*Реферат*

*Тема: защита маршрутизатора средствами CISCO IOS*

### Содержание.

### Введение 3

### Программное обеспечение маршрутизаторов Cisco 4

### Основные интерфейсы 6

### Консольные интерфейсы 7

### Решения Cisco Systems для обеспечения сетевой безопасности 8

### Пользовательский и привилегированный уровни доступа 10

### Парольная защита 12

### Ограничение доступа к маршрутизатору 15

### Заключение 16

### Список использованных источников 17

### Введение.

### Компания Cisco Systems является абсолютным лидером на рынке маршрутизаторов (занимает около 70% рынка; на втором месте Juniper c 21%). Cisco предлагает модели от простейших маршрутизаторов для малого офиса (серия 800) до мультигигабитных устройств, размещаемых в ядре Интернета (серия 12000).

### Кроме маршрутизаторов Cisco известна коммутаторами ЛВС марки Catalyst, межсетевыми экранами марки PIX, продуктами для IP-телефонии, продуктами марки Aironet для организации беспроводных сетей и др. С учетом всей номенклатуры выпускаемой продукции Cisco Systems является лидером мирового рынка оборудования связи (14%; на втором месте Siemens с 11,7%).

### Все модели, кроме серии 800, обладают той или иной степенью модульности, то есть, позволяют устанавливать сменные интерфейсные модули и специализированные вычислительные модули (для шифрования или обработки голоса). Соответственно, цена устройства сильно зависит от комплектации. Широко распространены также устройства серий 2500 и 4000, но в настоящее время они сняты с производства (за исключением моделей 2509 и 2511). На смену 2500 пришли маршрутизаторы серий 1700 и 2600, а на смену 4000 - 3600.

### Программное обеспечение маршрутизаторов Cisco.

### Все маршрутизаторы Cisco работают под управлением операционной системы Cisco IOS. Для каждой модели маршрутизатора предлагаются несколько разновидностей IOS.

### Образы IOS различаются по версии. Cisco использует достаточно сложную систему идентификации версий, ознакомиться с которой можно по этой ссылке.

### Для студентов достаточно будет следующего понимания: номер версии Cisco IOS состоит из трех частей:

### Номер основного релиза (major release; в настоящее время обычно встречаются основные релизы 11.3, 12.0, 12.1, 12.2).

### Номер обновления (maintenance release), начиная с 1. Обновления выпускаются каждые 8 недель, в них включаются исправления ошибок. Набор функциональных возможностей релиза не изменяется.

### Номер выпуска (software rebuild), обозначается буквой, начиная с а. Выпуски предназначены для экстренного исправления ошибок, которое не может ждать до следующего обновления.

### Таким образом, IOS 12.2(6с) - это основной релиз 12.2, обновление 6, выпуск c.

### Каждая версия характеризуется степенью зрелости, как правило это LD (Limited Deployment) или GD (General Deployment). LD подразумевает меньший объем тестирования и опыта эксплуатации по сравнению с GD.

### Кроме основного ряда IOS существует экспериментальный ряд, так называемый T-train (или, официально, Technology Releases). Именно в T-train включаются новые возможности и проходят "обкатку" до того, как будут введены в основной ряд. Нумерация версий ряда Т строится аналогично основному ряду (только выпуски нумеруются цифрами):

### IOS 12.1(6)T2 - этот T-train базируется на основном релизе 12.1. Это второй выпуск шестого обновления указанного T-train.

### Со временем из T-train получается следующий основной релиз (так например, 12.0(6)Т переходит в 12.1, и в тот же момент образуется ряд 12.1Т для добавления новых возможностей). Зрелость T-train характеризуется как ED (Early Deployment), что означает, что программное обеспечение не рекомендуется применять на ответственных участках, если аналогичную функциональность можно найти в версиях LD или GD.

### Не всякая версия может быть установлена на конкретный маршрутизатор в конретной конфигурации; предварительно следует проконсультироваться у специалиста компании-реселлера.

### Кроме версий, образы IOS различаются по заложенной в них функциональности. Функциональные возможности группируются в наборы, называемые feature sets. Минимальная функциональность содержится в IP only feature set (или просто "IP"); она включает в себя, в частности, поддержку IP-интерфейсов, статическую и динамическую IP-маршрутизацию, поддержку мониторинга и управления по SNMP. IP Plus feature set включает дополнительные возможности (например, поддержку технологии VoIP для передачи голоса). Также имеются feature sets с функциями межсетевого экрана (FW, Firewall), системы обнаружения атак (IDS), криптозащиты трафика (IPSEC) и др., в том числе имеются и комбинированные образы, например IP Plus FW IPSEC. Бесплатно с маршрутизатором поставляется только IP only feature set, остальные образы необходимо покупать. Для определения того, в каком feature set имеется требуемая вам возможность, следует обратиться к специалисту компании-реселлера.

### Таким образом, конкретный образ IOS идентифицируется тремя параметрами:

### аппаратная платформа, для которой он предназначен,

### feature set,

### версия.

### Пример имени файла с образом IOS: c3620-is-mz.122-13a.bin. Это IOS IP Plus 12.2(13a) для Cisco 3620. Feature set (IP Plus) идентифицируется символами "is", следующими за обозначением платформы. Другие примеры feature sets: "i" - IP, "js" - Enterprise Plus, "io" - IP FW. Подобная кодировка справедлива для серий 2600, 3600; для других платформ коды feature set могут отличаться.

### Буквы "mz" означают, что IOS при запуске загружается в оперативную память (m) и что в файле образ хранится в сжатом виде (z).

### 

### Основные интерфейсы.

### В каждом маршрутизаторе имеется некоторое число физических интерфейсов. Наиболее распространенными типами интерфейсов являются: Ethernet/FastEthernet и последовательные интерфейсы (Serial). Последовательные интерфейсы по своему аппаратному исполнению бывают синхронные, синхронно-асинхронные (режим выбирается командой конфигурации) и асинхронные (Async). Протоколы физического уровня последовательных интерфейсов: V.35 (чаще всего используется на синхронных линиях), RS-232 (чаще всего используется на асинхронных линиях) и другие.

### Каждому интерфейсу соответствует разъем на корпусе маршрутизатора. Интерфейсы Ethernet на витой паре обычно имеют разъем RJ-45, но на некоторых моделях (серия 2500) встречаются разъемы AUI (DB-15), которые требуют подключения внешнего трансивера, реализующего тот или иной интерфейс физического уровня Ethernet.

### Последовательные интерфейсы чаще всего снабжаются фирменными разъемами DB-60 F или SmartSerial F (последний более компактен). Для того, чтобы подключить интерфейс к внешнему оборудованию, необходимо использовать фирменный кабель - свой для каждого протокола физического уровня. Фирменный кабель имеет с одной стороны разъем DB-60 M, а с другой стороны - разъем выбранного стандарта физического уровня для устройства DTE или DCE. Таким образом, кабель выполняет следующие задачи:

### путем замыкания специальных контактов в разъеме DB-60 сигнализирует маршрутизатору, какой выбран протокол физического уровня, и каким типом устройства является маршрутизатор: DTE или DCE;

### является переходником с универсального разъема DB-60 на стандартный разъем выбранного протокола физического уровня.

### Примечание. В терминологии Cisco кабель DTE подключается к устройству DCE, а кабель DCE - к устройству DTE; то есть тип кабеля указывает, какого вида устройством является сам маршрутизатор, а не тот прибор, с которым его соединяет кабель.

### Обычно кабели DTE используются для подключения к маршрутизатору модемов, а связка двух кабелей DTE-DCE используется для соединения двух маршрутизаторов напрямую (back-to-back), при этом, естественно, один из маршрутизаторов будет в роли DCE. На рисунке 2.2 приведен пример сипользования кабедей для соединения устройств через интерфейс V.35 (стандартный разъем M.34).

### Кроме универсальных последовательных интерфейсов, рассматривавшихся выше, существуют специализированные последовательные интерфейсы, реализованные вместе с каналообразующим оборудованием: контроллеры E1, модули ISDN BRI, модули DSL, встроенные аналоговые или ISDN-модемы. В этом случае последовательный интерфейс находится внутри маршрутизатора, "между" каналообразующим оборудованием и ядром маршрутизатора. Для подключения линий связи к вышеуказанному каналообразующему оборудованию обычно используется разъем RJ-45 (для подключения линий к аналоговым модемам - RJ-11).

### Консольные интерфейсы.

### Два специальных последовательных интерефейса - CON и AUX - предназначены для доступа с терминала администратора к маршрутизатору для настройки и управления. Интерфейс CON подключается напосредственно к COM-порту компьютера администратора. К интерфейсу AUX подключается модем, что дает возможность удаленного управления маршрутизатором путем дозвона на модем. Интерфейс AUX может быть использован и как обычный последовательный интерфейс, через который производится маршрутизация дейтаграмм, но обрабока пакетов на этом интерфейсе требует большой доли процессорного времени (каждый полученный *байт* вызывает прерывание), а скорость ограничена 115 кбит/с. Интерфейс CON используется только для терминального доступа к маршрутизатору, параметры COM-порта должны быть 9600-8-N-1.

### Обычно разъемы CON и AUX выполнены в формате RJ-45. Подключение к ним производится с помощью специального кабеля RJ45-RJ45, прилагаемого к маршрутизатору. Одним концом кабель включается в CON или AUX, а на другой надевается переходник. Для подключения порта CON к компьютеру на кабель надевается переходник, помеченный как "TERMINAL", а для подключения порта AUX к модему со стороны модема используется переходник "MODEM".

### Виртуальные интерфейсы.

### Наряду с физическими интерфейсами в маршрутизаторе могут быть организованы виртуальные интерфейсы: Loopback, Null, Dialer, Virtual-Template, Multilink, BVI и др.

### Loopback и Null вообще никак не связаны с физическими интерфейсами.

### Loopback - это интерфейс обратной связи, ему можно назначать IP-адрес и указывать некоторые другие параметры, используемые при настройках интерфейсов. Loopback имеет следующие свойства:

### интерфейс всегда активен (в отличие от физических интерфейсов, где, например, обрыв кабеля переводит интерфейс в отключенное состояние);

### как и в случае физических интерфейсов, пакеты, адресованные на этот интерфейс, считаются адресованными маршрутизатору, а воображаемая IP-сеть, к которой он "подсоединен" (согласно своим адресу и маске), считается непосредственно подсоединенной к маршрутизатору;

### пакеты, маршрутизированные через такой интерфейс (то есть, направленные к узлам воображаемой сети, к которой подсоединен Loopback), уничтожаются.

### Применения интерфейсов Loopback будут рассмотрены по ходу лабораторного практикума.

### Интерфейс Null не имеет IP-адреса и прочих настроек. Пакеты, маршрутизированные через интерфейс типа Null, уничтожаются. Null применяется при фильтрации дейтаграмм, а также для создания защитных маршрутов при суммировании маршрутов.

### Другие виртуальные интерфейсы фактически получают и отправляют данные через физические интерфейсы, однако в данном случае IP-интерфейс больше не ассоциируется непосредственно с физическим портом маршрутизатора. Порт (порты), находящиеся "под" виртуальным интерфейсом, функционируют теперь только на уровнях 1 и 2 и им не присваиваются IP-адреса.

### Решения Cisco Systems для обеспечения сетевой безопасности.

### Компания Cisco Systems, являясь одним из ведущих производителей сетевого оборудования, предлагает полный спектр решений для обеспечения сетевой безопасности. Ниже приведен краткий перечень новых продуктов и решений, предлагаемых в данной области.

### **Для обеспечения защиты сетевых соеднений:** Network based IPSec VPN solution for Service Providers, VPN AIM Module for Cisco 2600XM, VAM2 Card for 7200s, VPN SM for Cat6500/7600, VPN 3000 Concentrator v4.0, AES Module for VPN 3000, VPN Client v.4.0. **Для управления системой безопасности:** Cisco IOS AutoSecure, Cisco Security Device Manager v1.0 , Cisco ISC v3.0, CiscoWorks VMS v2.2, CiscoWorks Security Information Management Solution (SIMS) v3.1. **Для обнаружения и предотвращения сетевых атак и вторжений:** IDS 4215 Sensor, IDS Network Module for Cisco 2600XM, 3660, 3700 series, Cisco Security Agents v4.0, Cisco CSS 11501S and WebNS v7.2 SSL s/w ,Cisco ACNS Software version 5.0.3 with Websense Content Filtering On-Box. **Для достоверной идентификации сторон, участвующих в защищенном обмене информацией**: Cisco IOS software Identity Enhancements.

### **Network based IPSec VPN solution for Service Providers** позволяет поставщикам услуг доступа управлять распределенными сетями на базе MPLS-VPN, IP-VPN и FR/ATM-VPN при помощи одного интегрированного пакета управления.

### **VPN AIM Module for Cisco 2600XM (AIM-VPN/BPII)** предоставляет маршрутизатору функции аппаратной шифрации с поддержкой алгоритмов DES, 3DES и AES и обеспечивает в два раза более высокую производительность по сравнению с предыдущим модулем ускорения шифрации (AIM-VPN/BP) - до 22 Мбит/сек.

### **VAM2 Card for Cisco 7200** - модуль аппаратного ускорения шифрации для маршрутизаторов серии Cisco 7200. Один модуль обеспечивает производительность шифрации до 260 Мбит/сек, два модуля - до 460 Мбит/сек.

### **VPN SM for Cat6500/7600** - сервисный модуль аппаратной шифрации для коммутаторов Catalyst 6500/7600. Обеспечивая производительность до 14 Гбит/сек он также поддерживает расширенную функциональность - поддержку и ускорение GRE-туннелей, полнофункциональне резервирование IPSec-соединений (stateful failover), IPSec Remote Access и возможность подключения WAN-интерфейсов.

### **VPN 3000 Concentrator v4.0** - новое ПО для концентратора VPN-соединений. Появились новые диагностические функции, поддержка авторизации пользователей через Kerberos/Active Directory, LAN-to-LAN backup для резервирования межсетевых соединений. Также появилась поддержка нового модуля шифрации AES - SEP-E, поддерживающего до 10000 одновременных соединений DES/3DES/AES.

### **VPN Client v.4.0** - новая версия ПО для клиентских рабочих станций, работающих через VPN. Интеграция с Cisco Security Agent предоставляет пользователю функции firewall, удобный и простой графический интерфейс облегчает настройку и управление, поддержка приложений, работающих с протоколом H.323 позволяет дистанционно общаться, не беспокоясь о защищенности соединения.

### **Cisco IOS AutoSecure** - функция интерфейса IOS, позволяющая быстро произвести настройку функций безопасности, отключить редко используемые сетевые сервисы и разрешить доступ и управление только для авторизованных пользователей.

### **Cisco Security Device Manager v1.0** - ПО управления сетевой безопасностью, доступное на всех моделях маршрутизаторов доступа, от Cisco 830 до Cisco 3700, позволяющее в графическом режиме, удаленно с любой раюбочей станции (через веб-браузер) изменять любые настройки безопасности на маршрутизаторе. Встроенный алгоритм аудита предупредит пользователя о потенциально опасных настройках и предложит варианты решения.

### **Cisco ISC v3.0** - Cisco IP Solution Center позволяет определять политики безопасности для всей сети, скрывая подробности реализации политик на конкретных устройствах. Политики позволяют учитывать схемы реализации механизмов LAN-to-LAN VPN, Remote Access VPN, EZ VPN и DMVPN, Firewall, NAT и QoS, а ISC реализует их на всех сетевых устройствах, работающих с механизмами безопасности (IOS, PIX, VPN3K Concentrator и т.п.).

### **CiscoWorks VPN/Security management Solution 2.2** централизует функции управления, мониторинга, учета, диагностики и обновления для ПО всех сетевых устройств Cisco, реализующих функции сетевой безопасности. CiscoWorks Security Information Management Solution (SIMS) v3.1 позволяет управлять безопасностью в сетях, использующих оборудование и ПО различных производителей.

### **IDS 4215 Sensor** - отдельное устройство в стоечном исполнении, высотой 1 RU, позволяет организовывать до 5 сенсоров с общей пропускной способностью до 80 Мбит/сек, которые способны прослушивать сетевой трафик, отслеживать потенциально опасную активность, предпринимать действия по предотвращению и остановке сетевых атак.

### **IDS Network Module for Cisco 2600XM, 3660, 3700 series** - аналогичное устройство, но предназначенное для слежения за трафиком на самом периметре сети - на маршрутизаторе доступа. Обеспечивая производительность до 45 Мбит/сек, модуль использует то же ПО, что и IDS sensor, что позволяет строить гомогенную инфраструктуру безопасности, с единым централизованным интерфейсом управления.

### **Cisco Security Agents v4.0** - "последняя линия" сетевой обороны, ПО, устанавливаемое на рабочие станции и серверы. Они отслеживают попытки несанкционированного доступа к операционной системе, а также следят за активностью приложений, в случае некорректных действий или нестабильной работы они могут остановить или перезапустить приложение или сервис. Оповещения о подозрительных событиях пересылаются и накапливаются на центральной консоли управления.

### **Cisco CSS 11500 Series Content Services Switch** - платформа управления трафиком на уровнях 4-7, позволяющая определять правила распределения трафика, его балансировки и резервирования.

### **Cisco ACNS Software version 5.0.3 with Websense Content Filtering On-Box** - версия 4 этого продукта работала как двухуровневая система, где модуль фильтрации размещался на устройствах Cisco Content Engine, а набор шаблонов WebSense для фильтрации - на внешнем сервере. Новая версия совмещает оба элемента на одной платформе (Content Engine).

### **Cisco IOS software Identity Enhancements** - новые функции IOS обеспечивают надежную идентификацию устройств и пользователей, участвующих в обмене информацией по защищенным каналам. Поддержка инфраструктуры PKI и интеграция с функциями AAA на серверах, маршрутизаторах и концентраторах доступа облегчают идентификацию в распределенной сети с использованием цифровых сертификатов и подписей. Secure RSA private key предотвращает использование украденных маршрутизаторов - в случае попытки вскрытия пароля приватные ключи маршрутизатора уничтожаются. N-tier CA Chaining позволяет отследить цепочку доверенных сертификатов, начиная с ближайшего и заканчивая центральным (root) certificate authority. Authentication Proxy проверяет права пользователя перед тем как выпустить пользователя за пределы сети. Secure ARP - связывает MAC и IP-адреса устройств, не позволяя подменить одно из устройств в процессе передачи данных. Поддержка 802.1X требует авторизации пользователя перед тем как пустить его трафик в сеть.

### 

### Пользовательский и привилегированный уровни доступа.

### Cisco IOS для конфигурации маршрутизатора поддерживает интерфейс командной строки, работать с которым можно с терминала, подключенного к маршрутизатору через консольный порт (Console port) или с помощью удаленного доступа по модему и telnet - соединения по сети. Сеанс командной строки называется EXEC-сессией.

### В целях безопасности Cisco IOS обеспечивает два уровня доступа к интерфейсу командной строки: пользовательский и привилегированный. Пользовательский уровень называется user EXEC режим, а привилегированный privileged EXEC режим. Предусмотрено 16 уровней привилегий: от 0 до 15. На нулевом уровне доступно всего пять команд: disable, enable, exit, help, logout. На уровне 15 доступны все возможные команды.

### Пользовательский режим

### Вид командной строки имеет вид Router> Этот режим позволяет временно изменить настройки терминала, выполнить основные тесты, просмотреть системную информацию и подключиться к удаленному устройству. Пользовательский режим по умолчанию имеет первый уровень привилегии. Набор команд существенно ограничен. Для перехода на другой уровень привилегий необходимо ввести команду enable [номер уровня], например

### Router>enable 7

### Команды enable и enable 15 являются аналогичными и приводят пользователя на привилегированный уровень.

### Привилегированный режим

### Вид командной строки в имеет вид Router# Набор привилегированных команд устанавливает параметры работы системы. Пользователь имеет доступ к командам глобального конфигурирования и специальным конфигурационным режимам.

### Возможности пользовательского режима с первым уровнем привилегий достаточно широкие. Из этого режима возможно выполнение "опасных" команд, таких как telnet, connect, tunnel, login и совсем не нужных для некоторых пользователей команд traceroute, enable, mstat, mrinfo, а также команд группы show: show hosts, show versions, show users, show flash: и многие другие.

### Права пользователей можно тонко настраивать: любому пользователю можно назначить определенный уровень при входе в маршрутизатор, любую команду можно перевести на уровень, отличный от стандартного. В свое время у нас возникла задача создания пользователя с минимальными возможностями: запрет команды enable, всех команд группы show и единственной разрешенной командой telnet. Это возможно реализовать следующим образом:

### 1. Создадим пользователя cook с нулевым уровнем привилегий

### Router(config)#username cook privilege 0 password 7 044D0908

### 2. Работать это будет только тогда, когда прописать следующее

### Router(config)#aaa new-model Router(config)#aaa authorization exec default local none

### После регистрации пользователь с именем cook по команде ? (список доступных команд) увидит перечень:

### Router>?

### Exec commands:

### <1-99> Session number to resume

### disable Turn off privileged commands

### enable Turn on privileged commands

### exit Exit from the EXEC

### help Description of the interactive help system

### logout Exit from the EXEC

### Router>

### Команду enable переведем на уровень выше (на уровень 1), а выполнение команды telnet разрешим для нулевого уровня

### Router(config)#privilege exec level 1 enable Router(config)#privilege exec level 0 telnet

### К данным командам действует некоторое исключение - их действие нельзя отменить при помощи стандартной команды no. Этот вариант здесь не проходит.

### Router(config)#no privilege exec level 1 enable Router(config)#no privilege exec level 0 telnet

### Для отмены действия этих команд необходимо ввести следующие команды:

### Router(config)#privilege exec reset enable Router(config)#privilege exec reset telnet

### Сейчас после регистрации пользователь cook по команде ? увидит следующее:

### Router>?

### Exec commands:

### <1-99> Session number to resume

### disable Turn off privileged commands

### exit Exit from the EXEC

### help Description of the interactive help system

### logout Exit from the EXEC

### telnet Open a telnet connection

### Router>

### Проделав все операции, получили пользователя с заранее заданными возможностями.

### Существует такой тип пользователей, для которых необходимо зарегистрироваться на маршрутизаторе и выполнить одну единственную команду (например, show users). Для этого можно завести на маршрутизаторе пользователя с входом без пароля и с выполнением автокоманды.

### Router(config)#username dream nopassword autocommand show users

### После ввода имени пользователя dream на экран выдается информация о присутствующих в данный момент на маршрутизаторе пользователях.

#### Парольная защита.

#### В соответствии с имеющимися пользовательским и привилегированным уровнями доступа существует два вида паролей: username password и enable secret (или enable password). Оба типа этих паролей могут иметь длину до 25 символов, содержать в себе различные знаки препинания и пробелы.

#### Пароль типа username password устанавливается с соответствующим ему именем пользователя. Задается это в режиме конфигурации следующей командой (пользователь cook с паролем queen):

#### Router(config)#username cook password queen

#### При выводе конфигурации (при помощи команды show running-config) на экране мы увидим следующую информацию:

#### username cook password 0 queen

#### Из этой строки видим, что пароль находится в "открытом виде", тип "0" означает "незашифрованный пароль". Если внимательно посмотреть самое начало конфигурации, то можно заметить следующую строку:

#### no service password-encryption

#### Это сервис шифрования видимой части пароля. По умолчанию он отключен. Правильным считается (для обеспечения безопасности - от простейшего подглядывания) включать этот сервис.

#### Router(config)#service password-encryption

#### Тогда строка конфигурации об имени и пароле пользователя будет иметь несколько другой вид, где мы уже не видим текст пароля в явном виде (тип "7" - зашифрованный пароль):

#### username cook password 7 03154E0E0301

#### Для входа в privileg EXEC level (привилегированный уровень) пользователь должен ввести пароль. При выключенном сервисе шифрования пароля соответствующая строка в конфигурации будет иметь вид:

#### enable password queen

#### При включенном же сервисе шифрования:

#### enable password 7 071E34494B07

#### Следует отметить, что данный метод шифрования пароля достаточно тривиален, существуют скрипты, которые за секунду декодируют его обратно в нормально читаемое состояние. Поэтому одним из важных элементов безопасности является вещь, с одной стороны очень далекая от телекоммуникаций и маршрутизаторов - порядок на собственном рабочем месте. Чтобы не были легко доступными бумажки с записями пароля в открытом виде, а также распечаток конфигураций роутеров, пусть даже пароль и будет зашифрован.

#### Лучшая возможность имеется для шифрования пароля к привилегированному уровню - использование не enable password, а enable secret, в котором для кодирования пароля применяется алгоритм MD5 (тип "5"):

#### Router(config)#enable secret queen

#### Строка конфигурации:

#### enable secret 5 $1$EuWt$SxHM5UPH3AIL8U9tq9a2E0

#### Преимущество такого шифрования пароля в том, что его кодирование производится даже при отключенном сервисе шифрования (забыли включить или не знали про такой сервис). Скриптов по расшифровке таких паролей я не встречал, но их существование вполне вероятно.

### Ограничение доступа к маршрутизатору.

### Управлять маршрутизаторами можно удаленно через telnet или локально через консольный порт или порт AUX. Отсюда следует два вида ограничения доступа к маршрутизатору: локальное и удаленное.

### Доступ к маршрутизатору для его конфигурирования и мониторинга может производиться 6 способами:

### с терминала, компьютера администратора (COM-порт), или терминального сервера через консольный порт маршрутизатора

### с терминала, компьютера администратора (COM-порт), или терминального сервера путем дозвона на модем, подсоединенный к порту AUX

### через Telnet

### посредством Unix-команды rsh

### по протоколу SNMP (community с правом записи - RW)

### через WWW-интерфейс (встроенный в маршрутизатор HTTP-сервер)

### Терминальным сервером называется хост, имеющий несколько последовательных асинхронных портов стандарта RS-232 (COM-порты), к которым подключаются консольные кабели маршрутизаторов. Поскольку обычный компьютер имеет 2 COM-порта, то для организации многопортового терминального сервера на базе ПК требуется установка карты расширения с дополнительными COM-портами (например, RocketPort). Из обрудования Cisco в качестве терминальных серверов обычно используются маршрутизаторы Cisco 2509 (8 асинхронных интерфейсов) и 2511 (16 асинхронных интерфейсов); при этом режим маршрутизации обычно отключается (no ip routing).

### В целях безопасности все способы доступа, кроме консольного, следует по возможности ограничить, а лучше - полностью отключить. По умолчанию rsh и SNMP отключены, а доступ по Telnet, наоборот, разрешен, причем без пароля. Статус HTTP-сервера зависит от версии IOS и модели оборудования.

### Консольный доступ уже сам по себе физически ограничен подключением консольного кабеля к терминальному серверу. Если администратор получает доступ к терминальному серверу удаленно, то встаёт задача защищенного доступа на терминальный сервер. Наиболее правильный способ организации удаленного доступа к терминальному серверу - протокол SSH.

### Локальное ограничение доступа к маршрутизатору

### Во-первых, необходимо специальное помещение с ограничением доступа для персонала, в котором бы находилось оборудование. Это рекомендуется для того, чтобы посторонний человек не имел физический доступ к маршрутизатору, т.к. при работе с маршрутизатором через консольный порт или порт AUX мы работаем в EXEC сессии без пароля на уровне обычного пользователя. И для получения доступа к привилегированному режиму посторонний человек может воспользоваться самым простым методом восстановление паролей - перезагрузка маршрутизатора, вход в режим ROM-монитора, изменение значения регистра конфигурации, снова перезагрузка маршрутизатора и элементарный вход в привилегированный режим без всякого пароля (вообще-то, это стандартный метод восстановления забытого пароля для доступа в privileg EXEC mode, но вот может использоваться и для совершенно противоположной цели).

### Если физический доступ к маршрутизатору не может быть достаточно ограничен, то необходимо установить пароль на работу в EXEC режиме по консольному порту и порту AUX. Вообще это лучше делать всегда, даже когда маршрутизатор находится в закрытом помещении под десятью замками (а вы уверены в своих коллегах?). Делается это достаточно просто и существует минимум два оптимальных варианта: совсем запретить вход в привилегированный режим или разрешить вход с нормальной авторизацией через пароль.

### Пример конфигурации, в которой для консольного порта разрешен вход через пароль с временем работы на порту в течении 1,5 минут, а для порта AUX запрещен вход EXEC режим:

### aaa new-model aaa authentication login default local

### line con 0   exec-timeout 1 30 line aux   no exec

### В этой конфигурации при подсоединении к консольному порту мы не сразу попадем в user EXEC режим как это происходит обычно, а только после ввода пользовательского имени и пароля. Хочу заметить, что в параметрах команды exec-timeout время задается в минутах и секундах (через пробел), но если мы захотим указать 0 минут и 0 секунд (exec-timeout 0 0), то это не означает, что совсем нельзя будет попасть на данный порт. А как раз наоборот - пользователь будет находиться в EXEC режиме бесконечно долго. Это нужно обязательно учитывать администраторам при конфигурации маршрутизатора. Самое минимальное время - 1 секунда (exec-timeout 0 1).

### Удаленное ограничение доступа к маршрутизатору

### Обычно рекомендуется совсем запрещать удаленный доступ к маршрутизатору по telnet или же жестко ограничивать его. Достичь этого можно благодаря применению списков доступа.

### 1. Полное запрещение доступа по telnet к маршрутизатору

### access-list 1 deny any

### line vty 0 4   access-class 1 in

### 2. Доступ к маршрутизатору по telnet разрешен только с определенного хоста (создадим расширенный список доступа и применим его к интерфейсу Ethernet 0/0)

### access-list 101 permit tcp host 140.11.12.73 host 140.11.12.236 eq telnet

### interface Ethernet0/0   ip address 140.11.12.236 255.255.255.0   ip access-group 101 in

### Необходимо заметить, что в списке доступа в структуре "от кого - кому" в качестве "кому" прописан IP адрес интерфейса Ethernet 0/0. А так же то, что при данной конфигурации через Ethernet 0/0 больше никто никуда не попадет, отсекаемый неявным оператором deny any. Поэтому нужно будет дополнить список доступа необходимыми "разрешениями".

#### Если необходимо конфигурировать маршрутизатор с удаленного хоста и терминальный сервер при маршрутизаторе отсутствует (например, одиночный маршрутизатор в удаленном филиале), то вместо Telnet следует использовать SSH. IPSEC Feature set операционной системы Cisco IOS поддерживает работу SSH-сервера непосредственно на маршрутизаторе. IPSEC Feature set имеет высокую стоимость, требует довольно зачительных ресурсов процессора и памяти и реализует относительно слабый алгоритм (DES с 40-битным ключом). Поддержка сильного алгоритма (Triple DES с 256-битным ключом) связана с преодолением экспортных ограничений США. Исходя из вышесказанного, организовывать административный доступ к маршрутизатору с помощью IPSEC Feature set следует только при невозможности подключения терминального сервера (или если IPSEC Feature set уже используется для организации VPN).

#### При доступе к маршрутизатору через WWW-интерфейс аутентификация пользователя HTTP-сервером проводится по ненадежной технологии. Отключение HTTP-сервера:

#### router(config)# no ip http server

#### Протокол SNMP (по крайней мере, версий 1 и 2) вообще не предоставляет адекватных средств обеспечения безопасности, поэтому разрешать запись через SNMP категорически не рекомендуется. Чтение следует разрешить только для административной станции - для этого надо сформировать соответствующий список доступа и указать его в команде активизации SNMP-агента:

#### router(config)#snmp-server community *public* RO *номер\_списка\_доступа*

### Заключение.

### Защита паролем, ограничение локального доступа, шифрованные пароли, расширенные списки доступа, учет и запись событий на маршрутизаторах обеспечивают защиту от несанкционированных попыток доступа и протоколируют информацию о таких попытках, всё это можно реализовать средствами CISCO IOS.

### Список использованных источников.

### http://cisco.com/

### http://www.mark-itt.ru/CISCO/ITO/

### http://telecom.opennet.ru/cisco/security.shtml#part\_3

### http://athena.vvsu.ru/net/labs/lab02\_cisco\_2.html#2.12