Улучшение безопасности на маршрутизаторах Cisco

***Интерактивный документ*. В данном документе содержится анализ конкретного устройства Cisco.**

Содержание

Введение

Этот документ представляет собой неформальное обсуждение некоторых настроек Cisco, изменение которых сетевые администраторы должны рассмотреть на своих маршрутизаторах, особенно на граничных маршрутизаторах, чтобы повысить безопасность. Данный документ содержит сведения о базовых, "шаблонных" элементах конфигурации, которые довольно широко используются в IP-сетях, а также о некоторых непредвиденных ситуациях, о которых также следует помнить.

Если выходные данные команды **show running-configuration** получены с устройства Cisco, то в этом случае для интерпретации результатов можно воспользоваться программой , которая помогает обнаружить потенциальные проблемы и найти способы их решения. Этой программой могут пользоваться только зарегистрированные пользователи, которые должны находиться в системе и у

которых должен быть включен JavaScript .

Служебная программа Output Interpreter отображает потенциальные проблемы, а также предлагает способы их решения. Данная программа доступна только для зарегистрированных пользователей, которые должны находиться в системе и у которых должен быть включен JavaScript.

Предварительные условия

Требования

Настоящий документ не содержит каких-либо специфических требований.

Используемые компоненты

Область применения настоящего документа не ограничивается какими-либо конкретными версиями аппаратного и программного обеспечения.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в разделе Технические советы Cisco. Условные обозначения.

Общие сведения

Настоящий документ не предоставляет исчерпывающей информации. Кроме того, ознакомление с данным документом не отменяет необходимости разбираться в вопросах сетевой безопасности. Настоящий документ служит своего рода памяткой по вопросам, которые иногда могут остаться незамеченными. В нем рассматриваются команды, которые являются важными для IP-сетей. Большая часть функций, включенных на маршрутизаторах Cisco, требуют тщательного подхода к настройке безопасности. В данном документе рассматриваются функции, включенные по умолчанию, а также функции, которые обычно включаются пользователями, и функции, которые может понадобиться отключить или повторно настроить.

Эти действия имеют особую важность, поскольку некоторые из стандартных настроек, используемых в программном обеспечении Cisco IOS®, являются результатом требований, оставшихся в прошлом. Выбор этих настроек был обоснован требованиями прошлого. Однако может потребоваться, чтобы стандартные настройки сообразовывались с требованиями сегодняшнего дня. Другие настройки по умолчанию остаются справедливыми для большинства систем, хотя при этом, если они применены для устройств, которые являются частью защиты по периметру сети, они могут создать угрозу безопасности. Некоторые настройки могут быть необходимы в силу требований, предъявляемых различными стандартами. Однако использование таких настроек не всегда желательно с точки зрения безопасности.

Программное обеспечение Cisco IOS предлагает множество специальных функций по обеспечению безопасности (например списки доступа фильтрации пакетов, набор функций брандмауэра Cisco IOS, TCP Intercept, AAA, шифрование). Другие функции, такие как учет пакетов и качество обслуживания (QoS), могут использоваться для усиления безопасности на случай различных сетевых атак. Однако в данном документе эти функции не рассматриваются подробно. Здесь также не обсуждается настройка брандмауэра. В целом этот документ посвящен обеспечению безопасности самого маршрутизатора и не затрагивает проблемы (не менее важные), которые связаны с защитой других устройств.

Управление паролями

Пароли и аналогичные средства обеспечения безопасности (например строка сообществ протокола SNMP) являются основными средствами защиты от неавторизованного доступа к вашему маршрутизатору). Лучший способ управления паролями — хранить их в TACACS+ или на сервере аутентификации RADIUS. Однако практически у каждого маршрутизатора по-прежнему останется локально настроенный пароль для привилегированного доступа, а также другие данные о пароле, хранящиеся в файле конфигурации.

enable secret

Команда **enable secret** используется для установки пароля, предоставляющего привилегированный административный доступ к системе IOS. Для команды enable secret всегда должен устанавливаться пароль. Используйте команду **enable secret** (но *не* старую команду **enable password**). Команда **enable password** использует слабый алгоритм шифрования. Более подробно см. раздел "Команда service password-encryption" данного документа.

Если задан параметр no enable secret и настроен пароль для консольной линии TTY, консольный пароль может использоваться для получения привилегированного доступа, даже с удаленного сеанса VTY. Можно почти с полной уверенностью сказать, что это не то, что требуется, и это будет еще один довод в пользу того, чтобы настроить функцию enable secret.

Команда service password-encryption и ее ограничения

Команда **service password-encryption** дает программному обеспечению IOS указание зашифровать пароли, секреты CHAP и другие, аналогичные данные, которые хранятся в файле конфигурации. Также необходимо следить за тем, чтобы рядом с системным администратором не находились посторонние лица, которые могут увидеть пароль, заглянув через плечо администратора.

При этом команда **service password-encryption** использует для шифрования алгоритм Виженера (Vigenere cipher). Любой опытный криптограф-любитель может с легкостью выполнить обратное преобразование, потратив несколько часов. Алгоритм не был предназначен для защиты файлов конфигурации от серьезного анализа даже более-менее опытными взломщиками, поэтому его не следует использовать для этих целей. К любому файлу конфигурации Cisco, содержащему зашифрованные пароли, следует относиться с такой же степенью осторожности, как и к незашифрованному списку этих паролей.

Предупреждение о слабости шифровального алгоритма не относится к паролям, установленным с помощью команды **enable secret**, но при этом оно остается справедливым для паролей, установленных с помощью команды **enable password**.

Для хэширования пароля команда **enable secret** использует алгоритм MD5. Алгоритм получил высокую общественную оценку и, по сведениям Cisco, для него невозможно выполнить обратное преобразование. Однако он может быть уязвим для "словарных" атак. Словарная атака – это процесс автоматической подстановки слов из словаря или списка возможных паролей. В связи с этим представляется целесообразным хранение файла конфигурации в надежном месте, особенно если надежность выбранных паролей вызывает сомнения.

Управление интерактивным доступом

Каждый, кто может зарегистрироваться на маршрутизаторе Cisco, может получить информацию, доступ к которой должен быть ограничен. Пользователь, который может подключиться к маршрутизатору, может использовать его в качестве промежуточного звена для организации дальнейших сетевых атак. Любой, кто может получить привилегированный доступ к маршрутизатору, может перенастроить его. Чтобы предотвратить несанкционированный доступ, интерактивные подключения к маршрутизатору должны находиться под контролем.

Хотя в большинстве случаев интерактивный доступ отключен по умолчанию, некоторые возможности все-таки сохраняются. Наиболее очевидное исключение представляют собой интерактивные сеансы, которые осуществляются с подключенных напрямую асинхронных терминалов (например, консольный терминал), а также подключения по линиям встроенных модемов.

Порты консоли

Важно помнить, что порт консоли устройства IOS имеет особые привилегии. Так, например, если сигнал BREAK посылается порту консоли в течение нескольких первых секунд после перезагрузки, то для перехвата управления системой можно легко использовать процедуру восстановления пароля. Это означает, что злоумышленники, которые могут вызвать сбой в электросети или аварийный отказ системы и которые имеют доступ к порту консоли через аппаратный терминал, модем, сервер терминала или другое сетевое устройство, могут получить контроль над системой, даже в том случае, если они не имеют физического доступа к ней или возможности обычного входа.

Следовательно, любой модем или сетевое устройство, обеспечивающее доступ к консольному порту, должно быть надежно защищено по стандарту, сравнимому с требованиями к безопасности привилегированного доступа к маршрутизатору. В случае подключения по телефонной линии любой консольный модем, как минимум, должен запрашивать у подключающегося пользователя пароль для доступа (при этом модемные пароли должны находиться под строгим контролем).

Общий интерактивный доступ

Существует огромное количество способов подключиться к маршрутизатору, о которых пользователи могут не подозревать. Программное обеспечение Cisco IOS может поддерживать следующие способы подключения (зависит от настройки и версии ПО):

- посредством Telnet
- rlogin
- SSH
- сетевые протоколы, не использующие IP (LAT, MOP, X.29, V.120 и др.)
- некоторые другие протоколы
- посредством местных асинхронных подключений и модемного доступа по телефонной линии

Продолжают появляться все новые и новые протоколы интерактивного доступа. Интерактивный доступ посредством Telnet возможен не только для стандартного порта TCP Telnet (порт 23), но также и для ряда других портов с номерами выше 23.

Все механизмы интерактивного доступа используют абстракцию IOS TTY. Другими словами, они используют сеансы связи посредством линий того или иного вида. Локальные асинхронные терминалы и коммутируемые модемы используют стандартные линии, известные как TTY. Для удаленных сетевых соединений (независимо от вида протокола) используются виртуальные терминалы – VTY. Самый лучший способ защиты системы – принять все необходимые меры по контролю в отношении всех линий, в том числе и в отношении линий VTY и TTY.

Поскольку никогда нельзя быть полностью уверенным в том, что все способы доступа были заблокированы, администраторам следует использовать тот или иной механизм аутентификации для того, чтобы обеспечить контроль за подключениями по всем линиям, даже на компьютерах, которые считаются недоступными со стороны ненадежных сетей. Это особенно важно как в случае линий VTY, так и в случае линий, подключенных к модемам или другим устройствам удаленного доступа.

Для того чтобы полностью блокировать интерактивные подключения, можно воспользоваться командами **login** и **no password**. Такой способ задан по умолчанию для терминалов VTY, но не для TTY. В случае линий TTY и VTY существует много способов настройки паролей и других видов аутентификации пользователя. Дополнительные сведения можно найти в документации, прилагающейся к программному обеспечению Cisco IOS.

Контроль за линиями TTY

Сегодня локальные асинхронные терминалы используются значительно реже, чем раньше. Однако они все еще имеются в некоторых устройствах. Если терминалы не защищены физически (и даже в случаях, когда такая защита есть), то маршрутизатор следует настраивать таким образом, чтобы для входя в систему пользователи локальных асинхронных терминалов должны были вводить имя и пароль. Большая часть портов TTY, имеющихся в современных маршрутизаторах, либо подключены к внешним модемам, либо реализуются посредством встроенных модемов. Очевидно, что обеспечение безопасности для таких портов значительно важнее, чем обеспечение безопасности для портов локальных терминалов.

По умолчанию удаленный пользователь может установить соединение с линией TTY через сеть. Это называется "обратным соединением Telnet" (reverse Telnet). Таким образом подключившийся пользователь может взаимодействовать с терминалом или модемом, которые подключены к линии TTY. Такие соединения можно защищать паролем. Зачастую бывает необходимо сделать так, чтобы пользователи, которым требуется совершить исходящий вызов, могли подключаться к модемным линиям. Однако при таком способе удаленный пользователь может подключиться к порту локального асинхронного терминала (или даже к порту телефонного модема) и сымитировать запрос на ввод логина маршрутизатора, чтобы выкрасть пароли. Такой способ позволяет проделывать и другие манипуляции, которые могут обмануть локальных пользователей или нарушить их работу.

Чтобы отключить поддержку обратных сеансов Telnet, ко всем асинхронным и модемным линиям, на которых следует запретить прием соединений от пользователей сети, необходимо применить команду конфигурации **transport input none** . Если это возможно, избегайте использовать один и тот же модем для внешнего и внутреннего доступа, а также установите запрет на установление обратных Telnet-соединений с линиями, которые используются для подключения извне.

Контроль и обеспечение бесперебойной работы терминалов VTY

Любой терминал VTY должен быть настроен только на прием подключений с использованием фактически необходимых протоколов.

Такая настройка осуществляется с помощью команды **transport input**. Например, если предполагается, что терминал VTY будет принимать только сеансы Telnet, тогда его необходимо настроить при помощи команды **transport input telnet**, в то время как для терминала VTY, поддерживающего сеансы Telnet и SSH, необходимо применить команду **transport input telnet ssh**. Если программное обеспечение поддерживает протокол зашифрованного доступа (например SSH), то будет целесообразным включить только данный протокол, отключив при этом незашифрованный протокол Telnet. Кроме того, чтобы задать IP-адреса, с которых разрешено устанавливать соединения с VTY линией, можно воспользоваться командой **ip access-class**.

Устройство Cisco IOS имеет ограниченное количество линий VTY (обычно пять). Если все линии VTY заняты, то новое удаленное подключение установить нельзя. Таким образом, потенциально имеется возможность организовать DoS-атаку ("отказ в обслуживании"). Если нападающему удастся открыть удаленные сеансы на всех линиях VTY, тогда "законный" администратор не сможет выполнить подключение. При этом злоумышленнику даже не обязательно входить в систему. Сеансы могут быть просто оставлены на стадии запроса на вход.

Такие атаки можно предотвратить, применив к одному из терминалов VTY более "жесткую" команду **ip access-class**. Последний терминал VTY (обычно это VTY 4) может быть настроен на прием соединений только от одной определенной управляющей рабочей станции, тогда как другие VTY могут принимать соединения от любого адреса в корпоративной сети.

Еще один действенный метод – настроить таймеры VTY, воспользовавшись командой **exec-timeout**. Такой способ позволяет предотвратить "засорение" терминала VTY бесконечно длящимся сеансом связи. Несмотря на то, что в случае целенаправленных атак эффективность такого метода ограничена, он все же позволяет "защитить" терминал от сеансов, оставленных открытыми непредумышленно. Точно так же можно включить таймер проверки активности TCP keepalive, воспользовавшись командой **service tcp-keepalives-in**. Такой метод позволит защититься от злоумышленных атак, а также от сеансов, оставшихся незакрытыми по причине сбоя удаленной системы.

Можно обеспечить полную защиту VTY. Для этого надо отключить все протоколы удаленного доступа, не использующие IP, и включить шифрование IPSec для всех удаленных интерактивных соединений с маршрутизатором. IPSec предоставляется за дополнительную плату, и его настройка выходит за рамки данного документа.

Предупреждающие сообщения

В некоторых юрисдикциях гражданское или уголовное преследование взломщиков, проникающих в чужие системы, станет намного проще, если разместить сообщение, предупреждающее неавторизованных пользователей о том, что они используют систему, не получив авторизации. В других юрисдикциях может быть запрещен мониторинг активности даже неавторизованных пользователей. Исключение составляют случаи, когда владелец предпринял определенные меры по уведомлению таких пользователей о своих намерениях. Одним из способов уведомления таких пользователей является размещение предупреждающего сообщения при помощи команды **banner login**.

Требования к правовым уведомлениям сложны и зависят от конкретной юрисдикции и конкретной ситуации. Даже в пределах конкретной юрисдикции судебные решения не всегда однозначны. Поэтому данную проблему следует обсудить с вашим личным юрисконсультом. Совместно с юрисконсультом необходимо решить, какие сведения должны быть включены в заголовок.

- Уведомление о том, что вход в систему и ее использование разрешен только авторизованному персоналу, и, возможно, сведения о лицах, могущих санкционировать пользование системой.
- Уведомление о том, что любое несанкционированное использование системы является незаконным и влечет за собой гражданскую и/или уголовную ответственность.
- Уведомление о том, что любое использование системы может регистрироваться или контролироваться без дальнейшего предупреждения, а полученные записи могут использоваться в суде в качестве доказательств.
- Особые примечания, необходимые в соответствии с некоторыми местными законами.

С точки зрения безопасности (но не с юридической точки зрения) отображаемое сообщение не должно содержать какой-либо информации о маршрутизаторе, его имени, модели, владельце и о программном обеспечении, которое используется на нем.Такая информация может быть использована злоумышленниками.

Стандартно настраиваемые службы управления

Для управления сетью многие пользователи используют протоколы, которые отличаются от протоколов интерактивного удаленного

входа. Наиболее распространенные протоколы для этих целей – SNMP и HTTP.

По умолчанию оба этих протокола выключены. И, что касается всех остальных служб, то надежнее всего вообще не включать эти протоколы. Тем не менее, если они все же включены, то их необходимо защитить так, как это описано в настоящем разделе.

SNMP

Протокол SNMP очень широко применяется для осуществления мониторинга маршрутизаторов. Кроме того, он довольно часто используется для внесения изменений в настройки маршрутизаторов. К сожалению, наиболее часто используемая версия 1 протокола SNMP имеет довольно слабую схему аутентификации, основанную на использовании “строки сообщества”. Это связано с тем, что фиксированный пароль передается по сети в открытом виде. По возможности старайтесь использовать 2-ю версию протокола SNMP, которая поддерживает схему проверки подлинности выборки на основе алгоритма MD5 и позволяет ограничить доступ к различной управляющей информации.

Если требуется использовать первую версию SNMP, тогда для строки сообщества следует выбирать неочевидные комбинации слов. Так, например, не следует использовать слова "public" (общедоступный) или "private" (частный). По возможности старайтесь не использовать одну и ту же строку сообщества для всех сетевых устройств. Для каждого устройства (или хотя бы для каждого участка сети) лучше использовать свою строку или строки сообщества. Строка, разрешающая только чтение, не должна совпадать со строкой, разрешающей чтение и запись. Если возможно, для строки сообщества, разрешающей только чтение, следует проводить периодический опрос SNMP версии 1. Строки для считывания и записи следует использовать только для фактических операций записи.

Протокол SNMP версии 1 не подходит для использования в общедоступной сети Интернет по следующим причинам:

- Он использует незашифрованные строки проверки подлинности.
- В большинстве реализаций SNMP такие строки отправляются неоднократно как часть периодических опросов.
- Он плохо защищен от спуфинга и является протоколом транзакций на основе датаграмм.

Прежде чем использовать этот протокол в Интернете, следует хорошо обдумать возможные последствия.

Во многих сетях разрешенные (легитимные) сообщения SNMP поступают только от определенных управляющих станций. Если это справедливо для вашей сети, то, возможно, следует использовать параметр номера списка доступа в команде **snmp-server community** для ограничения доступа SNMP версии 1 только к IP-адресам станций управления. Никогда не используйте команду **snmp-server community** при работе в среде, использующей только протокол SNMP версии 2. Эта команда автоматически включает протокол SNMP версии 1.

Для протокола SNMP версии 2 необходимо настроить проверку подлинности выборки, воспользовавшись для этого ключевыми словами **authentication** и **md5** командой конфигурации **snmp-server party**. По возможности, для каждого маршрутизатора старайтесь использовать уникальное секретное значение MD5.

Базы данных управляющих станций SNMP, содержащие информацию об аутентификации (например строки сообщества), очень часто имеют большой размер. Данная информация может быть использована для получения доступа ко многим маршрутизаторам и другим сетевым устройствам. Такая концентрация информации делает станцию управления SNMP естественной мишенью для атаки, и потому такая станция требует соответствующей защиты.

HTTP

Самые последние версии программного обеспечения Cisco IOS поддерживают удаленную настройку и контроль с использованием протокола WWW HTTP. В целом доступ посредством HTTP похож на интерактивный доступ к маршрутизатору. Используемый в HTTP протокол аутентификации равнозначен отправке открытого пароля по сети. К сожалению, в HTTP отсутствуют эффективные методы работы с одноразовыми паролями и паролями, основанными на вызовах. В силу этого довольно рискованно использовать HTTP в общедоступной сети Интернет.

Если для управления используется HTTP, то следует ограничить доступ к соответствующим IP-адресам, воспользовавшись командой **ip http access-class**. Кроме того, чтобы настроить процедуру аутентификации, воспользуйтесь командой **ip http authentication**. Точно так же, как и в случае интерактивных логинов, лучший способ проверки подлинности HTTP – использовать серверы TACACS+ или

RADIUS. Старайтесь не использовать разрешающий пароль в качестве пароля HTTP.

Управление и интерактивный доступ через Интернет (и другие ненадежные сети)

Многие пользователи управляют своими маршрутизаторами удаленно, при этом иногда управление осуществляется через Интернет. Любой незашифрованный удаленный доступ сопряжен с некоторым риском. Однако наибольшую опасность представляет собой доступ, осуществляемый через сеть общего пользования, такую как Интернет. Все схемы удаленного управления, включая интерактивный доступ, HTTP и SNMP, имеют слабые места.

Атаки, которые будут рассматриваться в этом разделе, являются относительно сложными в исполнении, но отнюдь не выходят за рамки возможностей нынешних взломщиков. Однако очень часто такие атаки можно предотвратить. Для этого необходимо, чтобы соответствующие провайдеры общедоступных сетей приняли необходимые меры безопасности. Необходимо оценить уровень надежности мер по обеспечению безопасности, которые используются всеми провайдерами, вовлеченными в передачу управляющего трафика. Даже если вы доверяете своим провайдерам, мы все равно рекомендуем принять меры, чтобы защититься от последствий ошибок, которые они могут допустить.

Все указанные меры предосторожности одинаково справедливы и для узлов, и для маршрутизаторов. В настоящем документе рассматривается организация защиты для сеанса регистрации маршрутизатора, однако аналогичные механизмы защиты необходимо использовать для ваших узлов, если вы управляете ими удаленно.

Удаленное администрирование через Internet является эффективным способом, но требует внимательного отношения к вопросам безопасности.

Анализаторы пакетов

Очень часто взломщики проникают в компьютеры, принадлежащие поставщикам Интернет-услуг или работающие в больших сетях, для того чтобы установить на этих машинах так называемые анализаторы пакетов (packet sniffer programs). Эти программы анализируют трафик, передаваемый по сети, и похищают различные данные (пароли, строки сообществ SNMP). Несмотря на то, что проделывать такие манипуляции стало сложнее (поскольку операторы сети усилили безопасность), время от времени такие атаки случаются. Кроме риска, исходящего от внешних взломщиков, возможны случаи, когда недобросовестные сотрудники компании-провайдера сами устанавливают такие анализаторы. Любая пересылка пароля по незашифрованному каналу сопряжена с риском. Сюда относятся регистрационные и разрешительные пароли для маршрутизаторов.

По возможности старайтесь не регистрироваться на маршрутизаторе через ненадежную сеть, если такой маршрутизатор не использует шифрованный протокол. Если программное обеспечение маршрутизатора поддерживает шифрованные регистрационные протоколы, такие как SSH или Telnet, использующий аутентификацию Kerberos, то лучше использовать эти протоколы. Другая возможность – использовать шифрование IPSec для всего трафика управления маршрутизатором, включая Telnet, SNMP и HTTP. На все перечисленные выше функции шифрования действуют экспортные ограничения, введенные правительством США, поэтому в случае маршрутизаторов Cisco их необходимо заказывать отдельно за дополнительную плату.

Если у вас нет возможности использовать протокол шифрованного удаленного доступа, тогда можно воспользоваться системами одноразовых паролей, такими как S/KEY или OPIE, в паре с сервером TACACS+ или RADIUS. Таким образом можно контролировать и интерактивную регистрацию, и привилегированный доступ к маршрутизатору. Преимущество заключается в том, что похищенный пароль оказывается бесполезным, поскольку он является действительным только на один сеанс связи, в ходе которого он был украден. Передаваемые в течение сеанса данные, не содержащие пароля, остаются доступными для шпионов, но, как правило, большинство программ-снифферов заняты отслеживанием паролей.

Если существует крайняя необходимость в передаче пароля в открытом сеансе Telnet, необходимо часто изменять пароли, а также уделять особое внимание пути прохождения сеанса.

Другие риски, связанные с доступом через Интернет

Помимо анализаторов пакетов удаленное Интернет-управление маршрутизаторами сопряжено со следующими рисками:

- Для того чтобы управлять маршрутизатором через Интернет, необходимо разрешить, по крайней мере, некоторым узлам Интернет получать доступ к маршрутизатору. Существует вероятность нарушения целостности узлов. Кроме того, адреса этих узлов могут подвергнуться спуфингу. При разрешенном интерактивном доступе из Интернета ваша система безопасности зависит не только от ваших мер борьбы со спуфингом, но также и от мер, принятых соответствующими провайдерами услуг.

Чтобы уменьшить возможные риски, необходимо сделать так, чтобы все узлы, которым разрешен доступ к маршрутизатору, находились под вашим личным контролем. Кроме того, следует использовать шифрованные протоколы входа, которые имеют надежные схемы аутентификации.

- Иногда злоумышленник может осуществить перехват незашифрованного TCP-соединения (например сеансы Telnet), при котором законный пользователь, теряет контроль над соединением. Хотя такие "перехваты" распространены не так широко, как технология "сниффинг", и требуют сложной подготовки, тем не менее, они все же возможны и могут использоваться злоумышленником, который хочет организовать целенаправленную атаку на вашу сеть. Единственный надежный способ решения проблемы перехвата – использовать протокол управления, имеющий сильную схему аутентификации.

- Атаки отказа от обслуживания (DoS-атаки) довольно широко распространены в сети Интернет. Если сеть подверглась DoS-атаке, то может оказаться так, что вы не сможете получить доступ к маршрутизатору, чтобы собрать данные или предпринять какие-либо защитные меры. Даже атака чужой сети может привести к повреждению управляющего доступа в вашей сети. Существует несколько способов увеличить устойчивость сети к DoS-атакам. Однако самый надежный метод защиты от таких атак заключается в использовании отдельного канала внеполосного управления. Это может быть модем удаленного доступа, который будет использоваться в экстренных случаях.

Регистрация в системе

Маршрутизаторы Cisco могут фиксировать информацию о различных событиях, многие из которых относятся к безопасности. Журналы являются неоценимым средством, помогающим выявлять инциденты, связанные с безопасностью, и реагировать на них. В маршрутизаторах Cisco используются два основных способа ведения журналов:

- Функция регистрация AAA (authentification, authorization, accounting) отвечает за сбор информации о следующих событиях: пользовательские входящие коммутируемые соединения, вход и выход из системы, доступы через HTTP, изменения в уровне привилегий, выполненные команды (а также другие аналогичные события). Записи журнала AAA отправляются на серверы аутентификации, которые используют протоколы TACACS+ и/или RADIUS, а также локально записываются на этих серверах (обычно в дисковые файлы). При наличии сервера TACACS+ или RADIUS можно использовать различные способы ведения журнала AAA. Чтобы включить функцию ведения журнала AAA, необходимо выполнить команду **aaa accounting**. Подробное описание настройки AAA не является темой настоящего документа.

- Регистрация ловушек SNMP позволяет отправлять уведомления о существенных изменениях в статусе системы на управляющих станциях SNMP. Используйте данную функцию только в том случае, если у вас уже существует инфраструктура управления SNMP.

- Ведение системного журнала — В зависимости от конфигурации системы системный журнал может регистрировать различные виды событий. События, зарегистрированные в системном журнале, могут передаваться в различные "инстанции", например:

    - Порт системной консоли (**logging console**).
    - Серверы, использующие протокол UNIX "syslog" (**logging *ip-address*, logging trap**).
    - Удаленные сеансы на VTY и локальные сеансы TTY (**logging monitor, terminal monitor**).
    - Локальный буфер журнала в RAM маршрутизатора (**logging buffered**).

  С точки зрения безопасности наиболее важными событиями, которые обычно заносятся в системный журнал, являются изменения состояний интерфейса, изменения в конфигурации системы, совпадения со списком доступа и события, обнаруженные с помощью дополнительного брандмауэра, и функции обнаружения вторжений.

  Каждое событие системной регистрации снабжается меткой уровня важности. Эти уровни варьируются начиная с отладочной информации (наименьший уровень важности) и заканчивая серьезными системными аварийными ситуациями. Для каждого регистрационного пункта можно настроить порог важности, после чего он будет получать информацию только о тех событиях, важность которых соответствует или превышает заданный порог важности.

Сохранение сведений, содержащихся в журнале

По умолчанию данные о системных событиях передаются на асинхронный консольный порт. Поскольку работа многих консольных портов не отслеживается (или такие порты могут быть подключены к терминалам, которые не хранят информацию о событиях и имеют довольно маленькие дисплеи), то такая информация может оказаться недоступной, особенно в тех случаях, когда происходит общесетевая отладка какой-либо неисправности.

Почти каждый маршрутизатор должен сохранять данные системного журнала в локальном буфере RAM. Буфер журнала имеет фиксированный размер, и в нем сохраняется только самая последняя информация. При перезагрузке маршрутизатора данные из этого буфера теряются. Даже при этих условиях буфер журнала среднего размера имеет огромное значение. На недорогих маршрутизаторах приемлемый размер буфера должен находиться в диапазоне от 16384 до 32768 байт. На маршрутизаторах высокого класса, которые имеют большие объемы памяти (и хранят большое количество записей журнала событий), размер буфера должен быть около 262144 байт. Используйте команду **show memory**, чтобы убедиться в том, что маршрутизатор обладает достаточным количеством свободной памяти для поддержки буфера журнала. Для создания буфера используйте конфигурационную команду **logging buffered *buffer-size***.

Большинство крупных систем используют серверы "syslog". Информацию о **регистрации системных событий** можно отправить на сервер при помощи logging server-ip-address. Для этой информации также можно настроить порог важности, при котором она будет регистрироваться на сервере (для этого воспользуйтесь командой **logging trap *urgency***). Даже если имеется syslog-сервер, то и в этом случае следует включить локальную регистрацию системных событий.

Если маршрутизатор имеет часы реального времени или использует протокол NTP, то в этом случае для проставления временных меток на записях журнала можно воспользоваться командой **service timestamps log datetime msecs**.

Регистрация нарушений списка доступа

Если для фильтрации трафика используются списки доступа, то в этом случае может потребоваться регистрировать пакеты, которые нарушают условия фильтрации. В ранних версиях программного обеспечения Cisco IOS для включения функции регистрации использовалось ключевое слово **log**. При этом осуществлялась регистрация IP-адресов и номеров портов, которые связаны с пакетами, удовлетворяющими критериям списка доступа. Последние версии включают ключевое слово **log-input**, добавляющее сведения об интерфейсе, от которого был получен пакет, а также MAC-адрес узла, отправившего этот пакет.

Было бы не слишком правильным настраивать ведение журнала для записей списка доступа, которые соответствуют большому числу пакетов. Это может привести к слишком сильному увеличению размера файлов журнала, что в свою очередь может сказаться на производительности. Тем не менее, к сообщениям журнала списка доступа применяются ограничения, поэтому производительность существенно не ухудшится.

Регистрация списка доступа также может использоваться для регистрации подозрительного трафика, связанного с сетевыми атаками.

Настройка безопасной IP-маршрутизации

В данном разделе описываются некоторые базовые меры безопасности, связанные со способом пересылки IP-пакетов маршрутизатором. Для получения дополнительной информации см. Основные функции IOS.

Борьба со спуфингом

Многие сетевые атаки основаны на фальсификации, или спуфинге, взломщиком адресов источника IP-датаграмм. Некоторые атаки полностью полагаются на спуфинг; другие атаки отследить намного труднее, когда атакующий "прикрывается" чужим IP-адресом. Таким образом, сетевые администраторы должны прилагать все усилия, чтобы предотвратить спуфинг.

Антиспуфинговые меры должны применяться ко всем точкам сети, там, где это целесообразно. Проще всего (и эффективнее) применять антиспуфинговые меры на границе между крупными блоками адресов или на границе между доменами сетевого администрирования. Как правило, считается нецелесообразным применять антиспуфинг на каждом маршрутизаторе сети, поскольку очень сложно определить, какие адреса источника данных могут легитимно появляться на определенных интерфейсах.

Если ваша компания является поставщиком Интернет-услуг (ISP), то вы, наверное, заметили, что эффективный антиспуфинг в сочетании с другими эффективными мерами безопасности приводит к тому, что крупные клиенты, раздраженные возникшими проблемами, начинают переходить к другим поставщикам. Поставщикам Интернет-услуг следует применять антиспуфинговые меры на телефонных пулах и на других точках соединения с конечными пользователями (см. RFC 2267).

Администраторы, отвечающие за корпоративные брандмауэры или пограничные маршрутизаторы, иногда используют средства антиспуфинга, чтобы помешать узлам, находящимся в Интернете, присваивать себе адреса внутренних узлов, однако не предпринимают никаких действий, чтобы помешать внутренним узлам присваивать себе адреса узлов, находящихся в Интернете. Необходимо предотвращать спуфинг в обоих направлениях. Существуют, по крайней мере, три веских причины использовать в корпоративном брандмауэре антиспуфинг в обоих направлениях:

1. У внутренних пользователей будет меньше искушения организовать сетевую атаку, кроме того, их шансы на успех будут значительно ниже.

2. Вероятность того, что внутренние узлы, имеющие непреднамеренные ошибки в конфигурации, могут создать проблемы для удаленных сайтов, будет ниже. Такие меры с меньшей вероятностью послужат источником жалоб со стороны клиентов или приведут к ухудшению репутации компании.

3. Внешние взломщики часто взламывают сеть, чтобы подготовить в ней платформу для последующих атак. Заинтересованность этих взломщиков будет ниже, если в сети установлена защита от исходящего спуфинга.

Борьба со спуфингом при помощи списков доступа

К сожалению, будет нецелесообразным просто перечислить список команд, которые призваны обеспечить должную защиту от спуфинга. Настройка списка доступа во многом зависит от условий работы конкретной сети. Основная задача заключается в отсеивании пакетов, которые поступают на интерфейсы, маршрут к которым не является допустимым для предполагаемых исходных адресов пакетов. Например, если на Интернет-интерфейс двухинтерфейсного маршрутизатора, который соединяет корпоративную сеть с Интернетом, поступает датаграмма, в исходном адресе которой "указан" адрес машины, находящейся в корпоративной сети, то такая датаграмма должна быть отброшена.

Подобным образом все датаграммы, которые поступают на интерфейс, подключенный к корпоративной сети, но при этом в поле исходного адреса указан адрес компьютера вне этой сети, должны быть точно так же отброшены. Если позволяют ресурсы CPU, антиспуфинг необходимо применять на всех интерфейсах, на которых возможно определить, какой приходящий трафик является легитимным.

Интернет-провайдеры, передающие транзитный трафик, могут иметь ограниченные возможности по настройке антиспуфинговых списков доступа, но такие ISP обычно могут как минимум отфильтровывать исходящий трафик, который выглядит как созданный в собственном адресном пространстве ISP.

В целом антиспуфинговые фильтры должны использоваться вместе со входными списками доступа. Это означает, что пакеты должны проходить фильтрацию на тех интерфейсах, через которые они поступают на маршрутизатор, а не на интерфейсах, через которые они уходят с маршрутизатора. Фильтрация настраивается при помощи команды конфигурирования интерфейса – **ip access-group *list* in**. В некоторых двухпортовых конфигурациях для антиспуфинга можно использовать выходные списки доступа. Однако даже в этом случае работать со входными списками значительно проще. Кроме того, входной список защищает сам маршрутизатор от спуфинговых атак, в то время как выходной список защищает только устройства, следующие за маршрутизатором.

При наличии списков для проверки подлинности адресов эти списки всегда должны отклонять датаграммы с широковещательными адресами источника или адресами источника для многоадресной рассылки, а также датаграммы с зарезервированным адресом "обратной связи", указанным в качестве адреса отправителя. Обычно антиспуфинговый список доступа должен также отфильтровывать все перенаправления ICMP, независимо от адресов отправителя или назначения. Ниже приведены соответствующие команды:

```
access-list number deny icmp any any redirect
access-list number deny ip 127.0.0.0 0.255.255.255 any
access-list number deny ip 224.0.0.0 31.255.255.255 any
access-list number deny ip host 0.0.0.0 any
```

Четвертая команда позволяет установить фильтрацию пакетов, поступающих от множественных BOOTP/DHCP-клиентов. Это значит, что такая команда не может использоваться во всех сетевых средах.

Борьба со спуфингом при помощи проверок RPF

Почти во всех версиях операционной системы Cisco IOS, которые поддерживают режим Cisco Express Forwarding (CEF), для маршрутизатора имеется возможность проверить исходный адрес любого пакета на соответствие интерфейсу, через который этот пакет поступил на маршрутизатор. Если, в соответствии с таблицей маршрутизации, входной интерфейс не подходит в качестве пути к исходному адресу, пакет отбрасывается.

Этот метод работает только при симметричной маршрутизации. Если сеть разработана таким образом, что при обычных обстоятельствах трафик из узла A в узел B идет путем, отличным от пути, по которому трафик проходит из узла B в узел A, то проверка

всегда будет заканчиваться ошибкой, а взаимодействие между двумя узлами окажется невозможным. Такая ассиметричная маршрутизация характерна для ядра Интернета. Прежде чем включить эту функцию, убедитесь, что сеть не использует асимметричную маршрутизацию.

Данная функция называется проверкой пересылки по обратному пути (reverse path forwarding – RPF) и включается с помощью команды **ip verify unicast rpf**. Эта функция имеется в программном обеспечении Cisco IOS (версии 11.1CC, 11.1CT, 11.2GS, а также все версии 12.0 и более новые), но для эффективной работы требуется, чтобы был включен режим CEF.

Осуществление контроля за прямыми широковещательными рассылками

Прямые широковещательные рассылки очень часто используются для атаки smurf (разновидность DoS-атаки). Кроме того, такие рассылки также могут использоваться и для атак, аналогичных атакам smurf.

Прямая широковещательная рассылка представляет собой датаграмму, которую отправляют на широковещательный адрес подсети, с которой компьютер, отправляющий сообщения, не имеет прямого соединения. Прямая широковещательная рассылка пересылается по сети в виде одноадресного пакета до тех пор, пока этот пакет не достигнет целевой подсети, где он преобразуется в широковещательную рассылку канального уровня. В силу особенностей архитектуры IP-адресации только последний маршрутизатор в цепочке, подключенный напрямую к подсети назначения, может окончательно определить прямую широковещательную рассылку. Прямые широковещательные рассылки иногда используются для вполне законных целей. Однако вне сферы финансовых услуг такое использование – редкость.

При атаке смарф злоумышленник, использующий сфальсифицированный адрес отправителя, отправляет эхо-запросы ICMP на адрес прямой широковещательной рассылки. После этого все узлы, принадлежащие атакуемой подсети, посылают отклики на сфальсифицированный адрес. Отправляя непрерывный поток таких запросов атакующий может создать намного больший по объему поток откликов. Таким образом, поток этих откликов может полностью "затопить" узел, адрес которого был сфальсифицирован.

Если для интерфейса Cisco была настроена команда **no ip directed-broadcast**, тогда направленные широковещательные рассылки, которые в противном случае были бы преобразованы в рассылки канального уровня, будут отброшены на этом интерфейсе. Это означает, что команду **no ip directed-broadcast** необходимо настроить на всех интерфейсах всех маршрутизаторов, которые подключены к атакуемой подсети. Настроить только маршрутизаторы с брандмауэрами будет недостаточно. Команда **no ip directed-broadcast** установлена по умолчанию в Cisco IOS версии 12.0 и последующих версий. В более ранних версиях данную команду необходимо применять ко всем интерфейсам LAN, о которых неизвестно, что они пересылают легальные направленные широковещательные рассылки.

Более подробную информацию о методе предотвращения атак смарф на маршрутизаторах с функциями брандмауэра (зависит от схемы сети), а также общие сведения об атаках смарф см. DoS-атаки .

Целостность пути

Многие атаки зависят от возможности влиять на пути, по которым датаграммы проходят по сети. Получив контроль над маршрутизацией, взломщики могут использовать адрес другого компьютера, чтобы получить обратный трафик. Они также могут перехватывать и считывать чужие данные. Кроме того, маршрутизация может быть нарушена с целью организации DoS-атаки.

Маршрутизация от источника

Протокол IP поддерживает функцию маршрутизации от источника, которая позволяет отправителю IP-датаграммы управлять маршрутом, по которому эта датаграмма будет отправлена конечному адресату, и, как правило, маршрутом, по которому будет отправлен ответ. В реальных сетях эти параметры редко используются для "законных" целей. Некоторые более старые реализации IP некорректно обрабатывают пакеты с маршрутизацией от источника. Таким образом, можно отправить им датаграммы с параметрами маршрутизации от источника для того, чтобы вызвать сбой на машинах, на которых выполняются старые протоколы IP.

Маршрутизатор Cisco, на котором настроена команда **no ip source-route**, никогда не будет пересылать IP-пакет, который содержит параметр маршрутизации по источнику. Эту команду необходимо использовать. Исключение составляют случаи, когда для сети требуется маршрутизация от источника.

ICMP-перенаправления

ICMP-сообщение о перенаправлении указывает конечному узлу использовать конкретный маршрутизатор в качестве пути к определенному месту назначения. В правильно функционирующей IP-сети маршрутизатор отправляет сообщения о перенаправлении только узлам, которые находятся в его собственной подсети. Конечный узел никогда не отправляет сообщение о перенаправлении. Кроме того, ни одно сообщение о перенаправлении никогда не пересылается более чем по одному сетевому сегменту. Однако злоумышленник может нарушить эти правила. Именно это лежит в основе некоторых сетевых атак. Входящие ICMP-сообщения о перенаправлении необходимо отфильтровывать на входных интерфейсах всех маршрутизаторов, которые находятся на границе двух административных доменов. Кроме того, будет вполне разумно сделать так, чтобы каждый список доступа, который используется на входном интерфейсе маршрутизатора Cisco, отфильтровывал все ICMP-перенаправления. В правильно настроенной сети это никак не скажется на функционировании.

Обратите внимание на то, что эта фильтрация предотвращает только переадресованные атаки, запущенные удаленными нарушителями. При этом у злоумышленников остается возможность организовать серьезный сбой при помощи перенаправлений, если их узел напрямую подключен к тому же сегменту, что и атакуемый узел.

Аутентификация и фильтр протокола маршрутизации

При использовании протокола динамической маршрутизации с поддержкой аутентификации эту аутентификацию необходимо включить. Это позволит предотвратить злонамеренные атаки, направленные на инфраструктуру маршрутизации, а также поможет избежать повреждений, вызванных неправильно настроенными "посторонними" устройствами в сети.

По той же самой причине поставщикам услуг и другим операторам больших сетей настоятельно рекомендуется использовать фильтрацию маршрутов (команда **distribute-list in**), запретив таким образом маршрутизаторам принимать заведомо некорректную информацию о маршрутизации. Несмотря на то, что чрезмерное использование фильтрации маршрутов может свести на нет преимущества динамической маршрутизации, разумное использование этой функции часто помогает предотвратить возникновение нежелательных последствий. Так, например, если вы используете протокол динамической маршрутизации для взаимодействия со шлейфной абонентской сетью, тогда вам следует принимать от этой сети только те маршруты, которые находятся в адресном пространстве, которые вы фактически выделили для данного абонента.

Подробное описание процедуры настройки проверки подлинности маршрутизации и фильтрации маршрутов не являются темой настоящего документа. Документацию можно найти в Интернете и на веб-сайте Cisco. Из-за высокого уровня сложности мы рекомендуем, чтобы новички обратились за консультацией к опытным сотрудникам, прежде чем приступить к конфигурации этих средств в важных сетях.

Управление лавинной маршрутизацией

Многие DoS-атаки основываются на "затоплении" сетевого канала бесполезными пакетами. Данные flood-атаки перегружают сетевые каналы, замедляют работу узлов и могут вызвать перегрузку маршрутизаторов. Благодаря продуманной настройке маршрутизатора воздействие таких лавинных потоков можно уменьшить.

Важная составляющая процесса управления лавинной маршрутизацией заключается в сборе сведений об ограничениях производительности. Если поток перегружает линию T1, то фильтрация потока на маршрутизаторе в начальной части линии будет эффективной, в то время как фильтрация в конечной части будет малоэффективна или вообще бесполезна. Если наиболее перегруженным компонентом сети является маршрутизатор, тогда использование защитной фильтрации, которая сама по себе интенсивно загружает маршрутизатор, может только ухудшить положение дел. Об этом необходимо помнить при реализации рекомендаций, указанных в данном разделе.

Транзитная лавинная пересылка

Функции качества обслуживания Cisco (QoS) можно использовать для защиты узлов и каналов от некоторых видов лавинных атак (flood attacks). К сожалению, общие методы борьбы с подобным управлением flood-атаками не являются темой данного документа: защитные меры, принимаемые против атаки, во многом зависят от конкретной обстановки. Единственным простым и общепринятым советом является использование очереди с весами (WFQ) во всех случаях, когда для этого достаточно ресурсов ЦП. В последних версиях программного обеспечения Cisco IOS очередь WFQ установлена по умолчанию для низкоскоростных линий последовательной передачи. Среди других полезных функций можно назвать гарантированную скорость доступа (CAR), общее формирование трафика (GTS) и пользовательскую организацию очередей. Иногда эти функции можно включить непосредственно в момент атаки.

Если вы планируете использовать QoS-функции для сдерживания flood-атак, то для этого необходимо представлять себе, как эти функции работают, а также механизм работы типичных flood-атак. Например, будет значительно эффективнее использовать очередь WFQ против лавины эхо-запросов (ping flood), нежели против лавины SYN. Дело в том, что типичная лавина ICMP-пакетов будет

восприниматься WFQ как единый поток трафика, в то время как при лавине запросов SYN каждый пакет воспринимается в виде отдельного потока. Ответный смарф-поток разделяется на два. Большое количество информации о QoS-функциях Cisco можно найти на официальной странице Cisco, а сведения о наиболее распространенных атаках можно найти на веб-сайтах других компаний.

Маршрутизаторы Cisco имеют две разные функции, специально предназначенные для ослабления воздействия SYN-атак на узлы. Функция TCP Intercept имеется в определенных версиях программного обеспечения многих маршрутизаторов, имеющих номер модели 4000 и выше. Набор функций брандмауэра Cisco IOS, который сейчас имеется во многих маршрутизаторах Cisco, включает другую функцию защиты от лавинной SYN-атаки. Защита от такой атаки может требовать принятия комплексных мер, при этом результаты такой защиты могут быть различными. Это зависит от степени переполнения, скорости маршрутизатора и объема памяти, а также используемых узлов. Прежде чем настроить одну из указанных функций, обязательно ознакомьтесь с документацией, находящейся на глобальном сайте Cisco. Кроме того, если возможно, протестируйте ваши настройки в режиме реальной flood-атаки.

Самозащита маршрутизатора

Защиту сети от воздействия лавинной маршрутизации может обеспечить только маршрутизатор, который сам обладает достаточной защитой от перегрузки трафика.

Режимы коммутации и режим Cisco Express Forwarding

Режим коммутации CEF, имеющийся в версиях 11.1CC, 11.1CT, 11.2GS и 12.0 программного обеспечения Cisco IOS, заменяет традиционный кэш маршрутизации Cisco структурой данных, которая зеркально отражает таблицу маршрутизации всей системы. Поскольку при поступлении трафика для новых мест назначения нет необходимости создавать записи кэша, CEF функционирует более предсказуемо, чем прочие режимы, при наличии больших объемов трафика, отправляемого во много отличающихся между собой пунктов назначения.

Хотя большинство лавинных DoS-атак направляют свой трафик на одну или несколько целей и не обременяют традиционный алгоритм управления кэшем, многие известные лавинные SYN-атаки используют случайные исходные адреса. Узел, подвергшийся атаке, отвечает на некоторую часть пакетов лавинной передачи SYN, создавая трафик для большого числа получателей. Таким образом, маршрутизаторы, настроенные для работы в режиме CEF, лучше работают в случае лавинных SYN-атак (направляемых на узлы, а не на сами маршрутизаторы), чем маршрутизаторы, использующие традиционный кэш. Всегда старайтесь использовать режим CEF.

Настройка планировщика

Когда маршрутизатор Cisco быстро переключает большое число пакетов, он может потратить столько времени на ответы прерываниям, поступающим от сетевых интерфейсов, что никакие другие работы не будут выполнены. Такое может происходить при прохождении очень быстрых потоков пакетов. Чтобы ослабить это воздействие, воспользуйтесь командой **scheduler interval**, которая приказывает маршрутизатору остановить обработку прерываний и выполнять другие операции через регулярные интервалы. Типичная конфигурация может включать команду **scheduler interval 500**, которая предписывает маршрутизатору обрабатывать задачи уровня обработки не реже чем каждые 500 миллисекунд. Поскольку эта команда редко становится причиной неполадок, ее следует включать в стандартную конфигурацию маршрутизатора, за исключением случаев, когда у вас есть серьезные причины не делать этого.

Во многих более новых платформах Cisco вместо команды **scheduler interval** используется команда **scheduler allocate**. Команда **scheduler allocate** принимает два параметра: период времени (мкс), в течение которого система работает с включенными прерываниями, а также период времени (мкс), когда система работает со скрытыми прерываниями. Если ваша система не принимает команду **scheduler interval 500**, тогда используйте команду **scheduler allocate 3000 1000**. Указанные значения соответствуют средним точкам диапазона. Числовой диапазон для первого значения варьируется от 400 до 60000, для второго – от 100 до 4000. Эти параметры можно подстраивать.

Возможно, излишние службы

Как правило, все ненужные службы следует отключить на всех маршрутизаторах, к которым может быть получен доступ из потенциально враждебной сети. Службы, перечисленные в настоящем разделе, время от времени бывают полезны. Однако если они не используются интенсивно, тогда их необходимо отключить.

Малые службы TCP и UDP

По умолчанию все версии Cisco IOS начиная с версии 11.3 и ниже имеют следующие малые службы:

- echo
- chargen
- discard

Эти службы, в особенности службы протокола UDP, довольно редко используются для "законных" целей. Однако они могут использоваться для проведения DoS-атак, а также для проведения других атак, которые в других случаях можно предотвратить при помощи фильтрации пакетов.

Например, нападающий может отправить DNS-пакет с поддельным исходным адресом, чтобы выступать в роли DNS-сервера, который в противном случае будет недоступен, а также с поддельным исходным портом службы DNS (порт 53). Если такой пакет был отправлен на эхо-порт Cisco UDP, результатом будет отправка Cisco пакета DNS на указанный сервер. Список для исходящего доступа к этому пакету не применяется, поскольку такой список генерируется локально самим маршрутизатором.

Хотя антиспуфинговые списки доступа помогают избежать несанкционированного использования малых служб или сделать такое использование менее опасным, практически во всех случаях эти службы должны быть выключены на всех маршрутизаторах, являющихся частью брандмауэра или находящихся в важных с точки зрения безопасности участках сети. Поскольку данные службы используются редко, наилучшей стратегией будет отключить эти службы на всех имеющихся маршрутизаторах.

В Cisco IOS начиная с версии 12.0 и выше все малые службы отключены по умолчанию. В ранних версиях ПО эти службы можно было отключить при помощи команд **no service tcp-small-servers** и **no service udp-small-servers**.

Служба "Finger"

В маршрутизаторах Cisco реализована служба "finger", которая позволяет узнать, какие пользователи в настоящее время зарегистрировались на сетевом устройстве. В большинстве случаев данная информация является секретной. Однако в некоторых случаях она может оказаться полезной для злоумышленника. Службу "finger" можно отключить при помощи команды **no service finger** .

Протокол NTP

Использование протокола сетевого времени (NTP) не сопряжено с каким-то особым риском. Однако любые излишние сервисы могут послужить лазейкой для нападающего. Если требуется использовать протокол NTP, то в этом случае очень важно однозначно указать надежный источник синхронизации, а также задействовать подходящий механизм аутентификации. Это связано с тем, что повреждение временной шкалы – хороший способ нарушить работу некоторых протоколов безопасности. Если интерфейс маршрутизатора не использует протокол NTP, тогда этот протокол можно отключить при помощи команды интерфейса **ntp disable**.

Протокол CDP

Протокол обнаружения Cisco (CDP) используется для некоторых функций управления сетью. Однако использование данного протокола небезопасно, поскольку протокол позволяет любой системе в подключенном напрямую сегменте определить, что маршрутизатор является устройством Cisco, и определить номер модели и версию используемой программы Cisco IOS. Эта информация может быть использована при планировании атак на маршрутизатор. Информация протокола CDP доступна только для напрямую подключенных систем. Протокол CDP можно отключить, воспользовавшись командой глобальной настройки **no cdp running**. Этот протокол можно отключить на отдельном интерфейсе при помощи команды **no cdp enable**.

Установка обновлений

Как и в любом программном обеспечении, в Cisco IOS встречаются ошибки. Некоторые из этих ошибок затрагивают безопасность. Кроме того, продолжают появляться новые виды сетевых атак. Это значит, что способ функционирования устройства, который в момент написания программы считался корректным, может в будущем представлять опасность, если он будет злонамеренно "эксплуатироваться".

При обнаружении в продукте Cisco серьезного нарушения безопасности компания Cisco распространяет информационное сообщение об обнаруженной уязвимости. Более подробно о процедуре выработки уведомления в связи с обнаружением слабых мест в защите

см.Ответ на обращение в службу безопасности продуктов Cisco. Более подробно об уведомлениях других видов см. Сообщения и примечания по безопасности продуктов Cisco.

Почти любое непредусмотренное поведение любого компонента программного обеспечения может создать ту или иную угрозу для безопасности. Однако в информационных бюллетенях упоминаются только те ошибки, которые имеют самое непосредственное отношение к безопасности системы. Безопасность системы улучшается за счет обновления ПО до последних версий, даже если при этом не было никаких уведомлений о случаях нарушения безопасности.

Существуют проблемы безопасности, которые не связаны с ошибками в программах. По этой причине для сетевых администраторов очень важно следить за появлением новых видов сетевых атак. Информированием о последних тенденциях в сфере сетевых атак занимаются различные сайты, списки Интернет-рассылок и новостные группы Usenet.

Список команд

Настоящий раздел представляет собой краткую памятку по настройкам, описанным в других разделах настоящего документа. Конфигурационные команды Cisco IOS сведены в таблицу для более удобного запоминания. Всегда внимательно читайте документацию по каждой команде, прежде чем применять ее.

Используйте команду	Чтобы
enable secret	Настроить пароль для привилегированного доступа к маршрутизатору.
service password-encryption	Обеспечить минимальную защиту для настроенных паролей.
no service tcp-small-servers **no service udp-small-servers**	Предотвратить злоумышленное использование малых служб для проведения различных сетевых атак, включая DoS-атаки.
no service finger	Предотвратить предоставление пользовательской информации потенциальным злоумышленникам.
no cdp running **no cdp enable**	Предотвратить предоставление информации о маршрутизаторе устройствам, которые напрямую подключены к этому маршрутизатору.
ntp disable	Предотвратить атаки против службы NTP.
no ip directed-broadcast	Помешать нападающим использовать маршрутизатор в качестве "усилителя" smurf-атаки.
transport input	Указать, какие протоколы могут использоваться удаленными пользователями для установления интерактивного подключения к терминалу VTY или к портам TTY на маршрутизаторе.
	Указать, какие IP-адреса могут использоваться для

ip access-class	подключения к портам TTY или VTY. Зарезервировать один порт VTY для доступа с управляющей рабочей станции.
exec-timeout	Запретить "пустым" сеансам связи занимать VTY на неопределенно долгое время.
service tcp-keepalives-in	Выявить и закрыть нерабочие интерактивные сеансы, которые необоснованно занимают VTY.
logging buffered *buffer-size*	Сохранить регистрационную информацию в RAM-буфере маршрутизатора. В последних версиях программного обеспечения после размера буфера можно указать порог важности.
ip access-group *list* in	Отбросить сфальсифицированные IP-пакеты. Сбросить входящие перенаправления ICMP.
ip verify unicast rpf	Сбросить сфальсифицированные IP-пакеты в *сетях с симметричной маршрутизацией* и только при использование режима CEF.
no ip source-route	Предотвратить использование функций IP-маршрутизации от источника в целях фальсификации трафика.
access-list *number action criteria* log **access-list *number action criteria* log-input**	Включить регистрацию пакетов, которые совпадают с критериями, указанными в данном списке доступа. Используйте команду **log-input**, если таковая имеется в вашем ПО.
scheduler-interval **scheduler allocate**	Предотвратить отключение важных процессов при лавинном трафике.
ip route 0.0.0.0 0.0.0.0 null 0 244	Включить быстрый сброс пакетов, имеющих недействительный конечный адрес.
distribute-list *list* in	Фильтровать данные о маршрутизации, чтобы предотвратить использование недействительных маршрутов.
snmp-server community *something-inobvious* ro *list* **snmp-server community *something-***	Включить протокол SNMP версии 1, настроить аутентификацию и ограничить доступ к определенным IP-адресам. Протокол SNMP версии 1 следует использовать только в случае, если недоступна версия 2, при этом нужно принять меры защиты от анализаторов пакетов. Включайте протокол SNMP, только если он нужен в вашей сети. Включайте доступ с правами чтение-запись, только если это действительно необходимо.

inobvious* rw *list	
snmp-server party... authentication md5 *secret* ...	Настроить процедуру аутентификации для протокола SNMP версии 2, использующего алгоритм аутентификации MD5. Включайте протокол SNMP, только если это действительно необходимо в данной сети.
ip http authentication *method*	Проводить аутентификацию запросов на HTTP-соединения (если HTTP включен на маршрутизаторе).
ip http access-class *list*	Осуществлять дальнейший контроль за HTTP-доступом, ограничив его определенными адресами узлов (если HTTP включен на маршрутизаторе).
banner login	Установить предупредительный баннер, который будет демонстрироваться пользователям, пытающимся зарегистрироваться на маршрутизаторе.

Смежные темы

- **Основные функции IOS для поставщиков Интернет-услуг**
- **Последняя информация о DoS-атаках: "Smurfing"**
- **Ответ на обращение в службу безопасности продуктов Cisco**
- **Информационные сообщения Cisco, посвященные вопросам безопасности**
- **RFC 2267**
- **Техническая поддержка и документация – Cisco Systems**

Дата генерации PDF файла: Jan 05, 2010

http://www.cisco.com/support/RU/customer/content/9/92078/21.shtml