n42d39c	Используется комбинация алфавитно-цифровых символов
12^h u4@1p7	Используется комбинация букв, цифр, символов, а также пробел

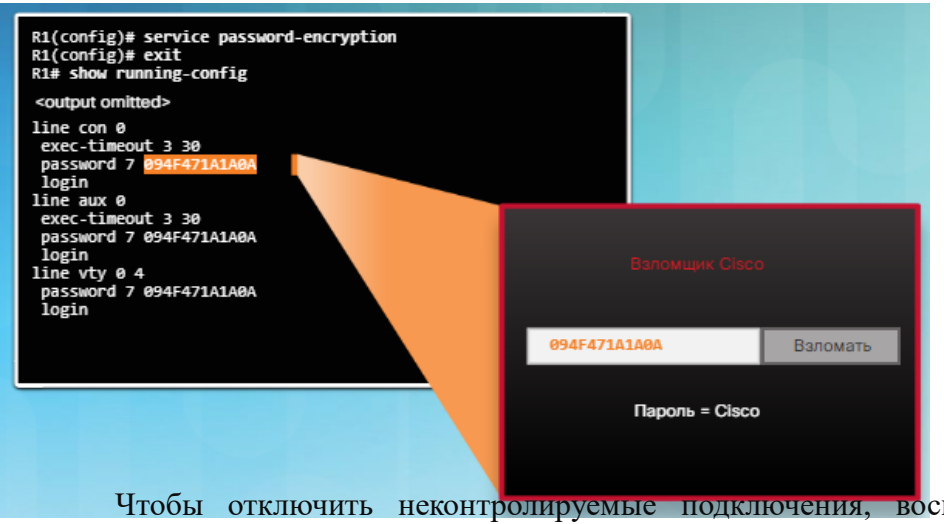




Администраторы должны гарантировать применение надежных паролей и рекомендациям по созданию надежных паролей для защиты таких ресурсов, коммутаторы. Рекомендации по созданию надежных паролей представлены на рис. 2

Второй учебный вопрос.
Защита сети с использованием паролей


```
R1(config)# security passwords min-length 10
R1(config)# service password-encryption
R1(config)# line vty 0 4
R1(config-line)# exec-timeout 3 30
R1(config-line)# line console 0
R1(config-line)# exec-timeout 3 30
```



Повышение безопасности доступа Как показано на рис. 1, для повышения безопасности паролей можно воспользоваться разными командами конфигурации маршрутизатора.

По умолчанию минимальная длина пароля – 6 символов. Для увеличения минимальной длины пароля воспользуйтесь командой режима глобальной конфигурации **security passwords min-length** *length* .

По умолчанию, за исключением пароля, сгенерированного командой **enable secret,** все пароли маршрутизаторов Cisco хранятся в виде простого текста в файлах конфигурации загрузки и запуска маршрутизатора. Для шифрования всех паролей, передаваемых простым текстом, используйте команду **service password-encryption** в режиме глобальной конфигурации. Как показано на рис. 2, шифрование очень просто взламывается, если использовать подходящий инструмент. Поэтому эта команда не должна использоваться с целью зашиты файлов конфигурации от серьезных атак.

По умолчанию интерфейс администратора остается активным, с выполненным входом, в течение 10 минут с момента активности последнего сеанса.

Чтобы отключить неконтролируемые подключения, воспользуйтесь командой **exec-timeout** *minutes* [*seconds*] в режиме конфигурации линий для каждой из линий, которые конфигурируются для доступа.

Можно также отключить процесс EXEC для определенной линии, например порта aux, используя команду **no exec** в режиме конфигурации линий. Эта команда разрешает только исходящее подключение по линии, отключая процесс EXEC для подключений, которые могут пытаться отправлять незатребованные данные на маршрутизатор.

Второй учебный вопрос.
Защита сети с использованием паролей

```
R2(config)# enable secret cisco12345
R2(config)# do show run | include enable
enable secret 5 $1$cam7$99EfzkvmJ5h1gEbryLVRy.
R1(config)# enable secret ?
  0       Specifies an UNENCRYPTED password will follow
  5       Specifies a MD5 HASHED secret will follow
  8       Specifies a PBKDF2 HASHED secret will follow
  9       Specifies a SCRYPT HASHED secret will follow
  LINE    The UNENCRYPTED (cleartext) 'enable' secret
  level   Set exec level password

R1(config)# line con 0
R1(config-line)# password ?
  0     Specifies an UNENCRYPTED password will follow
  7     Specifies a HIDDEN password will follow
  LINE  The UNENCRYPTED (cleartext) line password
R1(config-line)#
```

```
R1(config)# enable secret 9 cisco12345
ERROR: The secret you entered is not a valid encrypted secret.
To enter an UNENCRYPTED secret, do not specify type 9 encryption.
When you properly enter an UNENCRYPTED secret, it will be encrypted.

R1(config)# enable secret 9
$9$HZWdzLHwhPtZ3U$D9OlUDSGvBy.m8Tf9vCGDJRcYy8zIMbyRJgtxgRkwzY
R1(config)#
```

Чтобы ввести незашифрованный пароль, воспользуйтесь синтаксисом команды **enable algorithm-type,** показанным на рис. 3.

Алгоритмы пароля Secret

Хеши MD5 больше не считаются безопасными, так как злоумышленники могут воссоздавать сертификаты подлинности. После этого злоумышленники могут сфальсифицировать любой веб-сайт. Команда **enable secret password**, показанная на рис. 1, использует хеш MD5 по умолчанию. Поэтому сегодня рекомендуется, чтобы все секретные пароли конфигурировались с использованием паролей типа 8 или 9. Тип 8 и тип 9 были представлены в ОС Cisco IOS 15.3(3)M. В них используется шифрование SHA. Так как тип 9 несколько надежнее, чем тип 8, он будет использоваться в качестве примера в этом курсе (всегда, когда это разрешено Cisco IOS).

На рис. 2 показано, что конфигурирование шифрования типа 9 не так просто, как может показаться. Целая просто ввести команду

```
Router(config)#
enable algorithm-type {md5 | scrypt | sha256 } secret unencrypted-password
```

Ключевое слово алгоритма	Описание
md5	Тип 5; выбирает алгоритм дайджеста сообщения 5 (MD5) в качестве алгоритма хеширования.
scrypt	Тип 9; выбирает scrypt в качестве алгоритма хеширования.
sha256	Тип 8; выбирает функцию формирования ключей на основе пароля 2 (PBKDF2) с защищенным алгоритмом хеширования, 256 бит (SHA-256) в качестве алгоритма хеширования.

Второй учебный вопрос.
Защита сети с использованием паролей


```
R1(config)# enable algorithm-type ?
  md5     Encode the password using the MD5 algorithm
  scrypt  Encode the password using the SCRYPT hashing algorithm
  sha256  Encode the password using the PBKDF2 hashing algorithm
R1(config)# enable algorithm-type scrypt ?
  secret  Assign the privileged level secret (MAX of 25 characters)

R1(config)# enable algorithm-type scrypt secret cisco12345
R1(config)# do show run | include enable
enable secret 9 $9$Gyk9x3Ve4c0n5k$8.cR3yReBduzHymEyCOcErgPKW8MSKokRN
9KjEg4WQA
R1(config)#
```

Пример конфигурации показан на рис. 4. Обратите внимание, что текущая конфигурация теперь показывает **enable secret password** типа 9.

Шифрование типов 8 и 9 было также представлено в ОС Cisco IOS 15.3(3)M для команды **username secret** . Аналогично команде enable secret, если вы просто введете пользователя с командой username secret, шифрование по умолчанию будет MD5.

```
Router(config)#
username name algorithm-type {md5 | scrypt | sha256 } secret unencrypted-password
```

```
R1(config)# username Bob secret cisco54321
R1(config)# do show run | include username
username Bob privilege 15 secret 5 $1$lmBB$UjOC6JA4f1WgI3/La8wGz/
R1(config)#
R1(config)# username Bob algorithm-type scrypt secret cisco54321
R1(config)# do show run | include username
username Bob privilege 15 secret 9 $9$9FkS.zTuLs89pk$v5P2y.M6reR181S
92moKHdFauk8joK0xHICXxGDuurs
R1(config)#
```

Используйте команду **username** *name* **algorithm-type** для задания шифрования типа 9. Синтаксис показан на рис. 5, там же приведен пример.

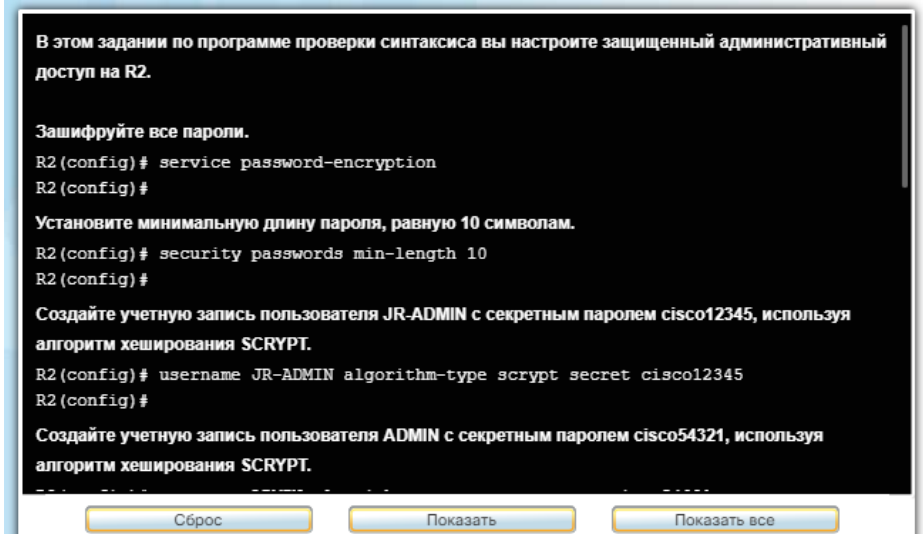
```
R1(config)# enable password ?
  0       Specifies an UNENCRYPTED password will follow
  7       Specifies a HIDDEN password will follow
  LINE    The UNENCRYPTED (cleartext) 'enable' password
  level   Set exec level password

R1(config)# username Bob password ?
  0       Specifies an UNENCRYPTED password will follow
  7       Specifies a HIDDEN password will follow
  LINE    The UNENCRYPTED (cleartext) user password

R1(config)# line con 0
R1(config-line)# password ?
  0       Specifies an UNENCRYPTED password will follow
  7       Specifies a HIDDEN password will follow
  LINE    The UNENCRYPTED (cleartext) line password
```

В целях обратной совместимости, в Cisco IOS доступны команды **enable password**, **username password** и **line password**. Эти команды не используют шифрование по умолчанию. В лучшем случае они могут использовать шифрование типа 7, как показано на рис. 6. Поэтому эти команды мы в данном курсе рассматривать не будем.

Второй учебный вопрос.
Защита сети с использованием паролей

```
R1(config)# username Bob algorithm-type scrypt secret cisco54321
R1(config)# line con 0
R1(config-line)# login local
R1(config-line)# exit
R1(config)# line aux 0
R1(config-line)# login local
R1(config-line)# exit
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
```

Воспользуйтесь программой проверки синтаксиса (см. рис. 2), чтобы защитить административный доступ к маршрутизатору R2.



Защита доступа к линии

По умолчанию консольный и aux-порты не требуют пароля для административного доступа. Кроме того, команда **password,** сконфигурированная на консоли, vty и вспомогательные (aux) линии могут использовать только тип 7. Таким образом, для аутентификации по имени пользователя/паролю консольную и вспомогательную линии нужно конфигурировать с помощью команды **login local** . Кроме того, vty-линии должны конфигурироваться только для SSH-доступа, как показано на рис. 1.

Некоторые устройства Cisco имеют более пяти vty-линий. Прежде чем настроить пароль, проверьте количество vty-линий в текущей конфигурации. Например, коммутаторы Cisco одновременно поддерживают до 16 vty-линий, пронумерованных от 0 до 15.

Второй учебный вопрос.
Защита сети с использованием паролей

Расширенные возможности обеспечения безопасности виртуального входа в систему

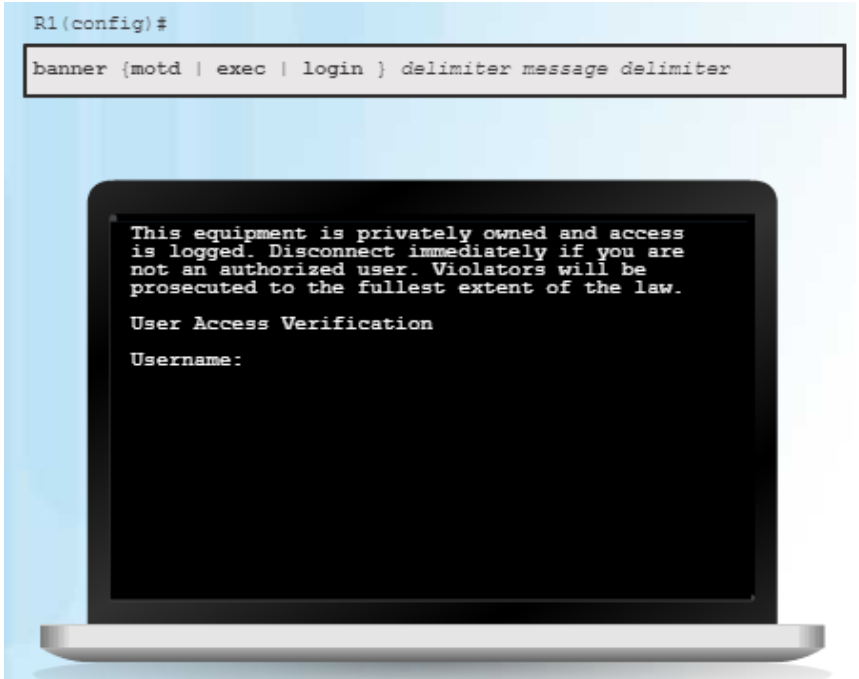
- Установите задержку между последовательными попытками входа в систему.
- Включите функцию отключения входа в систему, если предполагаются DoS-атаки.
- Генерируйте системные регистрируемые сообщения для обнаружения входа в систему.

Усовершенствование процесса входа в систему

Применение паролей и локальной аутентификации не может предотвратить целевую атаку на устройство. Усовершенствованные возможности входа в систему Cisco IOS, показанные на рис. 1, позволяют обеспечить усиленную защиту за счет замедления таких атак, как словарные атаки и DoS-атаки. Включения профиля обнаружения позволяет сконфигурировать сетевое устройство так, чтобы оно отказывало в дальнейших запросах на подключение (или блокировало вход в систему) в случае повторных неудачных попыток входа.

Такую блокировку можно задать на некоторый период времени, который называется «период тишины». Списки контроля доступа (access control lists, ACL) могут использоваться для разрешения легитимных подключений с адресов известных системных администраторов.

По умолчанию баннеры отключены и должны включаться явным образом. Используйте команду **banner** в режиме глобальной конфигурации, как показано на рис. 2, чтобы задать соответствующие сообщения. Баннеры защищают организацию с юридической стороны. Важно правильно формулировать сообщения, которые будут отображаться на баннере, поэтому до размещения баннеров на сетевых маршрутизаторах рекомендуется проконсультироваться с юристами. Никогда не используйте слова «добро пожаловать» или любое другое известное приветствие, которое можно интерпретировать как приглашение к использованию сети.



Второй учебный вопрос.
Защита сети с использованием паролей


```
R1(config)#
login block-for seconds attempts tries within seconds

R1(config)#
login quiet-mode access-class {acl-name|acl-number}

R1(config)#
login delay seconds

R1(config)#
login on-success log [every login]

R1(config)#
login on-failure log [every login]
```

Конфигурирование расширенных функций входа в систему

Команды усовершенствованного входа в систему Cisco IOS, показанные на рис. 1, позволяют повысить безопасность виртуального входа.

```
R1(config)# login block-for 15 attempts 5 within 60
R1(config)# ip access-list standard PERMIT-ADMIN
R1(config-std-nacl)# remark Permit only Administrative hosts
R1(config-std-nacl)# permit 192.168.10.10
R1(config-std-nacl)# permit 192.168.11.10
R1(config-std-nacl)# exit
R1(config)# login quiet-mode access-class PERMIT-ADMIN
R1(config)# login delay 10
R1(config)# login on-success log
R1(config)# login on-failure log
R1(config)#
```

На рис. 2 показан пример конфигурации. Команда **login block-for** может обеспечивать защиту от DoS-атак за счет отключения входа в систему в случае повторных неудачных попыток входа (количество неудачных попыток задается предварительно). Команда **login quiet-mode** выполняет сопоставление со списком ACL, в котором указаны разрешенные хосты. Таким образом гарантируется, что попытки входа на маршрутизатор могут идти только со стороны авторизованных хостов. Команда **login delay** определяет, сколько секунд пользователь должен подождать до новой попытки после неудачной попытки входа. Команды **login on-success** и **login on-failure** фиксируют удачные и неудачные попытки входа.

Такие возможности усовершенствованного входа не применяются для консольных подключений. Для таких подключений подразумевается, что только авторизованный персонал имеет физический доступ к устройствам.

Такие функции усовершенствованного входа могут быть включены только в том случае, если для аутентификации для локального и удаленного доступа используется локальная база данных. Если же линии сконфигурированы для аутентификации только по паролю, функции усовершенствованного входа включить нельзя.

Второй учебный вопрос.
Защита сети с использованием паролей

router(config)#

```
login block-for seconds attempts tries within seconds
```

```
R1(config)# login block-for 120 attempts 5 within 60
```

- Эту команду следует ввести до использования любых других команд входа в систему.
- Эта команда может помочь обеспечивать обнаружение DoS-атак и их предотвращение.

Включение расширенных функций входа в систему

Чтобы устройство Cisco IOS смогло обнаружить DoS-атаку, воспользуйтесь командой **login block-for**. Все остальные функции усовершенствованного входа отключены до тех пор, пока не будет сконфигурирована команда **login block-for** . На рисунке показан синтаксис команды и пример конфигурации команды **login block-for** .

В частности, команда **login block-for** выполняет мониторинг входа на устройство и работает в двух режимах:

- **Обычный режим.** Также называется режимом наблюдения. Маршрутизатор считает число неудачных попыток входа за указанный период времени.
- **Режим тишины.** Также называется периодом «тишины». Если число неудачных попыток входа превышает заданное пороговое значение, все попытки входа с использованием протоколов Telnet, SSH и HTTP блокируются на время, указанное для команды login block-for.

В этом примере показана конфигурация, которая вызывает список ACL с именем PERMIT-ADMIN. Хосты, соответствующие операторам PERMIT-ADMIN, выводятся из режима «тишины».

```
R1(config)# ip access-list standard PERMIT-ADMIN
R1(config-std-nacl)# remark Permit only Administrative hosts
R1(config-std-nacl)# permit 192.168.10.10
R1(config-std-nacl)# permit 192.168.11.10
R1(config-std-nacl)# exit
R1(config)# login quiet-mode access-class PERMIT-ADMIN
```

- Команда указывает, что ACL применяется к маршрутизатору при переключении в режим «тишины», и идентифицирует хосты, для которых разрешен доступ во время режима «тишины».
- Если это не сконфигурировано, все запросы входа в систему во время режима «тишины» будут отклоняться.

Когда режим «тишины» включен, все попытки входа, включая действующий административный доступ, запрещены. Однако, чтобы обеспечить постоянный доступ (например, административный доступ к определенным хостам) к критически важным хостам, такое поведение можно изменить с помощью списка ACL. Список ACL создается и определяется с использованием команды **login quiet-mode access-class,** как показано на рисунке. Во время режима «тишины» доступ к устройству будут иметь только хосты, указанные в списке ACL.

Второй учебный вопрос.
Защита сети с использованием паролей

При использовании команды **login block-for** между попытками входа автоматически устанавливается задержка в одну секунду. Чтобы осложнить жизнь злоумышленнику, время задержки между попытками входа можно увеличить с помощью команды **login delay,** как показано на рисунке ниже. Эта команда позволяет задать одинаковую задержку между последовательными попытками входа. Задержка устанавливается для всех попыток входа, как удачных, так и неудачных.

В данном примере устанавливается задержка в 3 секунды между последовательными попытками входа в систему.

```
R1(config)# login delay 3
```

- Это позволяет нейтрализовать словарные атаки.
- Это необязательная команда. Если значение задержки не задано, то после конфигурирования команды **login block-for** принудительно устанавливается задержка по умолчанию, равная одной секунде.

Команды **login block-for**, **login quiet-mode access-class,** и **login delay** позволяют блокировать неудачные попытки входа на ограниченный период времени. Однако они не могут помешать злоумышленнику снова пытаться войти в систему. Как же администратору узнать, что кто-то пытается проникнуть в сеть, пытаясь подобрать пароль?

Второй учебный вопрос.
Защита сети с использованием паролей

Неудачные попытки входа

Как показано на рисунке, существует три команды, которые можно сконфигурировать, чтобы помочь администратору обнаружить атаку с подбором пароля. Каждая команда позволяет устройству генерировать syslog-сообщения для удачных или неудачных попыток входа.

Первые две команды, **login on-success log** и **login on-failure log,** генерируют syslog-сообщения для удачных и неудачных попыток входа.

```
R1(config)# login on-success log [every login]
R1(config)# login on-failure log [every login]
R1(config)# security authentication failure rate threshold-rate log
```

Число попыток входа до того, как будет сгенерировано сообщение о входе, можно указать с использованием синтаксиса [**every login**], где значение по умолчанию = 1 попытка. Допустимый диапазон от 1 до 65535. В качестве альтернативного варианта команде **login on-failure log** можно сконфигурировать команду **security authentication failure rate,** чтобы создавать сообщение о входе в случае превышения частоты неудачных попыток входа.

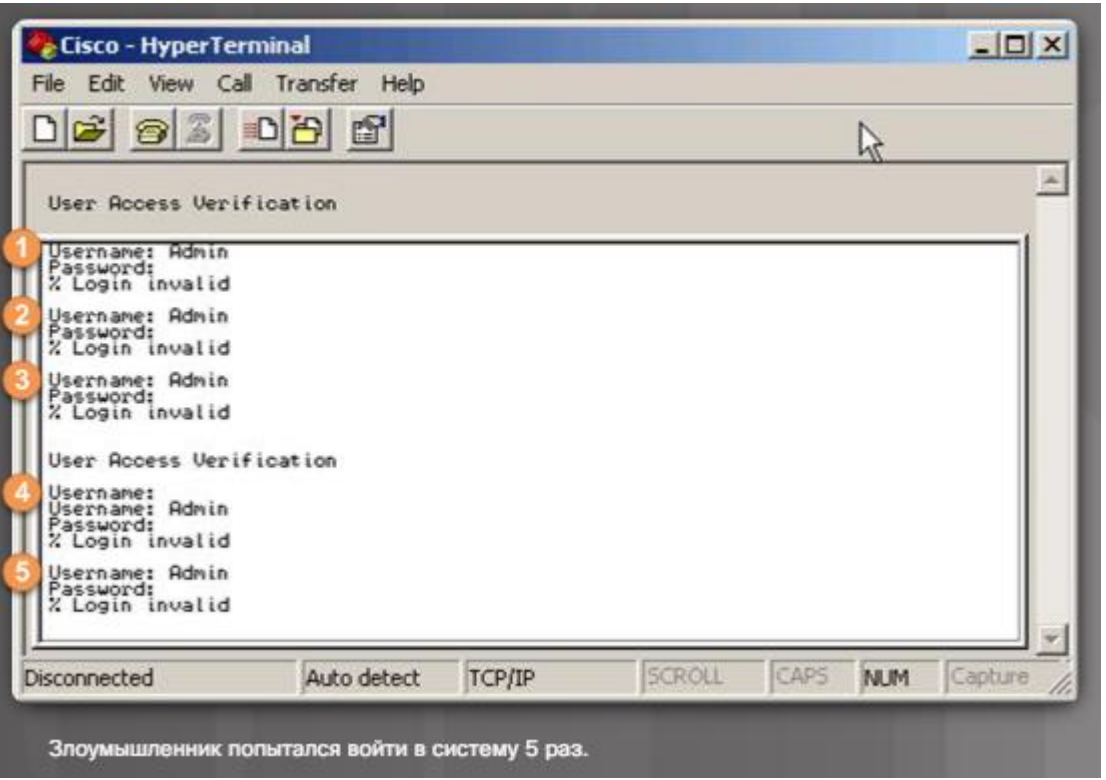
```
R1# show login
    A login delay for 10 sec is applied.
    Quiet-Mode access list PERMIT-ADMIN is applied.

    Router enabled to watch for login Attacks.
    If more than 5 login failures occur in 60 sec or less,
    login will be disabled for 120 secs.

    Router presently in Normal-Mode.
    Current Watch Window
        Time remaining: 5 seconds.
        Login failures for current window: 4.
    Total login failures:4.
```

Используйте команду **show login,** чтобы проверить параметры команды **login block-for** и текущий режим.

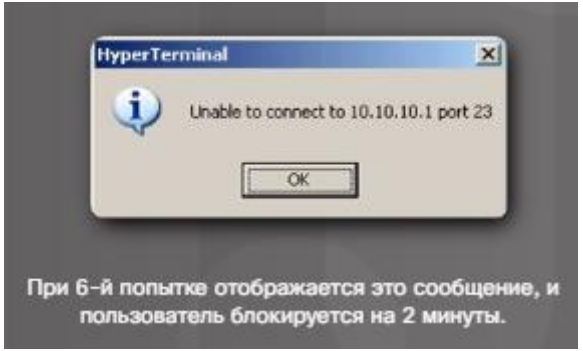
На рисунке маршрутизатор R1 был сконфигурирован таким образом, чтобы блокировать хосты входа на 120 секунд в случае, если в течение 60 секунд произошло более пяти неудачных попыток входа. Маршрутизатор R1 также подтверждает, что текущий режим является обычным (normal) и что за прошедшие 55 секунд произошло четыре неудачных попытки входа, так как в обычном режиме еще остается 5 секунд.

Второй учебный вопрос.
Защита сети с использованием паролей

На следующих рисунках показано, что происходит в случае превышения порогового значения неудачных попыток.



Злоумышленник попытался войти в систему 5 раз.



При 6-й попытке отображается это сообщение, и пользователь блокируется на 2 минуты.

Второй учебный вопрос.
Защита сети с использованием паролей


```
R1#
*Dec 10 15:38:54.455: %SEC_LOGIN-1-QUIET_MODE_ON: Still timeleft for watching failures
is 12 secs, [user: admin] [Source: 10.10.10.10] [localport: 23] [Reason: Login
Authentication Failed - BadUser] [ACL: PERMIT-ADMIN] at 15:38:54 UTC Wed Dec 10 2008

R1# show login
     A login delay of 3 seconds is applied.
     Quiet-Mode access list PERMIT-ADMIN is applied.

     Router enabled to watch for login Attacks.
     If more than 5 login failures occur in 60 seconds or
     less,logins will be disabled for 120 seconds.

     Router presently in Quiet-Mode.
     Will remain in Quiet-Mode for  105 seconds.
     Restricted logins filtered by applied ACL PERMIT-ADMIN.

R1#
```

На рисунке показан итоговый статус с использованием команды **show login**. Обращаем внимание, что теперь маршрутизатор находится в режиме «тишины» и будет оставаться в нем еще 105 секунд. R1 также определяет, что ACL-список PERMIT-ADMIN содержит список хостов, к которым можно подключаться во время режима «тишины».

Команда **show login failures** отображает дополнительную информацию о неудачных попытках, например IP-адрес, с которого происходили неудачные попытки входа.

На следующем рисунке показан пример результата команды **show login failures** .

```
R1# show login failures
Total failed logins: 22
Detailed information about last 50 failures

Username    SourceIPAddr    lPort Count TimeStamp
admin       1.1.2.1         23    5     15:38:54 UTC Wed Dec 10 2008
Admin       10.10.10.10     23    13    15:58:43 UTC Wed Dec 10 2008
admin       10.10.10.10     23    3     15:57:14 UTC Wed Dec 10 2008
cisco       10.10.10.10     23    1     15:57:21 UTC Wed Dec 10 2008

R1#
```

Второй учебный вопрос.
Защита сети с использованием паролей


```
R1(config)# logging 192.168.1.3
R1(config)# logging trap 4
R1(config)# logging source-interface g0/0
R1(config)# interface loopback 0
R1(config-if)#
*Jun 12 22:06:02.902: %LINK-3-UPDOWN: Interface Loopback0, changed state to up
*Jun 12 22:06:03.902: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up
*Jun 12 22:06:03.902: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.3
port 514 started - CLI initiated
R1(config-if)# shutdown
R1(config-if)#
*Jun 12 22:06:49.642: %LINK-5-CHANGED: Interface Loopback0, changed state to
administratively down
*Jun 12 22:06:50.642: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to down
R1(config-if)# no shutdown
R1(config-if)#
*Jun 12 22:09:18.210: %LINK-3-UPDOWN: Interface Loopback0, changed state to up
*Jun 12 22:09:19.210: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up
R1(config-if)#
```

Команды маршрутизатора и коммутатора для клиентов syslog

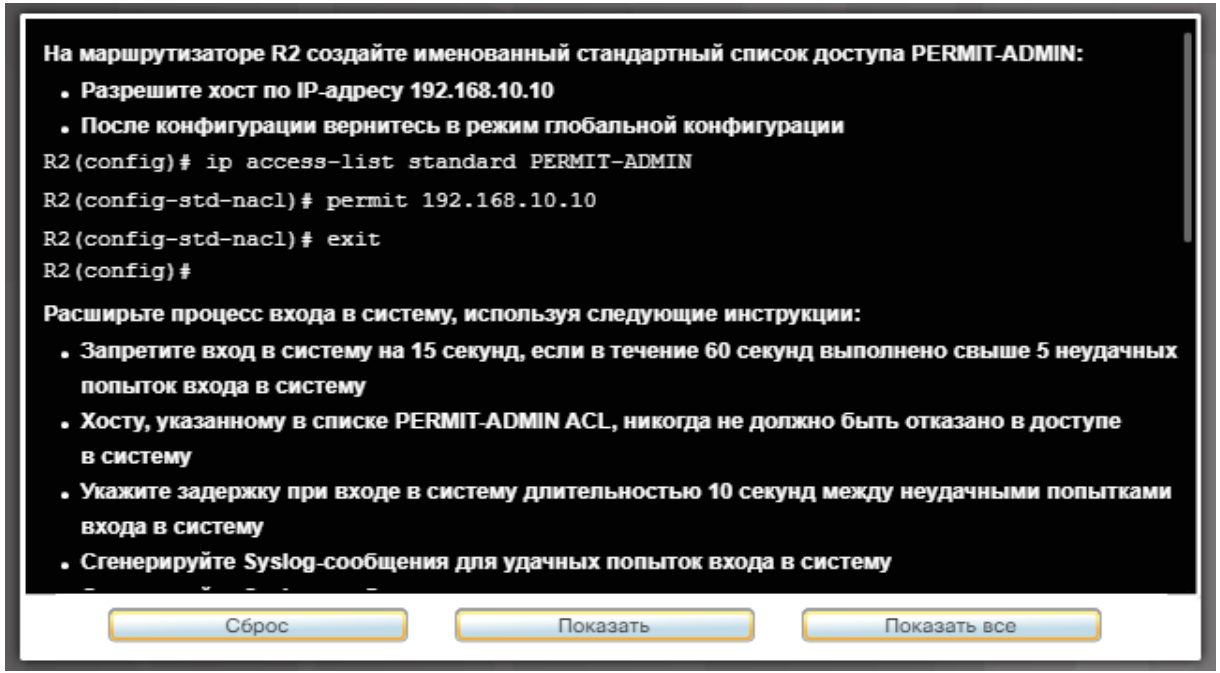
Настройка маршрутизатора для отправки системных сообщений на сервер syslog, где они могут храниться, фильтроваться и анализироваться, выполняется в три шага:

Шаг 1. В режиме глобальной настройки используйте команду **logging** для настройки имени хоста адресата или IPv4-адреса системного журнала.

Шаг 2. Укажите, какие сообщения следует отправлять на сервер системного журнала с помощью команды режима глобальной настройки уровня **logging trap**. Например, чтобы отправлять только сообщения уровня 4 и ниже (0—4), используйте одну из следующих двух эквивалентных команд.

Шаг 3. При необходимости настройте интерфейс источника, используя команду режима глобальной настройки **logging source-interface** *тип_интерфейса номер_интерфейса*. Таким образом, можно настроить, чтобы пакеты syslog содержали адрес IPv4 или IPv6 конкретного интерфейса независимо от того, какой интерфейс используется для отправки пакета с маршрутизатора.

Выводы по второму вопросу



Третий учебный вопрос.
Защита сети по протоколу SSH

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

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)

R1(config)#
*Feb 16 21:18:41.977: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)# ip ssh version 2
R1(config)# username Bob algorithm-type scrypt secret cisco54321
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# end
R1#
```

Шаги для настройки SSH

Прежде чем сконфигурировать SSH, маршрутизатор должен обеспечить соответствие четырем требованиям:

- Запустить версию Cisco IOS, поддерживающую SSH.
- Использовать уникальное имя хоста.
- Использовать правильное имя домена сети.
- Поддерживать конфигурацию для локальной аутентификации или сервисов AAA.

На рисунке приведен пример пяти шагов, необходимых для конфигурирования маршрутизатора Cisco для поддержки SSH с локальной аутентификацией:

Шаг 1. Сконфигурируйте имя IP-домена сети, используя команду **ip domain-name** *domain-name* в режиме глобальной конфигурации.

Шаг 2. Необходимо сгенерировать односторонние секретные ключи, чтобы маршрутизатор смог зашифровать SSH-трафик. Эти ключи называются ассиметричными ключами. Для генерации ключей ПО Cisco IOS использует алгоритм Rivest, Shamir, and Adleman (RSA). Чтобы создать RSA-ключ, используйте команду **crypto key generate rsa general-keys modulus** *modulus-size* в режиме глобальной конфигурации. Числовая характеристика определяет размер RSA-ключа и может быть настроена в диапазоне от 360 до 4096 бит. Чем больше эта характеристика, тем надежнее RSA-ключ. Однако ключи с большими числовыми значениями дольше генерировать, шифровать и расшифровывать. Минимальная рекомендуемая длина ключа 1024 бита. После того как RSA-ключи сгенерированы, SSH включается автоматически.

Шаг 3. На маршрутизаторах Cisco по умолчанию используется протокол SSH версии 2, версию 2 можно настроить вручную с помощью команды **ip ssh version 2** режима глобальной конфигурации.

Шаг 4. Проверьте, что имеется действительная запись имени пользователя локальной базы данных. Если ее нет, создайте ее с помощью команды **username** *name* **algorithm-type scrypt secret** *secret* .

Шаг 5. Активируйте входящие сеансы vty SSH с помощью команд vty-линии, **login local** и **transport input ssh**.

Третий учебный вопрос.
Защита сети по протоколу SSH


```
R1# show crypto key mypubkey rsa
% Key pair was generated at: 21:18:41 UTC Feb 16 2015
Key name: R1.span.com
Key type: RSA KEYS
 Storage Device: not specified
 Usage: General Purpose Key
 Key is not exportable.
 Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00CF35DB
  A58A1BD8 F7C7E600 F189C2F3 2EC6E584 D923EE5B 71841D98 B5472A03 D19CD620
  ED125825 5A58412B B7F29234 DE2A1809 6C421AC3 07F298E6 80BE149D 2A262E13
  74888DAF CAC8F187 B11111AF A413E76F 6C157CDF DFEF0D82 2961B58C BE1CAD21
  176E82B9 6D81F893 06E66C93 94E1C508 887462F6 90AC63CE 5E169845 C1020301 0001
% Key pair was generated at: 21:18:42 UTC Feb 16 2015
Key name: R1.span.com.server
Key type: RSA KEYS
Temporary key
 Usage: Encryption Key
 Key is not exportable.
 Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00AB914D 8172DFBE
  DE57ACA9 7B844239 1F3B5942 3943AC0D F54E7746 3895CF54 606C3961 8A44FEB3
  1A019F27 D9E71AAE FC73F423 A59CB8F5 50289272 3392CEBC 4C3CBD6D DB9233DE
  9DDD9DAD 79D56165 4293AA62 FD1CBAB2 7AB859DC 2890C795 ED020301 0001
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# crypto key zeroize rsa
% All keys will be removed.
% All router certs issued using these keys will also be removed.
Do you really want to remove these keys? [yes/no]: yes
```

Для проверки SSH и отображения сгенерированных ключей используйте команду **show crypto key mypubkey rsa** в привилегированном режиме. Если пары ключей уже есть, рекомендуется перезаписать их с помощью команды **crypto key zeroize rsa**. Если пары ключей уже есть, рекомендуется удалить их с помощью команды **crypto key zeroize rsa** .

На рисунке показан пример проверки шифроключей SSH и удаления старых ключей.

Третий учебный вопрос.
Защита сети по протоколу SSH


```
R1# show ip ssh
SSH Enabled - version 2.0
Authentication methods:publickey,keyboard-interactive,password
Authentication timeout: 120 secs; Authentication retries: 3
<output omitted>

R1# conf t
Enter configuration commands, one per line
R1(config)# ip ssh time-out 60
R1(config)# ip ssh authentication-retries
R1(config)# ^Z
R1#
*Feb 16 21:23:51.237: %SYS-5-CONFIG_I: Con
R1# show ip ssh
SSH Enabled - version 2.0
Authentication methods:publickey,keyboard-
Authentication timeout: 60 secs; Authentic
<output omitted>
```

Изменение настроек SSH

Для проверки дополнительных параметров команды SSH используйте команду **show ip ssh,** как показано на рисунке.

Можно также изменить период ожидания SSH и количество …манду **ip ssh time-**…ации, чтобы изменить …екундам. Таким образом …ротокол SSH должен …тификации запускается …ртный период ожидания

… попытки, чтобы ввести Чтобы настроить другое …ользуйте команду **ip ssh** …ной конфигурации.

Воспользуйтесь … …ре R2.

```
R2(config)# ip ssh version 2
R2(config)# ip ssh authentication-retries 2
R2(config)# ip ssh time-out 60
R2(config)# end
R2#
```

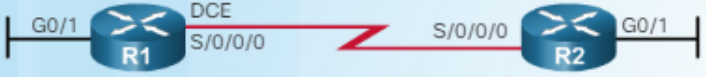
Проверьте конфигурацию SSH с помощью команды show ip ssh.

```
R2# show ip ssh
SH Enabled - version 2.0
Authentication methods:publickey,keyboard-interactive,password
Authentication timeout: 60 secs; Authentication retries: 2
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQDNJV02ayJzPD/Ys/HKpy78XVR+QlnBaHaABMEOKG1j
oC4DQf8Z2XRJTzORPrYUfk1FFFVku+ejsy0G+3LoCAUgSdfpg1X4c8DbJhvA1PwPgxPVPklS5yWS+URk
ur4ijJl/cPksQpXQ8i26ye5SlLslV+3I+3TSI3MOEmJP++3vvw==
R2#
```

Вы успешно настроили SSH на маршрутизаторе R2.

Сброс | Показать | Показать все

Третий учебный вопрос. Защита сети по протоколу SSH




```
R1# show ssh
Connection Version Mode Encryption  Hmac       State             Username
0          2.0     IN   aes128-cbc  hmac-sha1  Session started   Bob
0          2.0     OUT  aes128-cbc  hmac-sha1  Session started   Bob
%No SSHv1 server connections running.
R1#
```

Во входящем и исходящем сеансах SSHv2 имеется пользователь под именем Bob.

```
R2# ssh -l Bob 192.168.2.101

Password:

R1>
```

Маршрутизатор R2 устанавливает SSH-соединение с маршрутизатором R1, предоставляет имя пользователя и пароль.

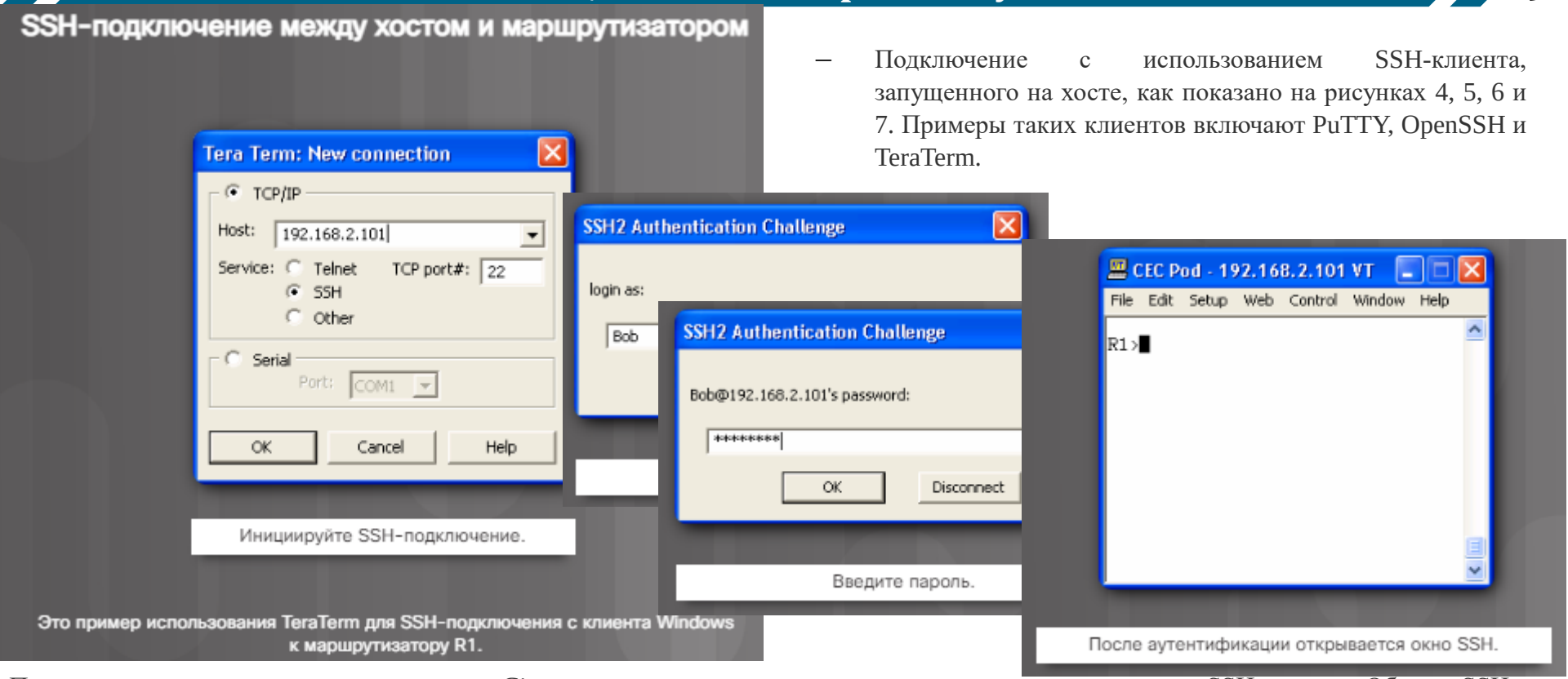
Подключение к маршрутизатору со включенным протоколом SSH

Чтобы проверить статус подключений клиента, используйте команду **show ssh**. Для подключения к маршрутизатору со включенным протоколом SSH существует два способа:

– По умолчанию, когда SSH включен, маршрутизатор Cisco может работать как SSH-сервер или как SSH-клиент. Как сервер, маршрутизатор может принимать подключения SSH-клиента. Как клиент, маршрутизатор может подключаться по протоколу SSH к другому маршрутизатору со включенным протоколом SSH (см. рисунки 1, 2 и 3).

Третий учебный вопрос.
Защита сети по протоколу SSH

– Подключение с использованием SSH-клиента, запущенного на хосте, как показано на рисунках 4, 5, 6 и 7. Примеры таких клиентов включают PuTTY, OpenSSH и TeraTerm.



Процедура подключения к маршрутизатору Cisco отличается в зависимости от используемого приложения SSH-клиента. Обычно SSH-клиент инициирует SSH-подключение к маршрутизатору. SSH-сервис маршрутизатора запрашивает действительную комбинацию имени пользователя и пароля. После того как вход подтвержден, маршрутизатором можно управлять так же, как если бы администратор использовал стандартный сеанс Telnet.

Учебные вопросы и цели занятия:

1. Защита сетевой инфраструктуры.
2. Защита сети с использованием паролей.
3. Защита сети по протоколу SSH.

Заключение

Защиту сети необходимо начинать с защиты ее устройств. Под этим понимается защита периметра сети, обеспечение безопасности административного доступа к инфраструктурным устройствам, повышение безопасности виртуального входа в систему и использование защищенных протоколов вместо незащищенных. Например, использование SSH вместо Telnet или HTTPS вместо HTTP.

Также важно ограничивать административный доступ. Администраторы должны предоставлять доступ к инфраструктурным устройствам в зависимости от уровней привилегий и внедрять интерфейс CLI на основе ролей для обеспечения иерархического административного доступа.

Образы IOS и файлы конфигурации должны быть защищены с использованием функции устойчивой конфигурации Cisco IOS. С данным направлением мы с вами познакомимся на следующем занятии.