Руководство Cisco по усилению защиты устройств Cisco IOS

Содержание

Шифрование сеансов управления
SSHv2
Расширения SSHv2 для ключей RSA
Консоль и порты AUX
Управление линиями vty и tty
Управление транспортом для линий vty и tty
Предупреждающие сообщения
Аутентификация, авторизация и учет
Аутентификация TACACS+
Откат аутентификации
Использование паролей типа 7
Авторизация TACACS+ Command
Учет команд TACACS+
Резервные серверы AAA
Защита протокола SNMP
Строки имени и пароля SNMP
Строки имени и пароля SNMP со списками ACL
Инфраструктурные списки ACL
Представления SNMP
Протокол SNMP версии 3
Защита уровня администрирования
Оптимальные методы ведения журнала
Отправка журналов в центральное расположение
Уровень регистрации
Отказ от входа в сеансы консоли или монитора
Ведение журнала с буферизацией
Настройка интерфейса источника журнала
Настройка меток времени ведения журнала
Управление конфигурацией программного обеспечения Cisco IOS
Замена конфигурации и откат конфигурации
Исключительный доступ к изменению конфигурации
Эластичная конфигурация программного обеспечения Cisco IOS
Цифровая подпись программного обеспечения Cisco
Ведение журнала и уведомление об изменении конфигурации
Плоскость управления
Общая защита уровня управления
Переадресации IP ICMP
Недостижимые ICMP
Протокол прокси-ARP
Ограничение влияния трафика уровня управления на ЦП
Общие сведения о трафике уровня управления
Инфраструктурные списки ACL
Списки ACL для входящего трафика
CoPP
Защита уровня управления

Введение

В данном документе содержится информация, которая поможет защитить системные устройства Cisco IOS® и повысить общий уровень безопасности вашей сети. Данный документ, разбитый на три плоскости, каждая из которых реализует разные функции сетевого устройства, содержит обзор всех входящих в них функций и ссылки на соответствующую документацию.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

Три функциональных уровня сети (уровень администрирования, уровень управления и уровень передачи данных), каждый предоставляет собственную функциональность, которая должна быть защищена.

- **Уровень администрирования управляет трафиком, направляемым устройству Cisco IOS и состоящим из приложений и протоколов, таких как Secure Shell (SSH) и SNMP.**
- **Уровень управления сетевого устройства обрабатывает трафик, необходимый для поддержания функциональности инфраструктуры сети.** Уровень управления состоит из приложений и протоколов между сетевыми устройствами, в том числе протокола BGP, а также протоколов IGP, таких как EIGRP и OSPF.
- **Уровень передачи данных пересылает данные через сетевое устройство.** Уровень передачи данных не содержит трафик, передаваемый локальному устройству Cisco IOS.

Сведений, приведенных в описаниях функций безопасности в данном документе, часто достаточно для их настройки. Однако в случаях, где описания недостаточно, функция объясняется таким образом, который позволяет оценить, требуется ли уделять ей дополнительное внимание. Там, где это возможно и уместно, документ содержит рекомендации, которые, будучи реализованными, помогут защитить сеть.

Защищенные операции

Защищенные сетевые операции — важная тема. Большая часть этого документа посвящена безопасной настройке устройства Cisco IOS, но одной лишь настройкой не удастся полностью защитить сеть. Используемые в сети рабочие процедуры влияют на защиту базовых устройств в такой же мере, как и настройки.

Данные разделы содержат рекомендации, которые полезно внедрить. В них описаны некоторые критические области работы сети, и они не являются исчерпывающими.

Отслеживание рекомендаций и ответов Cisco по безопасности

Группа реагирования на события безопасности (PSIRT) готовит и распространяет публикации, обычно именуемые рекомендациями PSIRT, по проблемам, связанным с безопасностью продуктов Cisco. Для менее серьезных проблем публикуются ответы по безопасности Cisco Security Response. Ответы и рекомендации по вопросам безопасности доступны на странице http://www.cisco.com/go/psirt.

Дополнительные сведения об этих механизмах связи см. в разделе Cisco Security Vulnerability Policy (Политика устранения уязвимостей Cisco).

Для поддержания безопасности сети необходимо принимать во внимание ответы и рекомендации по безопасности Cisco. Необходимо заранее знать об уязвимостях, чтобы оценить угрозу, которую они представляют для сети. Помощь по процессу оценки см. в материале Risk Triage for Security Vulnerability Announcements (Рассмотрение рисков для объявлений уязвимостей).

Применение аутентификации, авторизации и учетных записей

Платформа аутентификации, авторизации и учета (AAA) имеет важнейшее значение для устройств защищенной сети. Инфраструктура AAA обеспечивает аутентификацию сеансов управления и может ограничивать доступные пользователю команды до набора, определяемого администратором, а также записывать в журнал все команды, вводимые всеми пользователями. Дополнительную информацию об использовании AAA см. в разделе Аутентификация, авторизация и учет данного документа.

Централизация мониторинга и сбора журналов

Для того чтобы получить сведения о существующих, новых и прошлых событиях, связанных с инцидентами безопасности, организация должна иметь единый подход к ведению журнала событий и их взаимосвязи. Этот подход должен охватывать журналы со всех сетевых устройств и задействовать предварительно подготовленные и настраиваемые возможности корреляции.

После того как обеспечено централизованное ведение журналов, необходимо разработать структурированный подход к анализу журналов и отслеживанию инцидентов. Исходя из потребностей вашей организации, этот подход может меняться от простого внимательного просмотра данных журналов до расширенного анализа на основе правил.

В разделе Оптимальные методы ведения журнала данного документа можно получить дополнительную информацию о ведении журналов для сетевых устройств Cisco IOS.

Использование защищенных протоколов по мере возможности

Многие протоколы используются для передачи конфиденциальных данных управления сетью. По возможности необходимо использовать защищенные протоколы. Выбирая защищенный протокол, можно использовать SSH вместо Telnet, чтобы данные аутентификации и информация управления передавались в зашифрованном виде. Кроме того, необходимо использовать протоколы защищенной передачи файлов при копировании данных конфигурации. Примером является использование протокола SCP вместо FTP или TFTP.

В разделе Защищенные интерактивные сеансы управления данного документа содержится дополнительная информация о защищенном управлении устройствами Cisco IOS.

Обеспечение видимости трафика с помощью NetFlow

NetFlow позволяет вести мониторинг трафика в сети. NetFlow первоначально предназначался для экспорта информации о трафике в приложения для управления сетью и может использоваться для отображения сведений о потоках данных на маршрутизаторе. Эта возможность позволяет увидеть, какой трафик проходит по сети в реальном времени. Независимо от того, экспортируются ли сведения о потоках в удаленный коллектор, рекомендуется настроить сетевые устройства для NetFlow так, чтобы оперативно использовать их при необходимости.

Дополнительные сведения об этой функции см. в разделе Идентификация и обратная трассировка трафика данного документа и в материале http://www.cisco.com/go/netflow (только зарегистрированные заказчики).

Управление конфигурацией

Управление конфигурацией — это процесс предложения, просмотра, утверждения и развертывания изменений конфигурации. В контексте конфигурации устройств Cisco IOS критически важными являются два дополнительных аспекта управления конфигурацией: архивация конфигурации и безопасность.

Можно использовать архивные конфигурации для отката изменений, сделанных на сетевых устройствах. В контексте безопасности архивные конфигурации могут также использоваться с целью определить, какие изменения безопасности были сделаны и когда произошли эти изменения. В сочетании с данными журналов AAA эта информация может быть полезна в деле аудита безопасности сетевых устройств.

В конфигурации устройства Cisco IOS содержится множество конфиденциальных данных. Примеры такой информации — имена пользователей, пароли и содержимое списков управления доступом. Репозиторий, используемый для архивации конфигураций устройства

Cisco IOS, должен быть защищенным. Незащищенный доступ к этой информации может поставить под угрозу нарушения безопасности всю сеть.

Уровень администрирования

Уровень администрирования состоит из функций, предназначенных для администрирования сети. Они включают интерактивные сеансы управления, которые используют SSH, а также сбор статистики с SNMP или технологию NetFlow. При оценке безопасности сетевого устройства важно обеспечить защиту уровня администрирования. Если инцидент безопасности способен скомпрометировать функции уровня администрирования, может быть утрачена возможность восстановить или стабилизировать сеть.

В следующих разделах данного документа описываются конфигурации и функции безопасности, доступные в программном обеспечении Cisco IOS, которые помогают защитить уровень администрирования.

Общая защита уровня администрирования

Уровень администрирования позволяет производить доступ, настраивать устройство и управлять им, а также контролировать его работу и сеть, в которой устройство развернуто. Уровень администрирования получает и отправляет трафик, необходимый для работы этих функций. Необходимо защитить как уровень администрирования, так и уровень управления устройством, поскольку работа уровня управления напрямую влияет на уровень администрирования. Следующие протоколы используются на уровне администрирования:

- Simple Network Management Protocol
- Telnet
- Secure Shell
- Протокол передачи файлов
- Trivial File Transfer Protocol
- Secure Copy Protocol (SCP)
- TACACS +
- RADIUS
- NetFlow
- Протокол NTP (Network Time Protocol, протокол сетевого времени)
- Системный журнал

Должны быть предприняты действия, чтобы обеспечить выживание уровней управления и администрирования при нарушениях безопасности. Если один из этих уровней успешно взломан, то все уровни могут быть скомпрометированы.

Управление паролями

Пароли служат для управления доступом к ресурсам или устройствам. Это достигается через определение пароля или секрета, которые используются для аутентификации запросов. При получении запроса на доступ к ресурсу или устройству выполняется проверка пароля и удостоверения, а затем по результатам проверки доступ предоставляется, запрещается или ограничивается. Рекомендуется управлять паролями с помощью сервера аутентификации TACACS+ RADIUS. Но обратите внимание, что локально настроенный пароль для привилегированного доступа по-прежнему необходим на случай отказа сервисов TACACS+ или RADIUS. Устройство может также иметь другую информацию о паролях в своей конфигурации, например: ключ NTP, строку SNMP-сообщества или ключ протокола маршрутизации.

Команда enable secret служит для задания пароля, который предоставляет привилегированный административный доступ системе Cisco IOS. Должна использоваться команда enable secret, а не более старая команда enable password. Команда enable password использует слабый алгоритм шифрования.

Если enable secret не задан, а пароль настроен для линии консоли tty, то пароль консоли может быть использован для получения привилегированного доступа даже из сеанса удаленного виртуального tty (vty). Это действие почти наверняка нежелательно и является другой причиной настройки enable secret.

Команда глобальной конфигурации service password-encryption указывает программному обеспечению Cisco IOS шифровать пароли, секреты CHAP и аналогичные данные, которые сохраняются в его файле конфигурации. Такое шифрование полезно, чтобы помешать случайным наблюдателям видеть пароли, например, на экране администратора. **Но алгоритм, используемый командой service password-encryption >, является простым шифром Vigenere.** Алгоритм не разработан для защиты файлов конфигурации от серьезного анализа даже малоопытными злоумышленниками и не должен использоваться для этой цели. Любой файл конфигурации Cisco IOS, который содержит зашифрованные пароли, должен обрабатываться с той же осторожностью, как и незашифрованный список тех же паролей.

Хотя этот слабый алгоритм шифрования не используется командой enable secret, он используется командой глобальной конфигурации enable password, а также командой конфигурации командной строки password. Пароли этого типа необходимо исключить, заменив их командой enable secret или функцией Enhanced Password Security (Расширенная защита паролей).

Команда enable secret и функция расширенной защиты паролей используют алгоритм MD5 для хеширования пароля. Этот алгоритм был внимательно изучен общественностью и, насколько известно, необратим. Но этот алгоритм уязвим для атак перебором по словарю. При атаке перебором по словарю злоумышленник пробует каждое слово в словаре или другом списке вероятных паролей для обнаружения соответствия. Поэтому файлы конфигурации должны быть надежно сохранены и доступны только доверенным лицам.

Расширенная защита паролей

Функция расширенной защиты паролей, появившаяся в программном обеспечении Cisco IOS версии 12.2(8)T, позволяет администратору настроить хеширование MD5 для паролей в команде username. До появления этой функции существовали пароли двух типов: Тип 0, который является незашифрованным паролем, и тип 7, который использует алгоритм

шифрования Vigenere. Функция расширенной защиты паролей не может быть использована с протоколами, которые требуют возможности извлечения незашифрованного пароля, например CHAP.

Для шифрования пароля пользователя по алгоритму MD5 выполните команду глобальной конфигурации username secret.

```
!

username <name> secret <password>

!
```

Дополнительные сведения об этой функции см. в публикации Enhanced Password Security (Расширенная защита паролей).

Блокировка подбора пароля для входа

Функция блокировки подбора пароля для входа, появившаяся в программном обеспечении Cisco IOS версии 12.3(14)T, позволяет заблокировать учетную запись локального пользователя после заданного числа неуспешных попыток входа. После блокировки пользователя его учетная запись остается заблокированной до тех пор, пока вы не разблокируете ее. С помощью этой функции нельзя блокировать авторизованного пользователя, настроенного с уровнем привилегий 15. Число пользователей с уровнем привилегий 15 должно быть сведено к минимуму.

Обратите внимание, что авторизованные пользователи могут быть заблокированы на устройстве, если достигнуто максимальное число неудачных попыток входа. Кроме того, злоумышленник может создать условие отказа в обслуживании (DoS), повторяя попытки аутентификации с действительным именем пользователя.

В данном примере показано, как включить функцию блокировки подбора пароля для входа:

```
!

aaa new-model
aaa local authentication attempts max-fail <max-attempts>
aaa authentication login default local

!

username <name> secret <password>

!
```

Эта функция применима и для других методов аутентификации, например CHAP и PAP.

Функция No Service Password-Recovery

В программном обеспечении Cisco IOS версии 12.3(14)T и более поздних версиях эта функция не позволяет пользователям с консольным доступом незащищенный доступ к конфигурации устройства и сброс пароля. Она также не позволит злоумышленнику менять значения реестра конфигурации и обращаться к NVRAM.

```
!

no service password-recovery

!
```

Программное обеспечение Cisco IOS предусматривает процедуру восстановления пароля на основе доступа к режиму монитора ПЗУ (ROMMON) по нажатию клавиши Break во время запуска системы. В ROMMON программное обеспечение устройства может быть перезагружено в новой конфигурации системы с новым паролем.

Благодаря процедуре восстановления текущего пароля любой пользователь с консольным доступом обратится к устройству и его сети. Функция No Service Password-Recovery предотвращает выполнение последовательности по нажатию клавиши Break и вход в ROMMON во время запуска системы.

Если на устройстве включен режим no service password-recovery, то рекомендуется сохранить копию конфигурации устройства и применить решение для архивирования конфигурации. Если необходимо восстановить пароль устройства Cisco IOS, после того, как эта функция активирована, удаляется вся конфигурация.

Подробнее об этой функции см. Secure ROMMON Configuration Example (Пример защищенной конфигурации ROMMON).

Отключение неиспользуемых служб

В рамках оптимального подхода к безопасности все необязательные службы должны быть отключены. Необязательные службы, особенно использующие протокол UDP, иногда применяются для законных целей, но могут использоваться для DoS и других атак, которые в противном случае предотвращаются путем фильтрации пакетов.

Маленькие службы TCP и UDP должны быть отключены. В их число входят:

- echo (номер порта 7)
- discard (номер порта 9)
- daytime (номер порта 13)
- chargen (номер порта 19)

Можно избежать злоупотребления малыми службами или снизить их опасность за счет использования списков доступа с функцией антиспуфинга, эти службы должны быть отключены на всех устройствах, доступных в сети. В Cisco IOS начиная с версии 12.0 и выше все малые службы отключены по умолчанию. **В более ранних версиях ПО можно выполнить команды глобальной конфигурации no service tcp-small-servers и udp-small-servers no service для их отключения.**

Ниже приведен список дополнительных служб, которые должны быть отключены, если не используются:

- **Не Не Выполните команду глобальной конфигурации no ip finger, чтобы отключить службу Finger.** В версиях программного обеспечения Cisco IOS позже 12.1 (5) и 12.1 (5)

T эта служба отключена по умолчанию.

- **Выполните команду глобальной конфигурации no ip bootp server, чтобы отключить протокол начальной загрузки (BOOTP).**

- **В версии программного обеспечения Cisco IOS 12.2 (8) T и более поздних выполните команду ip dhcp bootp ignore в режиме глобальной конфигурации для отключения BOOTP.** Она оставит службы DHCP включенными.

- Если службы ретрансляции DHCP не требуются, службы DHCP можно отключить. **Выполните команду no service dhcp в режиме глобальной конфигурации.**

- **Не Не Выполните no mop enabled в режиме конфигурации интерфейса для отключения службы MOP.**

- **Выполните команду глобальной конфигурации no ip domain lookup для отключения служб разрешения DNS.**

- **Выполните команду no service pad в режиме глобальной конфигурации для отключения службы PAD, которая используется для сетей X.25.**

- **Сервер HTTP можно отключить командой no ip http server в режиме глобальной конфигурации, а сервер HTTPS можно отключить командой глобальной конфигурации no ip http secure-server.**

- **Если устройства Cisco IOS не получают конфигурацию из сети во время запуска, то необходимо использовать команду глобальной конфигурации no service config.** Тогда устройство Cisco IOS не будет пытаться найти файл конфигурации в сети через TFTP.

- Cisco Discovery Protocol (CDP) — сетевой протокол, который служит для обнаружения других устройств с поддержкой CDP для образования смежности и определения топологии сети. Протокол CDP может использоваться системами управления сетью (NMS) или для устранения проблем. CDP должен быть отключен на всех интерфейсах, которые подключены к ненадежным сетям. **Это можно сделать с помощью команды интерфейса no cdp enable. Иначе можно отключить CDP глобально с помощью команды глобальной конфигурации no cdp run.** Обратите внимание, что CDP может быть использован злоумышленником для разведки и выяснения топологии сети.

- Протокол LLDP является протоколом IEEE, который определен в 802.1AB. Протокол LLDP похож на CDP. Но этот протокол обеспечивает совместимость между другими устройствами, которые не поддерживают CDP. С LLDP следует обращаться так же, как и с CDP, и отключать на всех интерфейсах, подключенных к ненадежным сетям. **Для того чтобы добиться этого, выполните команды конфигурации интерфейса no lldp transmit и no lldp receive. Не Не Выполните команды глобальной конфигурации no lldp run , чтобы отключить LLDP глобально.** LLDP может также быть использован злоумышленником для разведки и выяснения топологии сети.

- Для коммутаторов, которые поддерживают загрузку с sdflash, уровень безопасности

можно повысить путем загрузки с карты флеш-памяти и отключения sdflash с помощью команды конфигурации no sdflash.

Тайм-аут EXEC

Для того чтобы задать интервал, в течение которого интерпретатор команд EXEC ожидает ввода от пользователя, прежде чем завершить сеанс, выполните в командной строке команду конфигурации exec-timeout. Команда exec-timeout должна использоваться для завершения сеансов на бездействующих линиях vty и tty. По умолчанию сеансы отключаются после десяти минут бездействия.

```
!

line con 0
exec-timeout <minutes> [seconds]
line vty 0 4
exec-timeout <minutes> [seconds]
!
```

Проверка активности для сеансов TCP

Команды глобальной конфигурации service tcp-keepalives-in и service tcp-keepalives-out позволяют устройству отправлять TCP-пакеты проверки активности для сеансов TCP. Эта конфигурация должна использоваться для включения проверки активности TCP на входящих подключениях к устройству и исходящих подключениях от устройства. Это гарантирует, что устройство на удаленном конце подключения все еще доступно и что полуоткрытые или потерянные подключения удалены из локального устройства Cisco IOS.

```
!

service tcp-keepalives-in
service tcp-keepalives-out
!
```

Использование интерфейса управления

К К Уровень администрирования устройства доступен по штатному каналу или внештатному каналу через физический или логический интерфейс управления. В идеале доступ для администрирования по штатному и внештатному каналу существует для каждого сетевого устройства, чтобы уровень администрирования был доступен в случае выхода сети из строя.

Один из наиболее распространенных интерфейсов, который используется для доступа к устройству по штатному каналу, является логический интерфейс замыкания на себя. Интерфейсы замыкания на себя подключены всегда, тогда как физические интерфейсы могут менять состояние, и интерфейс не всегда доступен. Рекомендуется добавлять интерфейс замыкания на себя к каждому устройству в качестве интерфейса администрирования и разрешать доступ к нему исключительно для уровня администрирования. Это позволяет администратору применять политики по всей сети для уровня администрирования. После настройки интерфейса обратной петли на устройстве он может использоваться протоколами уровня администрирования, такими как SSH, SNMP и syslog, для приема и передачи трафика.

```
!
interface Loopback0
 ip address 192.168.1.1 255.255.255.0
!
```

Уведомления о пороговых значениях памяти

Функция уведомлений о пороговых значениях памяти, которая появилась в программном обеспечении Cisco IOS версии 12.3(4)T, позволяет смягчать нехватку памяти на устройстве. Эта функция использует два метода для достижения этой цели: Уведомление о пороговых значениях памяти и резервирование памяти.

Уведомление о пороговых значениях памяти записывает в журнал сообщение, указывающее, что размер доступной памяти на устройстве ниже заданного порогового значения. **Следующий пример конфигурации показывает, как активировать эту функцию командой глобальной конфигурации memory free low-watermark.** Это позволяет устройству создать уведомление, когда объем свободной памяти ниже, чем заданная пороговая величина, и еще раз, когда объем свободной памяти на 5 % превышает заданную пороговую величину.

```
!

memory free low-watermark processor <threshold>
memory free low-watermark io <threshold>
!
```

Резервирование памяти служит для того, чтобы было достаточно памяти для важных уведомлений. Следующий пример конфигурации демонстрирует, как включить эту функцию. Она гарантирует, что процессы управления продолжат работать, если исчерпана память на устройстве.

```
!
memory reserve critical <value> !
```

Дополнительные сведения об этой функции см. в материале Memory Threshold Notifications (Уведомления о пороговых значениях памяти).

Уведомление о пороговых значениях загрузки ЦП

Возможность уведомления о пороговых значениях загрузки ЦП появилась в версии программного обеспечения Cisco IOS 12.3(4)T и позволяет обнаруживать и отправлять уведомление, когда загрузка ЦП на устройстве превышает заданное пороговое значение. При превышении порогового значения устройство создает и отправляет сообщение прерывания SNMP. Два метода задания порога загрузки ЦП поддерживаются программным обеспечением Cisco IOS: Пороговое значение повышения и пороговое значение понижения.

Пример конфигурации показывает, как включить пороговые значения повышения и понижения, которые инициируют уведомление о пороговом значении загрузки ЦП:

```
!

snmp-server enable traps cpu threshold
```

```
!

snmp-server host <host-address> <community-string> cpu
!

process cpu threshold type <type> rising <percentage> interval <seconds>
[falling <percentage> interval <seconds>]
process cpu statistics limit entry-percentage <number> [size <seconds>]
!
```

Дополнительные сведения об этой функции см. в материале CPU Thresholding Notification (Уведомление о пороговых значениях загрузки ЦП).

&

Резервная память для доступа к консоли

В версии программного обеспечения Cisco IOS 12.4(15)T и более поздних можно использовать функцию резервирования памяти для доступа к консоли. Она резервирует объем памяти, достаточный для доступа к консоли в целях администрирования и устранения проблем устройства Cisco IOS. Эта функция особенно полезна, когда на устройстве не хватает памяти. **Для того чтобы включить эту функцию, выполните команду глобальной конфигурации memory reserve console.** Данный пример настраивает устройство Cisco IOS для резервирования 4096 килобайт для этой цели.

```
!
memory reserve console 4096
!
```

Дополнительную информацию об этой функции см. в материале Reserve Memory for Console Access (Резервирование памяти для доступа к консоли).

Детектор утечек памяти

Функция детектора утечки памяти, которая появилась в версии программного обеспечения Cisco IOS 12.3 (8) T1, позволяет обнаруживать утечки памяти на устройстве. Детектор утечки памяти способен находить утечки во всех пулах памяти, буферах пакетов и блоках. Утечки памяти являются статическими или динамическими распределениями памяти, которые не служат никакой полезной цели. Эта функция отслеживает динамические распределения памяти. **Для обнаружения утечек памяти можно использовать команду EXEC show memory debug leaks.**

Переполнение буфера: Функция обнаружения и исправления порчи «красной зоны»

В программном обеспечении Cisco IOS версии 12.3(7)T и более поздних версий переполнение буфера: Можно включить функцию обнаружения и исправления порчи «красной зоны» для обнаружения и коррекции переполнения блоков памяти и продолжения работы.

Следующие команды глобальной конфигурации можно использовать для включения этой функции. **После настройки можно выполнить команду show memory overflow для отображения статистики обнаружения и исправления переполнения буфера.**

```
!
exception memory ignore overflow io
exception memory ignore overflow processor
!
```

Расширенный сбор файлов crashinfo

Функция расширенного сбора файлов crashinfo автоматически удаляет старые файлы crashinfo. Эта функция, которая появилась в версии Cisco IOS 12.3(11)T, позволяет устройству освобождать место для создания новых файлов crashinfo при сбое устройства. Эта функция также обеспечивает настройку количества сохраняемых файлов crashinfo.

```
!
exception crashinfo maximum files <number-of-files>
!
```

Протокол NTP (Network Time Protocol, протокол сетевого времени)

Протокол NTP не является особенно опасной службой, но любая ненужный служба может представлять вектор атаки. Если NTP используется, важно явным образом настроить доверенный источник времени и использовать надлежащую аутентификацию. Точная и надежная синхронизация времени необходима для ведения системного журнала, например для расследования потенциальных атак, а также для успешной работы VPN, когда подключение зависит от сертификатов при аутентификации фазы 1.

- **NTP Time Zone (Часовой пояс NTP). При настройке NTP часовой пояс должен быть настроен для точного соответствия меток времени.** Обычно Обычно Обычно существует два подхода к настройке часового пояса для устройств в сети с глобальным присутствием. Один метод — настройка всех сетевых устройств по времени UTC (ранее называлось временем по Гринвичу, или GMT). Другой подход — настройка на сетевых устройствах локального часового пояса. Дополнительные сведения об этой функции можно найти в материалах clock timezone (часовой пояс) в документации по продуктам Cisco.

- **Аутентификация NTP (Аутентификация NTP). Если настроена аутентификация NTP, то она обеспечивает обмен сообщениями NTP между доверенными одноранговыми узлами NTP.**

Пример конфигурации с использованием аутентификации NTP:

Клиент:

```
(config)#ntp authenticate
(config)#ntp authentication-key 5 md5 ciscotime
(config)#ntp trusted-key 5
(config)#ntp server 172.16.1.5 key 5
```

Сервер:

```
(config)#ntp authenticate
(config)#ntp authentication-key 5 md5 ciscotime
(config)#ntp trusted-key 5
```

Отключение Smart Install

Оптимальные методы безопасности, связанные с функцией Cisco Smart Install (SMI), зависят от того, как функция используется в конкретной среде заказчика. Cisco различает следующие варианты:

- Заказчики, которые не используют функцию Smart Install.
- Заказчики, которые задействуют функцию Smart Install только для автоматического развертывания.
- Заказчики, которые задействуют функцию Smart Install для более чем одного автоматического развертывания (управление конфигурацией и образами).

Следующие разделы описывают каждый сценарий подробно:

- Заказчики, которые не используют функцию Smart Install.
- **Заказчики, которые не используют функцию Cisco Smart Install и у которых имеется версия Cisco IOS и Cisco IOS XE, где команда доступна, должны отключить функцию Smart Install с помощью команды no vstack.**

  Примечание. Команда vstack появилась в версии Cisco IOS 12.2 (55) SE03.

Ниже приведен пример вывода команды show vstack на коммутаторе Cisco Catalyst с отключенной функцией клиента Smart Install:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Заказчики, которые задействуют функцию Smart Install только для автоматического развертывания

Отключите функцию Smart Install после того, как автоматическая установка завершена, или используйте команду no vstack.

Для распространения команды no vstack по сети используйте один из следующих методов:

- **Введите команду no vstack на всех клиентских коммутаторах вручную или с помощью сценария.**
- **Не Не Добавьте команду no vstack в конфигурацию Cisco IOS, которая отправляется в каждый клиент Smart Install в рамках автоматической установки.**
- **В версиях, которые не поддерживают команду vstack (Cisco IOS версии 12.2 (55) SE02 и более ранние), примените список контроля доступа (ACL) на клиентских коммутаторах для блокировки трафика по TCP-порту 4786.**

Для того чтобы включить функцию Smart Install позже, введите команду vstack на всех клиентских коммутаторах вручную или с помощью сценария.

Заказчики, которые задействуют функцию Smart Install для более чем одного автоматического развертывания

Архитектура Smart Install требует уделить внимание тому, чтобы адресное пространство IP-адресов инфраструктуры не было доступно для лиц, не пользующихся доверием. **В версиях, которые не поддерживают команду vstack, убедитесь, что только управляющий Smart Install имеет TCP-подключение ко всем клиентам Smart Install через порт 4786.**

Администраторы могут использовать эти оптимальные методы безопасности для Cisco

Smart Install на соответствующих устройствах:

- Списки ACL на интерфейсе
- Политики уровня управления (CoPP). Эта функция доступна не во всех версиях программного обеспечения Cisco IOS.

Следующий пример показывает ACL интерфейса с IP-адресом управляющего Smart Install 10.10.10.1 и IP-адресом клиента Smart Install 10.10.10.200:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Этот ACL должен быть развернут на всех IP-интерфейсах на всех клиентах. Он также должен быть отправлен через управляющего при первоначальном развертывании коммутаторов.

Для того чтобы еще больше ограничить доступ ко всем клиентам в рамках инфраструктуры, администраторы могут использовать следующие оптимальные методы безопасности для других устройств в сети:

- Списки управления доступом к инфраструктуре (iACL)
- Списки управления доступом к VLAN (VACL)

Ограничение доступа к сети с помощью инфраструктурных списков ACL

Списки управления доступом к инфраструктуре (iACL) предназначены для предотвращения несанкционированного прямого подключения к сетевым устройствам, поэтому они являются одним из важнейших средств управления безопасностью, которые могут применяться в сетях. Инфраструктурные списки ACL построены с учетом обстоятельства, что почти весь сетевой трафик пересекает сеть и не предназначен для самой сети.

IACL создается и применяется для определения подключений от хостов или сетей, которые необходимо разрешить сетевым устройствам. Распространенными примерами таких типов подключений являются eBGP, SSH и SNMP. После того как соответствующие подключения разрешены, весь остальной трафик к инфраструктуре явным образом запрещается. Весь транзитный трафик, который пересекает сеть и не предназначен для устройств инфраструктуры, явным образом разрешается.

Средства защиты, реализуемые iACL, относятся к уровням администрирования и управления. IACL проще реализовать за счет использования уникальной адресации для устройств сетевой инфраструктуры. *Дополнительные сведения о последствиях IP-адресации для безопасности см. в материале A Security Oriented Approach to IP Addressing (Ориентированный на безопасность подход к IP-адресации).*

Следующий пример конфигурации iACL иллюстрирует структуру, которая должна использоваться в качестве отправной точки процесса внедрения iACL:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

После создания iACL должен быть применен ко всем интерфейсам, обращенным к

устройствам, не относящимся к инфраструктуре. Сюда относятся интерфейсы, которые соединяются с другими организациями, сегментами удаленного доступа, пользовательскими сегментами и сегментами в центрах обработки данных.

Для получения дополнительной информации см. раздел "Защита ядра: Списки контроля доступа к инфраструктуре, где можно получить дополнительную информацию об инфраструктурных списках ACL.

Фильтрация пакетов ICMP

Протокол ICMP разработан как протокол управления IP. Поэтому передаваемые им сообщения могут иметь далеко идущие последствия для протоколов TCP и IP в целом. **Поскольку сетевые инструменты ping и traceroute используют ICMP, внешнее подключение ICMP редко необходимо для надлежащей работы сети.**

Программное обеспечение Cisco IOS располагает функциональностью для специальной фильтрации сообщений ICMP по имени или типу и коду. Данный пример ACL, который должен использоваться для записей контроля доступа (ACE) из предыдущих примеров, обеспечивает проверку связи от доверенных станций управления и серверов NMS и блокирует все другие пакеты ICMP:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Фильтрация IP-фрагментов

Процесс фильтрации фрагментированных пакетов IP может представлять угрозу для устройств. Это вызвано тем, что информация уровня 4, которая используется для фильтрации пакетов TCP и UDP, присутствует только в начальном фрагменте. Программное обеспечение Cisco IOS использует специальный метод для проверки последующих фрагментов по настроенным спискам доступа. Программное обеспечение Cisco IOS оценивает последующие фрагменты по ACL и игнорирует любую информацию фильтрации уровня 4. Это приводит к тому, что последующие фрагменты могут оцениваться только в части уровня 3 любого настроенного ACE.

В данном примере конфигурации, если пакет TCP, адресованный на 192.168.1.1 по порту 22, фрагментирован в пути, то начальный фрагмент, как и ожидается, отбрасывается вторым ACE на основании информации уровня 4 в пакете. Однако все оставшиеся (последующие) фрагменты получают разрешение от первого ACE исключительно на основе информации уровня 3 в пакете и ACE. Этот сценарий показан в следующей конфигурации:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Из-за неинтуитивной природы обработки IP-фрагментов они часто случайно разрешаются списками ACL. Фрагментация также часто используется при попытках обойти системы обнаружения атак. Именно по этой причине IP-фрагменты часто используются в атаках, поэтому они подлежат явной фильтрации вверху каждого настроенного списка iACL. Следующий пример ACL включает комплексную фильтрацию IP-фрагментов. Функциональность данного примера должна использоваться в сочетании с функциональностью предыдущих примеров.

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

В материале Access Control Lists and IP Fragments (Списки контроля доступа и IP-фрагменты) можно найти дополнительную информацию о том, как ACL обрабатывает фрагментированные IP-пакеты.

Поддержка ACL для фильтрации IP-параметров

В программном обеспечении Cisco IOS версии 12.3(4)T появилась поддержка использования ACL для фильтрации пакетов IP на основе IP-параметров, которые содержатся в пакете. IP-параметры представляют проблему безопасности для сетевых устройств, так как эти параметры необходимо обрабатывать как пакеты-исключения. Это требует затрат ресурсов ЦП, которые не требуются для обычных пакетов, которые проходят по сети. Присутствие параметров IP в пакете может также указывать на попытку обойти средства контроля безопасности в сети или иным образом изменить транзитные характеристики пакета. Именно поэтому фильтрация пакетов с IP-параметрами должна происходить на периферии сети.

Следующий пример должен использоваться с ACE от предыдущих примеров, чтобы обеспечить полную фильтрацию пакетов IP, которые содержат IP-параметры:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Поддержка ACL для фильтрации по значению TTL

В программном обеспечении Cisco IOS версии 12.4(2)T появилась поддержка ACL для фильтрации IP-пакетов по значению TTL. Значение TTL IP-дейтаграммы уменьшается на единицу для каждого сетевого устройства по мере прохождения пакета от источника до назначения. Начальное значение зависит от операционной системы, но, когда TTL пакета достигает нуля, пакет должен быть отброшен. Устройство, которое уменьшает TTL на единицу до нуля и таким образом отбрасывает пакет, должно создать и отправить ICMP-сообщение Time Exceeded Message источнику пакета.

Создание и передача этих сообщений являются процессом исключения. Маршрутизаторы могут выполнять эту функцию, когда количество таких IP-пакетов невелико, но, если количество пакетов с истекшим временем жизни большое, создание и отправка этих сообщений могут занять все доступные ресурсы ЦП. Эта особенность представляет собой вектор DoS-атаки. Именно по этой причине необходимо повысить устойчивость устройств к DoS-атакам, которые используют большое число IP-пакетов, время жизни которых скоро истекает.

Организациям рекомендуется фильтровать пакеты IP с низкими значениями TTL на периферии сети. Полная фильтрация пакетов со значениями TTL, недостаточными для прохождения по сети, уменьшает угрозы атак на основе TTL.

Следующий пример ACL фильтрует пакеты со значениями TTL меньше шести. Это защищает от атак на основе TTL для сетей, имеющих до пяти переходов.

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

> **Примечание. Некоторые протоколы законно используют пакеты с низкими значениями TTL.** один из таких протоколов — eBGP. В материале TTL Expiry Attack Identification and Mitigation (Идентификация и снижение эффективности атак на основе TTL) можно получить дополнительную информацию о снижении эффективности атак на основе TTL.

Дополнительные сведения об этой функции см. в материале ACL Support for Filtering on TTL Value (Поддержка ACL для фильтрации по значению TTL).

Защищенные интерактивные сеансы управления

Сеансы управления для устройств дают возможность просматривать и собирать информацию об устройстве и его работе. Если эта информация станет известна злоумышленнику, то устройство может подвергнуться атаке, быть скомпрометировано и использовано для проведения следующих атак. У У Любой пользователь с привилегированным доступом к устройству имеет возможность полного административного контроля этого устройства. Необходима защита сеансов управления для предотвращения раскрытия информации и неавторизованного доступа.

Защита уровня администрирования

В программном обеспечении Cisco IOS версии 12.4(6)T и более поздних версий функция защиты плоскости управления (MPP) позволяет администратору указать, для каких интерфейсов трафик администрирования может быть получен устройством. Это предоставляет администратору дополнительный контроль над устройством и способом доступа к нему.

Данный пример показывает, как включить MPP, чтобы разрешить только SSH и HTTPS на интерфейсе GigabitEthernet0/1:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

В материале Management Plane Protection (Защита уровня администрирования) можно получить дополнительную информацию о MPP.

Защита уровня управления

Защита уровня управления (CPPr) построена на функциональности политик уровня управления, ограничивая и определяя политики трафика уровня управления, передаваемого процессору маршрута устройства IOS. Функция CPPr, которая появилась в программном обеспечении Cisco IOS версии 12.4(4)T, делит уровень управления на отдельные категории, которые называются подынтерфейсами. Существует три подынтерфейса уровня управления: Хост, транзит и исключение CEF. Кроме того, CPPr включает следующие дополнительные функции защиты уровня управления:

- **Фильтрация портов. Эта функция обеспечивает применение политик и отбрасывание**

пакетов, проходящих к закрытому или непрослушивающему порту TCP или UDP.

- **Применение политик пороговых значений очереди. Эта функция ограничивает количество пакетов для указанного протокола, которое можно поместить во входящую очередь IP уровня управления.**

CPPr позволяет администратору классифицировать, определять политики и ограничивать трафик, который передается устройству для целей управления, по подынтерфейсу хоста. Примеры пакетов, классифицированных для категории подынтерфейса хоста, охватывают трафик управления, например SSH или Telnet, и протоколы маршрутизации.

Примечание. CPPr не поддерживает IPv6 и ограничен входным путем IPv4.

В материалах Control Plane Protection Feature Guide - 12.4T (Руководство по функции защиты уровня управления — 12.4T) и Understanding Control Plane Protection (Общие сведения о защите уровня управления) можно найти дополнительную информацию о функции Cisco CPPr.

Шифрование сеансов управления

В интерактивном сеансе управления может произойти раскрытие информации, поэтому трафик должен быть зашифрован таким образом, чтобы злоумышленник не мог получить доступ к передаваемым данным. Шифрование трафика обеспечивает защищенный удаленный доступ к устройству. Если трафик для сеанса управления передается по сети в открытом виде, то злоумышленник может получить конфиденциальные данные об устройстве и сети.

Администратор может обеспечить шифрование и защиту подключения управления удаленного доступа к устройству с помощью протоколов SSH или HTTPS. Программное обеспечение Cisco IOS поддерживает версии SSH 1.0 (SSHv1), SSH 2.0 (SSHv2) и HTTPS, в которых используются протоколы SSL и TLS для аутентификации и шифрования данных. SSHv1 и SSHv2 несовместимы. SSHv1 небезопасен и не стандартизирован, поэтому не рекомендован для использования, если доступен SSHv2.

Программное обеспечение Cisco IOS также поддерживает протокол SCP, который обеспечивает зашифрованное и защищенное соединение для копирования конфигураций устройства или образов программного обеспечения. SCP построен на основе SSH. Следующий пример конфигурации включает SSH на устройстве Cisco IOS:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Следующий пример конфигурации включает службы SCP:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Это пример конфигурации для служб HTTPS:

```
switch# show vstack
```

```
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

В материалах Configuring Secure Shell on Routers and Switches Running Cisco IOS (Настройка защищенной оболочки на маршрутизаторах и коммутаторах, работающих под управлением Cisco IOS) и Secure Shell (SSH) FAQ (Часто задаваемые вопросы по защищенной оболочке (SSH)) можно получить дополнительную информацию о функции SSH программного обеспечения Cisco IOS.

SSHv2

Поддержка SSHv2, которая появилась в программном обеспечении Cisco IOS версии 12.3(4)T, позволяет пользователю настроить SSHv2. (Поддержка SSHv1 реализована в предыдущих версиях программного обеспечения Cisco IOS.) SSH работает поверх уровня надежной передачи данных и обеспечивает строгую аутентификацию и хорошее шифрование. Единственным надежным транспортом для SSH является TCP. Протокол SSH обеспечивает возможность надежного доступа и защищенного выполнения команд на другом компьютере или устройстве по сети. Протокол SCP, который туннелируется через SSH, обеспечивает защищенную передачу файлов.

Если команда ip ssh verson 2 не настроена явным образом, то Cisco IOS включает версию SSH 1.99. Версия SSH 1.99 поддерживает подключения SSHv1 и SSHv2. SSHv1 считается ненадежным и может иметь негативное влияние на систему. **Если SSH включен, рекомендуется отключить SSHv1 с помощью команды ip ssh version 2.**

Следующий пример конфигурации включает SSHv2 (с отключенным SSHv1) на устройстве Cisco IOS:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Дополнительную информацию об использовании SSHv2 см. в материале Secure Shell Version 2 Support (Поддержка Secure Shell версии 2).

Расширения SSHv2 для ключей RSA

Cisco IOS SSHv2 поддерживает интерактивные методы аутентификации через клавиатуру и методы на основе пароля. Расширения SSHv2 для ключей RSA также поддерживают аутентификацию по открытому ключу RSA для клиента и сервера.

Для аутентификации каждого пользователя используется пара открытого и закрытого ключей RSA. Пользователь должен создать открытый и закрытый ключи на клиенте и настроить открытый ключ на сервере Cisco IOS SSH для выполнения аутентификации.

Пользователь SSH, который пытается задать учетные данные, передает подпись, зашифрованную закрытым ключом. Подпись и открытый ключ пользователя передаются серверу SSH для аутентификации. Сервер SSH вычисляет хеш по открытому ключу, предоставленному пользователем. Хеш используется для поиска соответствующей записи на сервере. Если соответствие найдено, проверка сообщения на основе RSA выполняется с помощью открытого ключа. Таким образом на основе зашифрованной подписи пользователь проходит проверку, или ему запрещается доступ.

Для аутентификации сервера клиент Cisco IOS SSH должен назначить ключ хоста каждому серверу. Когда клиент пытается установить сеанс с сервером SSH, он получает подпись сервера в сообщении обмена ключами. Если флаг строгой проверки ключа хоста включен на клиенте, то клиент проверяет, есть ли у него запись ключа для хоста, соответствующего предварительно настроенному серверу. Если соответствие найдено, то клиент проверяет подпись с помощью ключа сервера. Если сервер успешно прошел аутентификацию, установка сеанса продолжается; **в противном случае она завершается и выдается сообщение Server Authentication Failed (Ошибка аутентификации сервера).**

В следующем примере конфигурации включается использование ключей RSA с SSHv2 на устройстве Cisco IOS:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

В материале Secure Shell Version 2 Enhancements for RSA Keys (Расширения Secure Shell версии 2 для ключей RSA) можно получить дополнительную информацию об использовании ключей RSA с SSHv2.

Следующий пример конфигурации позволяет серверу Cisco IOS SSH аутентифицировать пользователя на основе RSA. Аутентификация пользователя успешна, если открытый ключ RSA, сохраненный на сервере, проверен с использованием пары открытого и закрытого ключей, хранящихся на клиенте.

```
!
! Configure a hostname for the device
!

hostname router
!
! Configure a domain name
!

ip domain-name cisco.com
!
! Generate RSA key pairs using a modulus of 2048 bits
!

crypto key generate rsa modulus 2048
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Configure the SSH username
!

username ssh-user
!
! Specify the RSA public key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
```

```
! key-hash command (followed by the SSH key type and version.)
!
```

В материале Configuring the Cisco IOS SSH Server to Perform RSA-Based User Authentication (Настройка сервера Cisco IOS SSH для аутентификации пользователя на основе RSA) можно получить дополнительную информацию об использовании ключей RSA с SSHv2.

Следующий пример конфигурации включает на клиенте Cisco IOS SSH аутентификацию сервера на основе RSA.

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

В разделе Настройка клиента Cisco IOS SSH для аутентификации сервера на основе RSA можно получить дополнительную информацию об использовании ключей RSA с SSHv2.

Консоль и порты AUX

В устройствах Cisco IOS порты консоли и вспомогательные порты (AUX) являются асинхронными линиями, которые могут использоваться для локального и удаленного доступа к устройству. Необходимо знать, что консольные порты на устройствах Cisco IOS имеют особые привилегии. В частности, эти привилегии позволяют администратору выполнять процедуру восстановления пароля. Для восстановления пароля злоумышленнику, не прошедшему аутентификацию, потребовался бы доступ к консольному порту и возможность отключения питания устройства или возможность ввести устройство в состояние сбоя.

Любой метод, используемый для доступа к консольному порту устройства, должен быть защищен способом, соответствующим уровню защиты привилегированного доступа к устройству. Методы, используемые для защиты доступа, должны включать использование аутентификации (AAA), тайм-аута EXEC и паролей модема, если модем подключен к консоли.

Если восстановление пароля не требуется, то администратор может помешать выполнить процедуру восстановления пароля с помощью команды глобальной конфигурации password-recovery no service; однако, как только команда no service password-recovery включена, администратор не сможет восстановить пароль на устройстве.

В большинстве случаев порт AUX устройства должен быть отключен, чтобы исключить неавторизованный доступ. Порт AUX можно отключить следующими командами:

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

Управление линиями vty и tty

Интерактивные сеансы управления в программном обеспечении Cisco IOS используют tty или виртуальный tty (vty). Tty является локальной асинхронной линией, к которой можно подключить терминал для локального (или к модему для удаленного) доступа к устройству. Обратите внимание, что tty можно использовать для подключения к консольным портам других устройств. Эта функция позволяет устройству с линиями tty работать как сервер консоли, где подключения можно устанавливать по сети к консольным портам устройств,

подключенных к линиям tty. Также необходимо контролировать линии tty для обратных подключений по сети.

Линия vty используется для всех остальных удаленных сетевых соединений, поддерживаемых устройством, независимо от протокола (например, SSH, SCP или Telnet). Для того чтобы гарантировать доступность устройства через локальный или удаленный сеанс управления, надлежащие средства управления должны быть включены на линиях vty и tty. Устройства Cisco IOS имеют ограниченное число линий vty; число доступных линий можно определить с помощью EXEC-команды show line. Если все линии vty заняты, то новые сеансы управления нельзя установить, что создает условие DoS-атаки для доступа к устройству.

Самая простая форма управления доступом к vty или tty устройства — аутентификация на всех линиях, независимо от размещения устройства в сети. Это важно для линий vty, так как они доступны через сеть. Линия tty, связанная с модемом, который используется для удаленного доступа к устройству, или линия tty, подключенная к консольному порту других устройств, также доступна через сеть. **Если используются списки доступа к интерфейсам на устройстве, другие формы доступа vty и tty можно применить с помощью команд конфигурации transport input и access-class с использованием функций CoPP и CPPr.**

Аутентификация может быть принудительно включена с помощью AAA, который является рекомендуемым методом санкционированного доступа к устройству с использованием локальной базы данных пользователей, или простой аутентификацией по паролю, настраиваемой непосредственно на линии tty или vty.

Команда exec-timeout должна использоваться для завершения сеансов на бездействующих линиях vty и tty. Команда service tcp-keepalives-in также должна использоваться для включения проверки активности TCP на входящих подключениях к устройству. Это гарантирует, что устройство на удаленном конце соединения все еще доступно, а полуоткрытые или потерянные соединения удаляются из локального устройства IOS.

Управление транспортом для линий vty и tty

Vty и tty должны быть настроены для приема только зашифрованных и защищенных управляющих подключений к устройству или через устройство, если оно используется в качестве сервера консоли. В этом разделе рассматриваются линии tty, так как они могут быть подключены к консольным портам на других устройствах, что позволяет обеспечить доступ к tty по сети. **Для того чтобы предотвратить раскрытие информации или неавторизованный доступ к данным, передающимся между администратором и устройством, необходимо использовать команду transport input ssh вместо протоколов открытого текста, таких как Telnet и rlogin. Конфигурацию transport input none можно включить на tty, что фактически запретит использование линии tty для обратных консольных соединений.**

Линии vty и tty позволяют администратору подключаться к другим устройствам. **Для ограничения типа транспорта, который администратор может использовать для исходящих соединений, используйте команду transport output. Если исходящие соединения не нужны, то следует использовать команду transport output none. Но если исходящие соединения разрешены, то зашифрованный и защищенный метод удаленного доступа для соединения должен быть принудительно включен с помощью команды ssh transport output.**

Примечание. IPSec может использоваться для шифрования и защиты подключений

удаленного доступа с устройством, если он поддерживается. При использовании IPSec он также увеличивает дополнительную нагрузку на ЦП устройства. Но SSH все же будет использоваться в качестве транспорта, даже если используется IPSec.

Предупреждающие сообщения

В некоторых юрисдикциях невозможно преследование по суду и является незаконным мониторинг злоумышленников, пока они не уведомлены, что им не разрешается пользоваться системой. Один из методов такого уведомления — размещение информации в виде сообщения на баннере, настраиваемого с помощью команды Cisco IOS banner login.

Юридические требования сложны, зависят от юрисдикции и ситуации и должны быть проработаны с юристом. Юридические заключения могут отличаться даже в рамках одной юрисдикции. По согласованию с юристом баннер может содержать следующую информацию:

- Обратите внимание, что входить в систему и пользоваться ей должны только авторизованные пользователи. Возможно, следует включить информацию о том, кто может авторизовать использование.
- Обратите внимание, что любое неавторизованное использование системы незаконно и может стать причиной гражданско-правовых санкций и уголовного преследования.
- Обратите внимание, что любое использование системы регистрируется и может быть проверено без дополнительного уведомления, а журналы могут использоваться в качестве доказательства в суде.
- Предупреждения, специфичные для местного законодательства.

С точки зрения безопасности, а не закона баннер входа в систему не должен содержать конкретной информации об имени маршрутизатора, модели, программном обеспечении или владении. Этой информацией могут воспользоваться злоумышленники.

Аутентификация, авторизация и учет

Платформа аутентификации, авторизации и учета (AAA) играет важную роль в обеспечении интерактивного доступа к сетевым устройствам. Инфраструктура AAA предоставляет собой глубоко настраиваемую среду, которую можно адаптировать исходя из потребностей сети.

Аутентификация TACACS+

TACACS+ — протокол аутентификации, который может использоваться устройствами Cisco IOS для аутентификации пользователей системы управления на удаленном сервере AAA. Пользователи системы управления могут производить доступ к устройству IOS через SSH, HTTPS, telnet или HTTP.

Аутентификация TACACS+ (или в общем случае аутентификация AAA) обеспечивает возможность использовать учетные записи отдельного пользователя для каждого администратора сети. Уровень безопасности сети и ее отслеживаемость повышаются, когда вы не зависите от одного разделяемого пароля.

Протокол RADIUS близок по назначению к протоколу TACACS+; однако он только шифрует пароль, передаваемый через сеть. В отличие от него TACACS+ шифрует всю полезную нагрузку TCP, которая содержит как имя пользователя, так и пароль. По этой причине использование TACACS+ предпочтительнее, чем RADIUS, если TACACS+ поддерживается сервером AAA. В материале TACACS+ and RADIUS Comparison (Сравнение TACACS+ и RADIUS) приведено более подробное сравнение этих двух протоколов.

Аутентификация TACACS+ может быть включена на устройстве Cisco IOS с конфигурацией, аналогичной приведенной в данном примере:

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

Предыдущая конфигурация может использоваться в качестве отправной точки для определенного организацией шаблона аутентификации AAA. В материале Authentication, Authorization, and Accounting (Аутентификация, авторизация и учет) можно получить дополнительную информацию о конфигурации AAA.

Список методов — последовательный список, содержащий методы аутентификации, запрашиваемые для аутентификации пользователя. Списки методов позволяют определить один или несколько протоколов безопасности, используемых для аутентификации, и таким образом гарантировать резервную систему для аутентификации на случай, если первый метод неудачен. Программное обеспечение Cisco IOS использует первый метод в списке, который успешно принял или отклонил пользователя. Следующие методы используются только тогда, когда предыдущие завершились ошибкой из-за недоступности сервера или неверной конфигурации.

В материале Named Method Lists for Authentication (Именованные списки методов для аутентификации) можно получить дополнительную информацию о настройке именованных списков методов.

Откат аутентификации

Если все настроенные серверы TACACS+ недоступны, то устройство Cisco IOS может задействовать вспомогательные протоколы аутентификации. Если все настроенные серверы TACACS+ недоступны, то типичная конфигурация задействует использование локальной аутентификации или аутентификации enable.

Полный список вариантов для аутентификации на устройстве: enable, local и line. Каждая из этих опций имеет преимущества. Использование enable secret предпочтительно потому, что секрет хешируется с помощью одностороннего алгоритма, который изначально более защищен, чем алгоритм шифрования, который используется с паролями типа 7 для аутентификации line или локальной.

Однако в выпусках Cisco IOS, которые поддерживают использование секретных паролей для локально определенных пользователей, откат к локальной аутентификации может оказаться желательным. Это позволяет создать локально определяемого пользователя для одного или нескольких администраторов сети. Если TACACS+ стал абсолютно недоступен, то администратор может воспользоваться своим локальным именем пользователя и паролем. Несмотря на то что это действие действительно повышает ответственность администраторов сети при неработоспособности TACACS+, одновременно значительно увеличиваются административные накладные расходы, так как необходимо поддерживать локальные учетные записи пользователей на всех сетевых устройствах.

Следующий пример конфигурации построен на основе предыдущего примера аутентификации TACACS+ для включения отката аутентификации к паролю, локально настроенному с помощью команды enable secret:

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
```

```
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

В материале Configuring Authentication (Настройка аутентификации) можно получить дополнительную информацию об использовании отката аутентификации при работе с AAA.

Использование паролей типа 7

Пароли типа 7, первоначально разработанные для быстрой расшифровки сохраненных паролей, не являются надежной формой хранения пароля. Существует много программных средств, способных легко расшифровать эти пароли. Использования паролей типа 7 нужно избегать, если только это не требуется для работы какой-либо функции на устройстве Cisco IOS.

Когда возможно, должен использоваться тип 9 (сценарий):

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

Удалять пароли этого типа можно с помощью аутентификации AAA и с использованием

функции расширенной защиты паролей, которая позволяет использовать секретные пароли пользователям, локально определенные командой глобальной конфигурации username.
Если вы не можете полностью исключить использование паролей типа 7, рассматривайте эти пароли как замаскированные, но не зашифрованные.

См. раздел Общая защита уровня администрирования данного документа, где можно получить дополнительную информацию об удалении паролей типа 7.

Авторизация TACACS+ Command

Авторизация команд с помощью TACACS+ и AAA предоставляет механизм, который разрешает или запрещает каждую команду, вводимую администратором. Когда пользователь вводит команды EXEC, Cisco IOS отправляет каждую команду к настроенному серверу AAA. Сервер AAA на основе настроенных политик разрешает или запрещает выполнение команды для данного конкретного пользователя.

Такая конфигурация может быть добавлена к предыдущему примеру аутентификации AAA, чтобы реализовать авторизацию выполнения команд:

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

В материале Configuring Authorization (Настройка авторизации) можно получить дополнительную информацию об авторизации команд.

Учет команд TACACS+

Если настроен учет команд, то AAA передает информацию о каждой введенной команде EXEC настроенному серверу TACACS+. Информация, передаваемая серверу TACACS+, включает выполняемую команду, дату выполнения и имя пользователя, который ввел команду. Учет команд не поддерживается в RADIUS.

Следующий пример конфигурации разрешает учет команд AAA для команд EXEC, введенных на уровне привилегий 0, 1 и 15. Эта конфигурация построена на основе предыдущих примеров, включая конфигурацию серверов TACACS.

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

В материале Configuring Accounting (Настройка учета) можно получить дополнительные сведения о настройке учета AAA.

Резервные серверы AAA

Серверы AAA, которые задействованы в среде, должны иметь избыточность и развертываться в отказоустойчивой конфигурации. Это позволит гарантировать, что интерактивный доступ управления, например SSH, возможен даже в случае, если сервер AAA недоступен.

При разработке или внедрении резервируемого решения для сервера AAA учитывайте

следующие факторы:

- Доступность серверов AAA во время возможных отказов сети
- Географически распределенное размещение серверов AAA
- Нагрузка на отдельные серверы AAA в стабильном состоянии и в условиях отказа
- Задержка в сети между серверами доступа к сети и серверами AAA
- Синхронизация баз данных серверов AAA

Дополнительную информацию см. в материале Deploy the Access Control Servers (Развертывание серверов управления доступом).

Защита протокола SNMP

В этом разделе описано несколько методов, которые могут использоваться для обеспечения защиты развертываний SNMP на устройствах IOS. Важно обеспечить надежную защиту SNMP для обеспечения конфиденциальности, целостности и доступности как сетевых данных, так и сетевых устройств, через которые пересылаются эти данные. Протокол SNMP предоставляет полную информацию о работоспособности сетевых устройств. Эта информация должна быть защищена от злоумышленников, которые могут использовать эти данные для атак на сеть.

Строки имени и пароля SNMP

Строки имени и пароля содержат пароли, действующие на устройстве IOS для ограничения доступа, доступа только для чтения и для чтения-записи, к данным SNMP на устройстве. Эти строки, как и все пароли, следует тщательно выбирать, чтобы их было нельзя легко угадать. Строки имени и пароля должны регулярно меняться в соответствии с политиками сетевой безопасности. Например, когда администратор сети меняет должность или покидает компанию, необходимо менять строки.

Следующие параметры настройки задают строку имени и пароля только для чтения и строку имени и пароля для чтения и записи:

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
```

```
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

> **Примечание. Предыдущие примеры строк имени и пароля были выбраны, чтобы ясно объяснить их использование.** Для производственных целей строки имени и пароля необходимо выбирать внимательно, они должны состоять из алфавитных, числовых и неалфавитно-цифровых символов. [В материале Recommendations for Creating Strong Passwords (Рекомендации по созданию стойких паролей) можно получить дополнительную информацию о выборе нетривиальных паролей.]

Дополнительную информацию об этой функции см. в разделе IOS SNMP Command Reference (Справочник по командам IOS SNMP).

Строки имени и пароля SNMP со списками ACL

В дополнение к строке имени и пароля необходимо применять ACL, чтобы еще больше ограничить доступ SNMP к избранной группе исходных IP-адресов. Следующая конфигурация ограничивает доступ только на чтение SNMP устройствами конечного хоста, которые находятся в подсети 192.168.100.0/24, и ограничивает доступ для чтения-записи SNMP только устройствами конечного хоста по адресу 192.168.100.1.

> **Примечание. Устройствам, которые разрешены этими списками контроля доступа ACL, требуется надлежащая строка имени и пароля для доступа к запрашиваемой информации SNMP.**

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!
```

```
ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

В разделе snmp-server community справочника по командам управления сетью Cisco IOS можно получить дополнительную информацию об этой функции.

Инфраструктурные списки ACL

Можно развернуть инфраструктурные списки ACL (iACL), которые позволяют гарантировать, что только конечные хосты с доверенными IP-адресами смогут отправлять трафик SNMP устройству IOS. IACL должен содержать политику, которая запрещает неавторизованные пакеты SNMP по порту 161 UDP.

В разделе Ограничение доступа к сети с помощью инфраструктурных списков ACL данного документа можно получить дополнительную информацию об использовании iACL.

Представления SNMP

Представления SNMP являются функцией безопасности, которая может разрешать или запрещать доступ к определенным MIB SNMP. **Как только представление создано и применено к строке имени и пароля с помощью команды глобальной настройки snmp-server community, при доступе к данным MIB вы ограничены разрешениями, определяемыми представлением.** Когда это уместно, рекомендуется использовать представления для ограничения доступа пользователей к необходимым им данным SNMP.

Следующий пример конфигурации ограничивает доступ SNMP со строкой имени и пароля LIMITED к данным MIB в группе систем:

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
```

```
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

Дополнительную информацию см. в материале Configuring SNMP Support (Настройка поддержки SNMP).

Протокол SNMP версии 3

SNMP версии 3 (SNMPv3) определяется RFC3410, RFC3411, RFC3412, RFC3413, RFC3414 и RFC3415 и является совместимым стандартным протоколом для управления сетью. SNMPv3 обеспечивает защищенный доступ устройствам, так как производит аутентификацию и может выполнять шифрование пакетов, проходящих по сети. Там, где поддерживается SNMPv3, его можно использовать для создания другого уровня безопасности при развертывании SNMP. SNMPv3 состоит из трех основных вариантов конфигурации:

- **no auth — этот режим не требует ни аутентификации, ни шифрования пакетов SNMP**
- **auth —** Этот режим требует аутентификации пакета SNMP без шифрования
- **priv — этот режим требует как аутентификации, так и шифрования (конфиденциальности) каждого пакета SNMP**

При использовании механизмов обеспечения безопасности SNMPv3 — аутентификации или аутентификации и шифрования — для обработки пакетов SNMP должен существовать заслуживающий доверия идентификатор механизма; по умолчанию идентификатор механизма генерируется локально. **Идентификатор механизма можно вывести с помощью команды show snmp engineID, как показано в следующем примере:**

```
router#show snmp engineID
Local SNMP engineID: 800000090300000152BD35496
Remote Engine ID IP-addr Port
```

> **Примечание. Если engineID изменится, то все учетные записи пользователя SNMP должны быть перенастроены.**

Следующим шагом нужно настроить группу SNMPv3. **Эта команда настраивает устройство на базе Cisco IOS для SNMPv3 с группой серверов SNMP AUTHGROUP и включает только аутентификацию для этой группы с ключевым словом auth:**

```
router#show snmp engineID
Local SNMP engineID: 80000009030000152BD35496
Remote Engine ID IP-addr Port
```

Эта команда настраивает устройство на базе Cisco IOS для SNMPv3 с группой серверов SNMP PRIVGROUP и включает аутентификацию и шифрование для этой группы с ключевым словом priv:

```
router#show snmp engineID
Local SNMP engineID: 80000009030000152BD35496
Remote Engine ID IP-addr Port
```

Эта команда настраивает пользователя SNMPv3 snmpv3user с аутентификацией MD5 по паролю authpassword и шифрованием 3DES по паролю privpassword:

```
router#show snmp engineID
Local SNMP engineID: 80000009030000152BD35496
Remote Engine ID IP-addr Port
```

Обратите внимание, что команды настройки snmp-server user не отображаются в выходных данных конфигурации устройства, как требует RFC 3414; поэтому пароль пользователя недоступен для просмотра в файле конфигурации. **Для просмотра настроенных пользователей введите команду show snmp user, как показано в следующем примере:**

```
router#show snmp user
User name: snmpv3user
Engine ID: 80000009030000152BD35496
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: 3DES
Group-name: PRIVGROUP
```

В материале Configuring SNMP Support (Настройка поддержки SNMP) можно получить дополнительную информацию об этой функции.

Защита уровня администрирования

Функция защиты уровня администрирования (MPP) в программном обеспечении Cisco IOS поможет обеспечить защиту SNMP, так как ограничивает интерфейсы, через которые трафик SNMP может завершиться на устройстве. Функция MPP позволяет администратору определить один или несколько интерфейсов в качестве интерфейсов администрирования. Трафику администрирования разрешен вход в устройство только через эти интерфейсы. После того как MPP включен, никакие интерфейсы, кроме назначенных интерфейсов администрирования, не принимают трафик администрирования сети, предназначенный для устройства.

Обратите внимание, что MPP является подмножеством функции CPPr и требует версии IOS, которая поддерживает CPPr. [В разделе Understanding Control Plane Protection (Общие сведения о защите уровня управления) можно получить дополнительную информацию о CPPr.]

В данном примере MPP служит для ограничения доступа SNMP и SSH только интерфейсом FastEthernet 0/0:

```
router#show snmp user
User name: snmpv3user
Engine ID: 80000090300000152BD35496
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: 3DES
Group-name: PRIVGROUP
```

В Management Plane Protection Feature Guide (Руководство по функциям защиты уровня администрирования) можно получить дополнительную информацию.

Оптимальные методы ведения журнала

Ведение журнала событий обеспечивает видимость работы устройства Cisco IOS и сети, в которой оно размещено. Программное обеспечение Cisco IOS предусматривает несколько гибких параметров ведения журналов, которые могут помочь в достижении целей обеспечения видимости и управления сетью для организации.

Следующие разделы содержат некоторые основные оптимальные методы ведения журналов, которые помогут администраторам успешно вести журналы и одновременно уменьшить влияние операций по ведению журналов на устройства Cisco IOS.

Отправка журналов в центральное расположение

Рекомендуется отправлять журналы на удаленный сервер syslog. Это обеспечит более эффективную корреляцию и аудит сети и событий, связанных с безопасностью, на сетевых устройствах. Обратите внимание, что сообщения syslog передаются ненадежно через UDP и открытым текстом. Поэтому все меры защиты, которые сеть накладывает на трафик управления (шифрование или доступ по внештатному каналу), должны быть распространены и на трафик syslog.

Следующий пример конфигурации настраивает устройство Cisco IOS для передачи информации журналов на удаленный сервер syslog:

```
router#show snmp user
User name: snmpv3user
Engine ID: 80000090300000152BD35496
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: 3DES
Group-name: PRIVGROUP
```

В материале Identifying Incidents Using Firewall and IOS Router Syslog Events (Выявление инцидентов с использованием межсетевого экрана и событий syslog маршрутизатора IOS) можно получить дополнительную информацию о корреляции журналов.

Функция ведения журналов в локальной энергонезависимой памяти, встроенная в систему в версии 12.4 (15)T, и впервые появившаяся в версии 12.0 (26)S позволяет сохранять сообщения системных журналов на флеш-диске ATA. Сообщения, сохраненные на диске ATA, сохраняются после перезагрузки маршрутизатора.

Следующие параметры настройки задают 134 217 728 байт (128 Мбайт) сообщений журналов в каталоге syslog на флеш-памяти ATA (disk0), указывая размер файла 16 384 байта:

```
router#show snmp user
User name: snmpv3user
Engine ID: 80000009030000152BD35496
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: 3DES
Group-name: PRIVGROUP
```

Прежде чем записать сообщения журнала в файл на диске ATA, программное обеспечение Cisco IOS проверяет наличие свободного места. Если места недостаточно, самый старый (по метке времени) файл журнала удаляется, а затем сохраняется текущий. **Формат имени файла: log_month:day:year:: time.**

> **Примечание. Флеш-накопитель ATA ограничивает дисковое пространство и поэтому требует обслуживания, чтобы избежать перезаписи сохраненных данных.**

Данный пример показывает, как скопировать сообщения журналов с флеш-диска ATA на маршрутизаторе на внешний диск на FTP-сервере 192.168.1.129 в рамках процедуры технического обслуживания:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

В материале Logging to Local Nonvolatile Storage (ATA Disk) (Ведение журнала в локальной энергонезависимой памяти (диск ATA)) можно получить дополнительную информацию об этой функции.

Уровень регистрации

Каждому сообщению журнала, которое создается устройством Cisco IOS, назначается одна из восьми степеней серьезности ошибки, от 0 (аварийная ситуация) до 7 (отладка). Если не требуется особо, рекомендуется избегать вывода в журнал сообщений уровня 7. Вывод в журнал сообщений уровня 7 повышает нагрузку на ЦП устройства, что может привести к нестабильной работе устройства и сети.

Команда глобальной конфигурации logging trap служит для указания того, какие сообщения журнала передаются удаленным серверам syslog. Заданный уровень указывает самую низкую степень серьезности ошибки, которая передается. **Для ведения журнала с буферизацией используется команда уровня logging buffered.**

Следующий пример конфигурации ограничивает сообщения журнала, которые отправляются удаленным серверам syslog и в локальный буфер журнала для степеней серьезности ошибки от 6 (информационные) до 0 (аварийные ситуации):

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Дополнительную информацию см. в разделе Troubleshooting, Fault Management, and Logging (Устранение проблем, защита от сбоев и ведение журналов).

Отказ от входа в сеансы консоли или монитора

Программное обеспечение Cisco IOS позволяет отправлять сообщения журнала в сеансы мониторинга, которые представляют собой интерактивные сеансы управления, в которых была выполнена EXEC-команда terminal monitor, и на консоль. Однако это может увеличить нагрузку на ЦП устройства IOS и поэтому не рекомендуется. **Вместо этого рекомендуется отправлять информацию журналов в локальный буфер журнала, который можно просмотреть с помощью команды show logging.**

Используйте команды глобальной конфигурации no logging console и no logging monitor для отключения ведения журнала на консоли и в сеансе мониторинга. Следующий пример конфигурации показывает использование этих команд:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

В разделе Cisco IOS Network Management Command Reference (Справочник по командам управления сетью Cisco IOS) можно получить дополнительную информацию о командах глобальной конфигурации.

Ведение журнала с буферизацией

Программное обеспечение Cisco IOS поддерживает использование локального буфера журнала, позволяя администратору просматривать локально созданные сообщения журнала. Ведение журнала с буферизацией настоятельно рекомендуется использовать вместо вывода журнала на консоль или в сеанс мониторинга.

Существует два параметра конфигурации, связанные с настройкой ведения журнала с буферизацией: размер буфера журнала и важность сообщений, сохраняемых в буфере. **Размер буфера журнала настраивается с помощью команды глобальной конфигурации logging buffered.** Самая низкая степень серьезности ошибки, помещаемой в буфер, настраивается с помощью команды logging buffered severity. **Администратор может просмотреть содержимое буфера журнала с помощью EXEC-команды show logging.**

Следующий пример конфигурации включает конфигурацию буфера журнала 16 384 байта, а также уровень серьезности 6 (информационные сообщения), который указывает, что сохраняются сообщения уровней от 0 (аварийные ситуации) до 6 (информационные сообщения):

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

В разделе Cisco IOS Network Management Command Reference (Справочник по командам управления сетью Cisco IOS) можно получить дополнительную информацию о ведении журнала с буферизацией.

Настройка интерфейса источника журнала

Для повышения уровня согласованности при сборе и просмотре сообщений журнала рекомендуется статически настроить все интерфейсы источников журналов. **Выполняемая с помощью команды интерфейса logging source-interface статическая настройка интерфейса источников журналов гарантирует, что один и тот же IP-адрес будет указан во всех сообщениях журнала, передаваемых от каждого конкретного устройства Cisco IOS.** Для повышения устойчивости рекомендуется использовать интерфейс обратной связи в

качестве источника журналов.

Следующий пример конфигурации иллюстрирует использование команды глобальной конфигурации интерфейса logging source-interface для указания IP-адреса интерфейса loopback 0 для всех сообщений журнала:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Для получения дополнительной информации см. Cisco IOS Command Reference (Справочник по командам Cisco IOS).

Настройка меток времени ведения журнала

Настройка меток времени ведения журнала поможет обеспечить корреляцию событий между сетевыми устройствами. Важно реализовать правильную и последовательную конфигурацию меток времени ведения журнала, чтобы сопоставлять данные журналов. Метки времени ведения журнала должны быть настроены так, чтобы включать дату и время с точностью до миллисекунд, а также часовой пояс, используемый на устройстве.

Следующий пример включает конфигурацию меток времени ведения журнала с точностью до миллисекунд в часовом поясе UTC:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Если вы предпочитаете не выводить в журнал время UTC, то можно настроить конкретный локальный часовой пояс, а затем назначить эту информацию для вывода в сообщения создаваемого журнала. Следующий пример показывает конфигурацию устройства для часового пояса PST:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Управление конфигурацией программного обеспечения Cisco IOS

Программное обеспечение Cisco IOS располагает рядом функций, которые могут включить форму управления конфигурацией на устройстве Cisco IOS. Они позволяют архивировать конфигурации и откатывать их к предыдущей версии, а также выводить подробные журналы изменений конфигурации.

Замена конфигурации и откат конфигурации

В программном обеспечении Cisco IOS версии 12.3(7)T и более поздних функция замены и отката конфигурации позволяет архивировать конфигурацию устройства Cisco IOS на устройстве. Конфигурации в этом архиве, охраняемые вручную или автоматически, могут использоваться для замены текущей рабочей конфигурации с помощью команды имени файла configure replace. В этом состоит отличие от команды copy filename running-config. Команда configure replace filename заменяет рабочую конфигурацию, в отличие от слияния, выполняемого командой copy.

Рекомендуется включать эту функцию на всех устройствах Cisco IOS в сети. После включения администратор может добавлять текущую рабочую конфигурацию в архив с помощью привилегированной EXEC-команды archive config. Просмотреть архивные конфигурации можно с помощью команды show archive.

Следующий пример иллюстрирует настройку автоматического архивирования конфигурации. Следующий пример указывает устройству Cisco IOS сохранять архивные конфигурации в виде файлов с именами archived-config-N в файловой системе disk0: поддерживает не более 14 резервных копий, архивирование производить раз в день (1440 минут) и при выполнении администратором команды write memory.

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Хотя архив конфигурации может хранить до 14 резервных копий конфигурации, рекомендуется рассмотреть требования к свободному месту перед использованием команды maximum.

Исключительный доступ к изменению конфигурации

Функция исключительного доступа к изменению конфигурации появилась в программном обеспечении Cisco IOS версии 12.3(14)T. Она гарантирует, что только один администратор изменяет конфигурацию устройства Cisco IOS в данный момент времени. Эта функция поможет исключить нежелательное воздействие одновременных изменений, вносимых в связанные компоненты конфигурации. Эта функция настраивается с помощью команды глобальной конфигурации configuration mode exclusive и работает в одном из двух режимов: auto и manual. Когда администратор выполняет команду configure terminal в режиме auto, конфигурация автоматически блокируется. В режиме manual администратор использует команду configure terminal lock для блокировки конфигурации, когда входит в режим конфигурации.

Следующий пример иллюстрирует настройку функции автоматической блокировки конфигурации:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Эластичная конфигурация программного обеспечения Cisco IOS

Функция эластичной конфигурации, которая появилась в программном обеспечении Cisco IOS версии 12.3(8)T, позволяет надежно сохранить копию образа ПО Cisco IOS и конфигурации устройства, которые в настоящее время используются устройством Cisco IOS. Когда эта функция включена, невозможно изменить или удалить эти файлы резервных копией. Рекомендуется включать эту функцию для предотвращения непреднамеренных и злонамеренных попыток удалить эти файлы.

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Когда эта функция включена, можно восстановить удаленную конфигурацию или образ ПО Cisco IOS. Текущее состояние этой функции можно вывести с помощью команды show secure boot.

Цифровая подпись программного обеспечения Cisco

Цифровая подпись программного обеспечения Cisco, появившаяся в программном обеспечении Cisco IOS версии 15.0(1)M для маршрутизаторов Cisco 1900, 2900 и 3900, упрощает использование снабженного цифровой подписью и потому доверенного программного обеспечения Cisco IOS с применением надежного, асимметричного (с

открытым ключом) шифрования.

Цифровая подпись программного обеспечения Cisco включает зашифрованный (секретным ключом) собственный хеш. При проверке устройство дешифрует хеш с соответствующим открытым ключом из ключей, содержащихся в его базе ключей, а также вычисляет свой собственный хеш образа. Если дешифрованный хеш совпадает с вычисленным хешем образа, то образ не изменялся и ему можно доверять.

Ключи цифровой подписи программного обеспечения Cisco определяются типом и версией ключа. Ключ может быть специальным, производственным или переходным (rollover). Производственные и специальные ключи имеют версию ключа, которая увеличивается в алфавитном порядке при каждом отзыве и замене ключа. Когда используется цифровая подпись программного обеспечения Cisco, ROMMON и обычные образы Cisco IOS подписываются специальным или производственным ключом. Образ ROMMON обновляется и должен подписываться тем же ключом, что и загруженный специальный или производственный образ.

Следующая команда проверяет целостность образа c3900-universalk9-mz. SSA во флеш-памяти с ключами в хранилище ключей устройства:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Снабженная цифровой подписью функция Программного обеспечения Cisco была также интегрирована в Выпуске Cisco IOS XE 3.1.0.SG для Cisco Catalyst Коммутаторы серии E 4500.

В материале Digitally Signed Cisco Software (Цифровая подпись программного обеспечения Cisco) можно найти дополнительную информацию об этой функции.

В программном обеспечении Cisco IOS версии 15.1(1)T и позже появилась замена ключа цифровой подписи программного обеспечения Cisco. При замене и аннулировании ключа происходит замена и удаление ключа для проверки цифровой подписи программного обеспечения Cisco в хранилище ключей платформы. Только специальные и производственные ключи могут быть отозваны в случае компрометации.

Новые (специальные или производственные) ключи для образа (производственного или отзыва) включены в этот образ и используются для отмены предыдущего специального или производственного ключа. Целостность образа отзыва проверяется с помощью переходного (rollover) ключа, который предварительно сохранен на платформе. Переходный (rollover) ключ не изменяется. При отзыве производственного ключа после загрузки образа отзыва новый ключ, который он содержит, добавляется в хранилище ключей, а соответствующий старый ключ может быть отозван при обновлении образа ROMMON и загрузки с нового производственного образа. При отзыве специального ключа загружается производственный образ. Этот образ добавляет новый специальный ключ и может отозвать старый специальный ключ. После обновления ROMMON может быть выполнена загрузка с использованием нового специального образа.

Следующий пример описывает отзыв специального ключа. Следующие команды добавляют новый специальный ключ в хранилище ключей из текущего производственного образа, копируют новый образ ROMMON (C3900_rom-monitor.srec. SSB) в область хранилища (usbflash0:), обновляют файл ROMMON и отзывают старый специальный ключ:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Новый специальный образ (c3900-universalk9-mz. SSB) после этого может быть скопирован на флеш-память для загрузки и проверки подписи с использованием ранее добавленного специального ключа (.SSB):

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Отзыв и замена ключа не поддерживаются на коммутаторах Catalyst 4500 серии E, где работает программное обеспечение Cisco IOS XE, хотя эти коммутаторы поддерживают цифровую подпись программного обеспечения Cisco.

В разделе the Digitally Signed Cisco Software Key Revocation and Replacement (Отзыв и замена цифровой подписи программного обеспечения Cisco) руководства Digitally Signed Cisco Software (Цифровая подпись программного обеспечения Cisco) можно получить дополнительную информацию об этой функции.

Ведение журнала и уведомление об изменении конфигурации

Функция ведения журнала и уведомления об изменении конфигурации, которая появилась в программном обеспечении Cisco IOS версии 12.3(4)T, позволяет вести журнал изменений конфигурации устройства Cisco IOS. Журнал ведется на устройстве Cisco IOS и содержит сведения о пользователе, внесшем изменение, введенную команду конфигурации и время, когда изменение было внесено. **Эта функциональность включается командой режима настройки регистратора изменения конфигурации logging enable. Опциональные команды hidekeys и logging size служат для улучшения конфигурации по умолчанию, так как предотвращают вывод в журнал данных пароля и увеличивают размер журнала изменений.**

Рекомендуется включить эту функциональность, чтобы история изменений конфигурации устройства Cisco IOS была более понятной. **Кроме того, рекомендуется выполнить команду notify syslog, чтобы включить формирование сообщений syslog при внесении изменений в конфигурацию.**

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

После включения функции ведения журнала и уведомления об изменении конфигурации можно с помощью привилегированной EXEC-команды show archive log config all просматривать журнал конфигурации.

Плоскость управления

Функции уровня управления состоят из протоколов и процессов, которые выполняют обмен данными между сетевыми устройствами для их передачи от источника до назначения. К ним относятся протоколы маршрутизации, например Border Gateway Protocol (BGP), а также протоколы вроде ICMP и RSVP.

Важно, чтобы события на уровнях администрирования и передачи данных не оказывали негативного влияния на уровень управления. Если событие уровня передачи данных, например DoS-атака, влияет на уровень управления, то вся сеть может стать нестабильной. Эта информация о функциях ПО Cisco IOS и конфигурациях поможет обеспечить эластичность уровня управления.

Общая защита уровня управления

Защита плоскости контроля сетевого устройства имеет решающую важность, так как плоскость контроля гарантирует, что плоскости управления и данных останутся в рабочем состоянии. Если уровень управления становится нестабильным в результате события безопасности, то, возможно, не удастся восстановить устойчивость сети.

Во многих случаях можно отключить прием и передачу определенных типов сообщений на интерфейсе для минимизации нагрузки на ЦП, которая возникает из-за необходимости обработки ненужных пакетов.

Переадресации IP ICMP

Сообщение переадресации ICMP может быть создано маршрутизатором, когда отправка и получение пакета производятся одним и тем же интерфейсом. В этом случае маршрутизатор пересылает пакет и отправляет сообщение переадресации ICMP отправителю исходного пакета. Это позволяет отправителю обойти маршрутизатор и отправлять последующие пакеты непосредственно получателю (или на маршрутизатор, находящийся ближе к получателю). В правильно функционирующей IP-сети маршрутизатор отправляет перенаправления только хостам, которые находятся в его локальных подсетях. Иными словами, переадресация ICMP не должна пересекать границу уровня 3.

Существует два типа сообщений переадресации ICMP: перенаправление на адрес хоста и перенаправление на всю подсеть. Злоумышленник может использовать способность маршрутизатора отправлять переадресацию ICMP, непрерывно передавая маршрутизатору пакеты и вынуждая его отправлять сообщения переадресации ICMP, что может повлиять на загрузку ЦП и производительность работы маршрутизатора. **Для того чтобы предотвратить отправку сообщений переадресации ICMP маршрутизатором, выполните команду конфигурации интерфейса no ip redirects.**

Недостижимые ICMP

Фильтрация по списку доступа интерфейса вызывает отправку сообщений о недоступности ICMP источнику фильтруемого трафика. Формирование этих сообщений может увеличить загрузку на ЦП устройства. В программном обеспечении Cisco IOS формирование сообщения о недоступности ICMP по умолчанию ограничена одним пакетом один раз в 500 миллисекунд. **Формирование сообщения о недоступности ICMP можно отключить с помощью команды настройки интерфейса no ip unreachables. Ограничение частоты отправки сообщений о недоступности ICMP по умолчанию можно изменить с помощью команды ip icmp rate-limit unreachable interval-in-ms.**

Протокол прокси-ARP

Прокси ARP — технология, в которой одно устройство, обычно маршрутизатор, отвечает на запросы ARP, которые предназначены для другого устройства. За счет "подделки" своей идентификации маршрутизатор принимает на себя ответственность за маршрутизацию пакетов к "реальному" пункту назначения. Агент ARP позволяет компьютерам подсети получить доступ к удаленным подсетям без настройки маршрутизации или шлюза по умолчанию. [Протокол прокси-ARP описан в разделе RFC 1027 .]

Существует несколько недостатков использования прокси-ARP. Это может привести к

увеличению объема трафика ARP в сегменте сети и истощению ресурсов, а также к атакам по перехвату и изменению передаваемых данных. Прокси-ARP представляет вектор атаки истощения ресурсов, так как каждый обработанный запрос ARP занимает небольшой объем памяти. Злоумышленник сможет занять всю доступную память, отправляя огромное число запросов ARP.

Атаки по перехвату и возможному изменению передаваемых данных позволяют хосту в сети имитировать MAC-адрес маршрутизатора, и ничего не подозревающие хосты передают трафик злоумышленнику. **Прокси-ARP можно отключить с помощью команды конфигурации интерфейса no ip proxy-arp.**

В материале Enabling Proxy ARP (Включение прокси-ARP) можно найти дополнительную информацию об этой функции.

Ограничение влияния трафика уровня управления на ЦП

Защита уровня управления имеет очень важное значение. Поскольку производительность приложения и производительность конечного пользователя могут пострадать без трафика данных и администрирования, жизнеспособность уровня управления гарантирует, что два других уровня поддерживаются в рабочем состоянии.

Общие сведения о трафике уровня управления

Для надлежащей защиты уровня управления устройством Cisco IOS важно понимать типы трафика, коммутируемого процессором. Коммутируемый трафик обычно состоит из двух различных типов трафика. Первый тип трафика направлен к устройству Cisco IOS и должен быть обработан непосредственно процессором устройства Cisco IOS. *Этот трафик состоит из категории Трафик receive-adjacency.* **Этот трафик содержит запись в таблице CEF, где следующий прыжок маршрутизатора является самим устройством, на что указывает наличие термина receive в выходных данных команды show ip cef.** Это указание имеет место для любого IP-адреса, который требует прямой обработки процессором устройства Cisco IOS, и включает IP-адреса интерфейса, адресное пространство для многоадресной пересылки и адресное пространство широковещательных адресов.

Второй тип трафика, который обрабатывается ЦП, является трафиком уровня передачи данных, направленного за пределы устройства Cisco IOS, который требует специальной обработки ЦП. Хотя это не исчерпывающий список типов трафика уровня передачи данных, влияющего на ЦП, для этих типов трафика используется процессорная коммутация, что может повлиять на работу уровня управления:

- **Ведение журнала списка управления доступом. Трафик ведения журналов ACL состоит из пакетов, которые формируются из-за соответствия (разрешено или запрещено) ACE, на котором используется ключевое слово log.**
- **Проверка обратного маршрута IP-пакетов (Unicast RPF)). Используется в сочетании с ACL и может привести к процессорной коммутации определенных пакетов.**
- **Параметры IP. Любые IP-пакеты с параметрами должны обрабатываться ЦП.**
- **Фрагментация. Любой пакет IP, который требует фрагментации, должен быть передан ЦП для обработки.**

- **Истечение срока жизни (TTL) Пакеты, которые имеют значение TTL, меньше того, которое требуется для отправки сообщений ICMP (ICMP тип 11, код 0), или равное ему, передаются на обработку ЦП.**

- **Недостижимый ICMP. Пакеты, которые приводят к формированию сообщений о недоступности ICMP из-за маршрутизации, MTU или фильтрации, передаются на обработку ЦП.**

- **Трафик, требующий запроса ARP. Назначения, для которых не существует записи ARP, требуют обработки ЦП.**

- **Трафик, отличный от IP. Весь трафик, не относящийся к IP, обрабатывается ЦП.**

В этом списке описываются несколько методов определения, какие типы трафика обрабатываются ЦП устройства Cisco IOS:

- **Команда show ip cef выводит информацию о следующем прыжке для каждого префикса IP, содержащегося в таблице CEF.** Как указывалось выше, записи, которые содержат получателя в качестве следующего прыжка, рассматриваются как смежности и указывают, что трафик должен быть передан напрямую ЦП.

- **Команда show interface switching выводит сведения о количестве пакетов, коммутированных устройством.**

- **Команда show ip traffic выводит сведения о количестве пакетов IP:**

  с локальным назначением (то есть трафик receive-adjacency),с параметрамикоторые требуют фрагментациикоторые отправлены в пространство широковещательных адресовкоторые отправлены в адресное пространство многоадресной пересылки

- **Трафик receive-adjacency можно выявить с помощью команды show ip cache flow.** Все потоки, которые направлены к устройству Cisco IOS, имеют локальный интерфейс назначения (DstIf).

- **Политики уровня управления могут использоваться для определения типа и скорости трафика, который достигает уровня управления устройством Cisco IOS. Политики уровня управления могут применяться через списки ACL для детальной классификации, ведение журналов и использование команды show policy-map control-plane.**

Инфраструктурные списки ACL

Инфраструктурные списки ACL (iACL) ограничивают внешний обмен данными с устройствами в сети. Инфраструктурные списки ACL подробно описаны в разделе Ограничение доступа к сети с помощью инфраструктурных списков ACL данного документа.

Рекомендуется реализовать iACL для защиты уровня управления всеми сетевыми устройствами.

Списки ACL для входящего трафика

Для распределенных платформ ACL входящего трафика (rACL) может оказаться подходящим выбором для Cisco IOS версии 12.0 (21) S2 для коммутаторов 12000 (GSR), 12.0 (24) S для 7500 и 12.0 (31) S для 10720. RACL защищает устройство от вредоносного трафика, прежде чем он повлияет на процессор маршрутизатора. ACL входящего трафика предназначен только для защиты устройства, на котором он настроен, а на транзитный трафик не влияет. В результате этого любой IP-адрес назначения, указанный в записях ACL в нижеприведенном примере, относится только к физическим или виртуальным IP-адресам маршрутизатора. ACL входящего трафика также считается оптимальным методом сетевой безопасности и должен рассматриваться как средство долгосрочного обеспечения безопасности сети.

Ниже приведен ACL входящего пути, который записан для разрешения трафика SSH (TCP-порт 22) от надежных хостов в сети 192.168.100.0/24:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

В материале GSR: Receive Access Control Lists (Списки управления доступом для входящего трафика) показано, как определить и разрешить легальный трафик к устройству и запретить все нежелательные пакеты.

CoPP

Функция CoPP также может быть использована для ограничения IP-пакетов, предназначенных устройству инфраструктуры. В данном примере только трафик SSH от надежных хостов достигает ЦП устройства Cisco IOS.

> **Примечание. Отклонение трафика от неизвестных или ненадежных IP-адресов может привести к тому, что хосты с динамически назначаемыми IP-адресами не смогут подключиться к устройству Cisco IOS.**

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

В предыдущем примере CoPP записи ACL, которые совпадают с несанкционированными пакетами со значением permit action, приводят к сбросу этих пакетов функцией policy-map drop, в то время как на пакеты, которые совпадают со значением deny action, функция policy-map drop не влияет.

CoPP доступен в версиях программного обеспечения Cisco IOS Train 12.0S, 12.2SX, 12.2S, 12.3T, 12.4 и 12.4T.

В материале Deploying Control Plane Policing (Развертывание политик уровня управления) можно получить дополнительную информацию о настройке и использовании функции CoPP.

Защита уровня управления

Защита уровня управления (CPPr), которая появилась в программном обеспечении Cisco IOS версии 12.4(4)T, позволяет ограничить или определить политику трафика уровня управления, направляемого процессору устройства Cisco IOS. В отличие от CoPP, CPPr имеет способность ограничить трафик с большой степенью детализации. CPPr делит

объединенный уровень управления на три отдельные категории, которые называются подынтерфейсами. Подынтерфейсы существуют для категорий трафика хоста, транзита и исключений CEF. Кроме того, CPPr включает следующие защитные функции уровня управления:

- **Фильтрация портов. Эта функция обеспечивает применение политик и отбрасывание пакетов, адресованных к закрытому или непрослушивающему порту TCP или UDP.**
- **Пороговое значение очереди. Эта функция ограничивает количество пакетов для указанного протокола, которые разрешено поместить во входящую очередь IP уровня управления.**

В материалах Control Plane Protection (Защита уровня управления) и Understanding Control Plane Protection (CPPr) (Общие сведения о защите уровня управления (CPPr)) можно получить дополнительные сведения о настройке и использовании функции CPPr.

Аппаратные ограничители скорости

Cisco Catalyst Supervisor Engine серии 6500 32 и Supervisor Engine 720 поддерживают определяемые платформой аппаратные ограничители скорости (HWRL) для специальных сетевых сценариев. Такие аппаратные ограничители скорости называются ограничителями скорости особых случаев, так как они покрывают определенный заранее указанный набор сценариев IPv4, IPv6, одноадресных рассылок и многоадресных DoS. HWRL могут защитить устройство Cisco IOS от множества атак, которые требуют обработки пакетов процессором.

Существует несколько HWRL, которые включены по умолчанию. В материале PFC3 Hardware-based Rate Limiter Default Settings (Настройки по умолчанию аппаратного ограничителя скорости PFC3) можно получить дополнительную информацию.

В материале Hardware-Based Rate Limiters on the PFC3 (Аппаратные ограничители скорости на PFC3) можно получить дополнительную информацию о HWRL.

Защищенный BGP

Протокол BGP является основой маршрутизации в Интернете. Поэтому любая организация, даже с очень скромными требованиями к подключению, часто использует BGP. *На BGP часто направлены атаки из-за его повсеместного распространения и подхода настроил и забыл, используемого в настройке конфигурации BGP в небольших организациях.* Но существует много специфичных для BGP функций безопасности, которые могут быть усилены для повышения уровня безопасности BGP.

Здесь представлен обзор наиболее важных функций безопасности BGP. При необходимости приведены рекомендации по настройке.

Обеспечение безопасности на основе TTL

Каждый IP-пакет содержит 1-байтовое поле, которое называется сроком жизни (TTL). Каждое устройство, через которое проходит IP-пакет, уменьшает это значение на единицу. Начальное значение определяется операционной системой и, как правило, находится в пределах от 64 до 255. Когда значение TTL достигает нуля, пакет отбрасывается.

Защита безопасности на основе TTL, которую также называют обобщенным механизмом обеспечения безопасности на основе TTL (GTSM) или средством безопасности TTL BGP (BTSH), использует значение TTL для IP-пакетов, чтобы гарантировать, что пакеты BGP получены от непосредственно подключенного узла. Эта функция часто требует координации одноранговых маршрутизаторов; однако при включении эта функция может полностью устранить многие атаки на основе TCP против BGP.

GTSM для BGP включается с помощью параметра ttl-security команды neighbor настройки маршрутизатора под управлением BGP. Данный пример иллюстрирует настройку этой функции:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

При получении пакетов BGP значение TTL проверяется и должно быть больше или равно 255 минус заданное число прыжков.

Аутентификация одноранговое соединения по протоколу BGP с MD5

Аутентификация одноранговое узла с использованием MD5 создает хеш-код MD5 для каждого пакета, передаваемого в сеансе BGP. В частности, заголовки IP и TCP, полезная нагрузка TCP и секретный ключ используются для создания хеш-кода.

Созданный хеш-код сохраняется в виде параметра TCP 19, который был создан именно с этой целью в документе RFC 2385. Принимающий BGP-спикер использует тот же алгоритм и секретный ключ для регенерации хеш-кода сообщения. Если полученные и вычисленные хеш-коды не совпадают, то пакет отбрасывается.

Аутентификация одноранговое узла с использованием MD5 настраивается с помощью параметра password команды neighbor настройки маршрутизатора под управлением BGP. Использование этой команды иллюстрируется следующим примером:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

В материале Neighbor Router Authentication (Аутентификация соседнего маршрутизатора) можно найти дополнительную информацию об аутентификации одноранговое соединения по протоколу BGP с MD5.

Настройка максимального числа префиксов

Префиксы BGP сохраняются маршрутизатором в памяти. Чем больше префиксов, которые должен хранить маршрутизатор, тем больше памяти занимает BGP. В некоторых конфигурациях может храниться подмножество всех интернет-префиксов, например в конфигурациях, которые используют только маршрут по умолчанию или маршруты для сетей заказчика поставщика.

Для того чтобы предотвратить истощение памяти, важно настроить максимальное число префиксов, принимаемое на каждом узле. Рекомендуется задать ограничение для каждого узла BGP.

При настройке этой функции с помощью команды настройки маршрутизатора под управлением BGP neighbor maximum-prefix один аргумент является обязательным: максимальное число префиксов, которые принимаются перед завершением работы узла.

Можно также ввести число от 1 до 100. Это число представляет процент от значения максимального числа префиксов, при котором отправляется сообщение в журнал.

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

В материале Configuring the BGP Maximum-Prefix Feature (Настройка максимального префикса BGP) можно найти дополнительную информацию о максимальном количестве префиксов на узел.

Фильтрация префиксов BGP с помощью списков префиксов

Списки префиксов позволяют администратору сети разрешать или запрещать определенные префиксы, отправка и получение которых производится через BGP. Списки префиксов должны использоваться, когда возможно, чтобы обеспечить передачу сетевого трафика по намеченным путям. Списки префиксов должны применяться к каждому узлу eBGP на входящем и исходящих направлениях.

Настроенные списки префиксов ограничивают префиксы, которые передаются или принимаются специально разрешенными политикой маршрутизации сети. Если этого не происходит из-за большого числа получаемых префиксов, то список префиксов нужно настроить для блокирования известных плохих префиксов. Плохие префиксы включают невыделенное адресное пространство IP и сети, которые зарезервированы для внутреннего использования или целей тестирования в соответствии с RFC 3330. Списки исходящих префиксов должны быть настроены так, чтобы разрешить только префиксы, которые организация намеревается объявить.

Следующий пример конфигурации использует списки префиксов для ограничения маршрутов, которые изучены и объявлены. В частности, только маршрут по умолчанию разрешен входящим списком префиксов BGP-PL-INBOUND, а префикс 192.168.2.0/24 является единственным маршрутом, разрешенным для объявления BGP-PL-OUTBOUND.

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

В материале Connecting to a Service Provider Using External BGP (Подключение к поставщику услуг с использованием внешнего BGP) можно найти полный обзор фильтрации префиксов BGP.

Фильтрация префиксов BGP с помощью списков доступа к пути автономной системы

Списки доступа BGP к путям автономной системы (AS) позволяют пользователю фильтровать полученные и объявленные префиксы на основе атрибута AS-path префикса. Это может сочетаться со списками префиксов для задания надежного набора фильтров.

Следующий пример конфигурации использует списки доступа путей AS для ограничения входящих префиксов формируемыми удаленным AS и исходящими префиксами, формируемыми локальной автономной системой. Префиксы, которые получены от всех других автономных систем, фильтруются и не устанавливаются в таблицу маршрутизации.

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Защищенные протоколы внутреннего шлюза

Способность сети правильно передавать трафик и восстановиться после изменения топологии или отказов зависит от точного представления топологии. Для получения такого представления часто используют протокол IGP. По умолчанию IGP являются динамическими и обнаруживают дополнительные маршрутизаторы, которые обмениваются данными с конкретным используемым IGP. IGP также обнаруживают маршруты, которые могут использоваться во время отказа сетевого подключения.

Следующие подразделы содержат обзор наиболее важных функций безопасности IGP. В надлежащих случаях предоставлены рекомендации и примеры, относящиеся к версии 2 (RIPv2) протокола RIP (Routing Information Protocol), протоколу EIGRP и протоколу OSPF.

Аутентификация и проверка протокола маршрутизации с использованием алгоритма хеширования MD5

Невозможность защиты обмена данными о маршрутизации позволяет злоумышленнику водить ложные сведения о маршрутизации в сеть. Использование аутентификации по паролю с протоколами маршрутизации между маршрутизаторами может повысить безопасность сети. Но поскольку аутентификация передается в виде открытого текста, злоумышленник может обойти контроль безопасности.

Благодаря алгоритму хеширования MD5, применяемому в процессе проверки подлинности, обновления маршрута более не содержат незашифрованных паролей, а все содержимое обновления маршрута более устойчиво к вмешательству. Но аутентификация MD5 все еще восприимчива к грубой силе и подбору пароля по словарю, если назначен слабый пароль. Рекомендуется использовать пароли с достаточной рандомизацией. Поскольку аутентификация MD5 гораздо безопаснее, чем аутентификация с использованием пароля, следующие примеры относятся к аутентификации MD5. Может также использоваться IPSec для проверки и защиты протоколов маршрутизации, однако в этих примерах его использование не детализируется.

EIGRP и RIPv2 используют цепочки ключей как часть конфигурации. *В материале key можно получить дополнительную информацию о настройке и использовании цепочек ключей.*

Ниже приведен пример конфигурации для аутентификации маршрутизатора EIGRP с использованием MD5:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Ниже приведен пример конфигурации аутентификации MD5 для RIPv2. RIPv1 не поддерживает аутентификацию.

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Ниже приведен пример конфигурации для аутентификации маршрутизатора OSPF с использованием MD5. OSPF не использует цепочки ключей.

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Дополнительную информацию см. в материале Configuring OSPF (Настройка OSPF).

Команды пассивного интерфейса

С утечкой информации или вводом ложной информации в IGP можно бороться за счет использования команды passive-interface, которая поможет управлять объявлением информации о маршрутизации. Рекомендуется не объявлять в сетях любую информацию вне рамок вашего административного контроля.

Данный пример демонстрирует использование этой функции:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Фильтрование маршрутов

Для сокращения возможности предоставления ложных сведений о маршрутизации в сети необходимо использовать фильтрацию маршрута. **В отличие от команды настройки маршрутизатора passive-interface, маршрутизация происходит на интерфейсах, как только фильтрация маршрута включена, но информация, которая объявляется или обрабатывается, ограниченна.**

Для EIGRP и RIP использование команды distribute-list с ключевым словом out ограничивает объявление информации, тогда как ключевое слово in ограничивает обработку обновлений. Команда distribute-list доступна для OSPF, но не препятствует распространению маршрутизатором фильтруемых маршрутов. Вместо этого должна использоваться команда area filter-list.

Следующий пример EIGRP фильтрует исходящие объявления с помощью команды distribute-list и списка префиксов:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Следующий пример EIGRP фильтрует входящие обновления со списком префиксов:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

В материале Configuring IP Routing Protocol-Independent Features (Настройка функции маршрутизации IP, независимых от протокола) можно получить дополнительную информацию о том, как управлять объявлениями и обработкой обновлений маршрута.

Следующий пример OSPF использует список префиксов со специфичной для OSPF командой area filter-list:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Потребление ресурсов процесса маршрутизации

Префиксы протокола маршрутизации сохраняются маршрутизатором в памяти. Чем больше префиксов должен хранить маршрутизатор, тем больше он потребляет ресурсов. Для предотвращения истощения ресурсов важно настроить протокол маршрутизации на ограничение потребления ресурсов. Это возможно для OSPF, если используется функция защиты от перегрузок базы данных состояния канала.

Следующий пример демонстрирует настройку функции защиты от перегрузок базы данных состояний канала OSPF:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

В материале Limiting the Number of Self-Generating LSAs for an OSPF Process (Ограничение количества самогенерируемых LSA для процесса OSPF) можно получить дополнительную информацию о защите от перегрузок базы данных состояний каналов OSPF.

Надежные протоколы резервирования первого сегмента

Протоколы FHRP обеспечивают эластичность и резервирование для устройств, работающих в качестве шлюзов по умолчанию. Эта ситуация и эти протоколы распространены в средах, где пара устройств уровня 3 обеспечивает функциональность шлюза по умолчанию для сегмента сети или набора VLAN, которые содержат серверы или рабочие станции.

Протокол распределения нагрузки для шлюзов (GLBP), протокол HSRP и протокол VRRP являются протоколами FHRP. По умолчанию эти протоколы обмениваются данными с участниками, не прошедшими аутентификацию. Такой тип обмена данными позволяет злоумышленнику представиться устройством FHRP, взяв на себя роль шлюза по умолчанию. Это позволило бы ему произвести атаку по перехвату и возможному изменению передаваемых данных и перехватывать весь трафик пользователя, который выходит из сети.

Для предотвращения такого типа атак все протоколы FHRP, которые поддерживаются программным обеспечением Cisco IOS, включают возможность аутентификации через MD5 или через текстовые строки. Из-за угрозы, которую представляют не прошедшие аутентификацию FHRP, рекомендуется, чтобы экземпляры этих протоколов использовали аутентификацию MD5. Следующий пример конфигурации демонстрирует использование GLBP, HSRP и аутентификации MD5 в VRRP:


```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```


Уровень данных

Несмотря на то что уровень передачи данных отвечает за перенос данных от источника к месту назначения в контексте безопасности, уровень передачи данных является наименее важной из этих трех уровней. Именно по этой причине важнее защитить уровни управления и администрирования, чем уровень передачи данных, при защите сетевого устройства.

Однако на самом уровне передачи данных существует множество функций и параметров конфигурации, которые могут помочь защитить трафик. В следующих разделах подробно описаны эти функции и параметры, которые позволят легко защитить сеть.

Общая защита уровня передачи данных

Большая часть трафика уровня передачи данных проходит по сети, как определено конфигурацией маршрутизации сети. Однако имеется функциональность IP-сети для изменения пути проходящих по ней пакетов. Такие компоненты, как параметры IP, особенно параметр маршрутизации источника, образуют проблему безопасности в современных сетях.

Использование транзитных ACL также относится к мерам защиты уровня передачи данных.

В разделе Фильтрация транзитного трафика с помощью транзитных списков ACL данного документа можно получить дополнительную информацию.

Выборочное удаление IP-параметров

Существует две проблемы безопасности, которые представляют IP-параметры. Трафик, который содержит IP-параметры, должен проходить процессорную коммутацию устройством Cisco IOS, что может привести к повышению нагрузки на ЦП. IP-параметры также включают функциональность для изменения пути, который трафик проходит через сеть, что позволяет обойти средства безопасности.

Из-за этих проблем добавленная команда глобальной конфигурации ip options {drop | ignore} появилась в версиях программного обеспечения Cisco IOS 12.3 (4) T, 12.0 (22) S и 12.2 (25) S. В первом варианте этой команды ip options drop отбрасываются все IP-пакеты, которые содержат IP-параметры, полученные устройством Cisco IOS. Это позволяет избавиться от нагрузки на ЦП и возможности подмены средств защиты, которые могут задействовать IP-параметры.

Второй вариант этой команды ip options ignore настраивает устройство Cisco IOS для игнорирования IP-параметров, которые содержатся в полученных пакетах. Это смягчает угрозы, связанные с IP-параметрами для локального устройства, но может повлиять на нисходящие устройства. **По этой причине настоятельно рекомендуется использовать вариант этой команды drop.** Это показано в следующем примере конфигурации:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Обратите внимание на то, что некоторые протоколы, например RSVP, легитимно используют IP-параметры. На На Эта команда повлияет на функциональность этих протоколов.

После включения выборочного отбрасывания IP-параметров команда show ip traffic может использоваться для определения количества пакетов, отброшенных из-за присутствия IP-параметров. Эта информация указывается в счетчике принудительного сброса.

В материале ACL IP Options Selective Drop (Выборочное отбрасывание IP-параметров ACL) можно получить дополнительную информацию об этой функции.

Отключение маршрутизации IP-адреса отправителя

Маршрутизация IP-адреса отправителя задействует параметры Loose Source Route и Record Route в тандеме либо параметр Strict Source Route наряду с Record Route, чтобы позволить источнику IP-дейтаграммы задать сетевой путь пакета. Эта функциональность может использоваться для того, чтобы направить трафик в обход средств безопасности в сети.

Если параметры IP не были полностью отключены через функцию выборочного отбрасывания IP-параметров, важно, чтобы была отключена маршрутизация IP-источника. **Маршрутизация IP-источника, которая включена по умолчанию во всех выпусках программного обеспечения Cisco IOS, отключается через команду глобальной конфигурации no ip source-route.** Следующий пример конфигурации иллюстрирует использование этой команды:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Отключение переадресации ICMP

Переадресация ICMP служит для информирования сетевого устройства о наличии более эффективного пути до IP-адреса назначения. По умолчанию программное обеспечение Cisco IOS отправляет перенаправление при получении пакета, который должен маршрутизироваться через интерфейс, через который он был получен.

В некоторых случаях злоумышленник может заставить устройство Cisco IOS отправлять множество сообщений переадресации ICMP, что приводит к повышению нагрузки на ЦП. Поэтому рекомендуется отключить передачу переадресации ICMP. **Переадресации ICMP отключаются с помощью команды конфигурации интерфейса no ip redirects, как показано в следующем примере конфигурации:**

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Отключение или ограничение направленных широковещательных IP-рассылок

Направленные широковещательные IP-рассылки позволяют отправлять широковещательные IP-пакеты к удаленной IP-подсети. Как только пакет достигает удаленной сети, передающее IP-устройство передает пакет как широковещательный уровня 2 всем станциям подсети. Эта функциональность широковещательной рассылки используется как усилитель и отражатель в некоторых атаках, в том числе атаке smurf.

В текущих версиях программного обеспечения Cisco IOS эта функциональность по умолчанию отключена; **однако ее можно включить с помощью команды настройки интерфейса ip directed-broadcast.** В версиях программного обеспечения Cisco IOS до 12.0 эта функциональность по умолчанию была включена.

Если сети абсолютно необходима возможность широковещательной рассылки, ее использование должно контролироваться. **В качестве варианта можно воспользоваться списком управления доступом совместно с командой ip directed-broadcast.** Следующий пример конфигурации ограничивает направленные широковещательные рассылки теми пакетами UDP, которые происходят из надежной сети 192.168.1.0/24:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Фильтрация транзитного трафика с помощью транзитных списков ACL

Можно управлять тем, какой трафик следует через сеть, используя для этого транзитные ACL (tACL). В отличие от инфраструктурных списков ACL, которые должны фильтровать трафик, предназначенный для самой сети. Фильтрация, которую реализуют списки tACL, выгодна тогда, когда желательно отфильтровать трафик, направленный к конкретной группе устройств, или трафик, который проходит по сети транзитом.

Этот тип фильтрации традиционно выполняется межсетевыми экранами. Однако есть случаи, когда выгодно выполнять такую фильтрацию на устройстве Cisco IOS в сети, например, если фильтрация нужна, но отсутствует межсетевой экран.

Транзитные списки ACL также подходят для случаев, когда нужно реализовать статические меры защиты от спуфинга.

В разделе Защита от спуфинга данного документа можно получить дополнительную информацию.

Для получения дополнительной информации см. "Транзитные списки контроля доступа: Фильтрация на периферии сети, где можно получить дополнительную информацию о tACL.

Фильтрация пакетов ICMP

Протокол ICMP был разработан как управляющий протокол для IP. Сообщения, которые передаются им, могут иметь далеко идущие общие последствия для протоколов TCP и IP. **ICMP используется сетевыми инструментами ping и traceroute, а также для обнаружения MTU-маршрута;** однако внешний обмен данными ICMP редко необходим для правильной работы сети.

Программное обеспечение Cisco IOS реализует функциональность для специальной фильтрации сообщений ICMP по имени или типу и коду. В данном примере ACL разрешает ICMP из надежных сетей, в то же время блокирует все пакеты ICMP из других источников:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Фильтрация IP-фрагментов

Как подробно описано ранее в разделе Ограничение доступа к сети с помощью инфраструктурных списков ACL данного документа, фильтрация фрагментированных пакетов IP может создать проблему безопасности для устройств.

Из-за неинтуитивной природы обработки IP-фрагментов они часто непреднамеренно разрешаются списками ACL. Фрагментация также часто используется при попытках обойти системы обнаружения атак. Поэтому IP-фрагменты часто используются в атаках и должны быть явным образом отфильтрованы вверху любого настроенного tACL. Показанный ниже ACL включает комплексную фильтрацию IP-фрагментов. Функциональность, показанная в данном примере, должна использоваться в сочетании с функциональностью предыдущих примеров:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

В материале Access Control Lists and IP Fragments (Списки управления доступом и IP-фрагменты) можно получить дополнительную информацию об обработке с помощью ACL фрагментированных пакетов IP.

Поддержка ACL для фильтрации IP-параметров

В программном обеспечении Cisco IOS версии 12.3(4)T и позже поддерживается использование ACL для фильтрации IP-пакетов на основе IP-параметров, которые содержатся в пакете. Присутствие IP-параметров в пакете может указывать на попытку обойти средства безопасности в сети или иным способом изменить транзитные характеристики пакета. Поэтому пакеты с IP-параметрами должны быть отфильтрованы на периферии сети.

Следующий пример должен использоваться с содержимым из предыдущих примеров для включения полной фильтрации пакетов IP, которые содержат параметры IP:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Защита от спуфинга

Во многих атаках используется спуфинг IP-адреса источника, чтобы добиться эффекта или скрыть истинный источник атаки и помешать точно отследить ее путь. Программное обеспечение Cisco IOS предусматривает функции Unicast RPF и IP Source Guard (IPSG) для сдерживания атак, основанных на спуфинге IP-адреса источника. Кроме того, ACL и null-маршрутизация часто развертываются как средство предотвращения спуфинга вручную.

IP Source Guard способствует уменьшению спуфинга для сетей, которые находятся под прямым административным контролем, путем выполнения проверки порта коммутатора, MAC-адреса и адреса источника. Unicast RPF предусматривает проверку исходной сети и может уменьшить атаки спуфинга из сетей, которые не находятся под прямым административным контролем. Защита на уровне портов может использоваться для проверки MAC-адресов на уровне доступа. Протокол DAI противодействует векторам атаки, в которых используется модификация ARP на локальных сегментах.

Unicast RPF

Проверка обратного маршрута IP-пакетов (Unicast RPF) позволяет устройству проверить, что адрес источника переданного пакета достижим через интерфейс, который получил пакет. Нельзя полагаться на Unicast RPF как на единственную защиту от спуфинга. Если соответствующий маршрут возврата к IP-адресу источника существует, поддельные пакеты могли ввести сеть через Unicast RPF-совместимый интерфейс. Пользователь Unicast RPF должен включить технологию Cisco Express Forwarding на каждом устройстве и настроить его для каждого интерфейса.

Unicast RPF можно настроить в одном из двух режимов: свободный или строгий. В случае если применяется асимметричная маршрутизация, предпочтителен свободный режим, поскольку строгий режим, как известно, отбрасывает пакеты в таких ситуациях. **Во время настройки команды настройки интерфейса ip verify ключевое слово any задает свободный режим, а ключевое слово rx задает строгий режим.**

Следующий пример иллюстрирует настройку этой функции:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

В материале Understanding Unicast Reverse Path Forwarding (Общие сведения о проверке обратного маршрута IP-пакетов) можно получить дополнительную информацию о настройке и использовании функции RPF одноадресной пересылки.

Защита от подделки IP-адреса (IP Source Guard)

IP Source Guard является эффективным средством предотвращения спуфинга и может использоваться, если вы управляете интерфейсами 2-го уровня. Защита от подделки IP-адреса использует информацию от отслеживания DHCP для динамической настройки списка контроля доступа порта (PACL) на интерфейсе 2-го уровня, запрещая любой трафик от IP-адресов, которые не имеют привязки в таблице привязки источников IP.

IP Source Guard применима к интерфейсам 2-го уровня, принадлежащим VLAN с

поддержкой отслеживания DHCP. Следующие команды включают анализ DHCP-трафика:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

После того как отслеживание DHCP включено, эти команды включают IPSG:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Защита на уровне порта может быть включена с помощью команды настройки интерфейса ip verify source port security. Это потребует выполнения команды глобальной конфигурации ip dhcp snooping information option; кроме того, DHCP-сервер должен поддерживать опцию 82.

В материале Configuring DHCP features and IP Source Guard (Настройка функций DHCP и IP Source Guard) содержится дополнительная информация об этой функции.

Безопасность портов

Защита портов используется для смягчения спуфинга MAC-адресов на интерфейсе доступа. Защита портов может динамически сохранять MAC-адреса для упрощения начальной конфигурации. Как только защита на уровне порта определила нарушение MAC, она может использовать один из четырех режимов нарушения. Это следующие режимы: защита, ограничение, завершение работы и завершение работы VLAN. В случае если порт только предоставляет доступ для одной рабочей станции с использованием стандартных протоколов, максимальное число 1 может оказаться достаточным. Протоколы, которые задействуют виртуальные MAC-адреса, например HSRP, не работают, если максимальное число имеет значение 1.

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

В материале Configuring Port Security (Настройка защиты на уровне порта) можно получить дополнительную информацию о настройке защиты на уровне порта.

Динамическая проверка ARP

Динамическая проверка ARP (DAI) может использоваться для противодействия атакам внедрения ARP в локальные сегменты. Атака внедрения ARP заключается в том, что злоумышленник передает локальному сегменту ложную информацию об ARP. Эта информация предназначена для повреждения кеша ARP других устройств. Часто взломщик использует внедрение ARP для атаки «злоумышленник в середине».

DAI перехватывает и проверяет связь IP с MAC-адресом для всех пакетов ARP на ненадежных портах. В средах DHCP DAI использует данные, сформированные функцией анализа DHCP-трафика. Пакеты ARP, полученные от доверенных интерфейсов, не проверяются, а недопустимые пакеты от ненадежных интерфейсов отбрасываются. В средах без DHCP требуется использование ACL ARP.

Следующие команды включают анализ DHCP-трафика:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Как только анализ DHCP-трафика включен, эти команды включают DAI:

copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog

В средах DHCP ACL ARP необходимы для включения DAI. Следующий пример демонстрирует базовую конфигурацию DAI с ACL ARP:

copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog

На На DAi можно также включить для каждого интерфейса, где он поддерживается.

copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog

В материале Configuring Dynamic ARP Inspection (Настройка динамической проверки ARP) можно получить дополнительную информацию о настройке DAI.

Списки ACL для защиты от спуфинга

Вручную настроенные ACL могут обеспечить статическую защиту против атак, где используется известное неиспользованное и недоверенное адресное пространство. Обычно эти списки ACL для противодействия спуфингу применяются к входящему трафику на границах сети как компонент большего ACL. Списки ACL для противодействия спуфингу требуют регулярного мониторинга, так как они могут часто изменяться. Спуфинг можно уменьшить в трафике, который исходит из локальной сети, если применить исходящие ACL, которые ограничивают трафик допустимыми локальными адресами.

Данный пример демонстрирует, как ACL могут использоваться для ограничения IP-спуфинга. Следующий ACL применяется для входящего трафика на нужном интерфейсе. ACE, которые входят в этот ACL, не являются исчерпывающими. При настройке этих типов ACL ищите актуальную и полную справочную информацию.

copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog

В материале Configuring Commonly Used IP ACLs (Настройка часто используемых списков IP ACL) можно получить дополнительную информацию о настройке списков управления доступом.

Официальный список невыделенных интернет-адресов ведется компанией Team Cymru. [Дополнительные сведения о фильтрации неиспользуемых адресов доступны на справочной странице Bogon.]

Ограничение влияния трафика уровня передачи данных на ЦП

Основной целью маршрутизаторов и коммутаторов является передача пакетов и кадров через устройство конечному получателю. Эти пакеты, которые проходят через устройства, размещенные по всей сети, могут повлиять на загрузку ЦП устройства. Уровень передачи данных, которая состоит из трафика, который пересылается через сетевое устройство, должен быть защищен, чтобы обеспечить работу уровней управления и администрирования. Если транзитный трафик может заставить устройство обрабатывать трафик коммутации, то это может повлиять на уровень управления устройством, что может привести к сбоям в работе.

Функции и типы трафика, влияющего на загрузку ЦП

Этот список не является исчерпывающим, но включает типы трафика уровня передачи данных, которые требуют специальной обработки ЦП и коммутируются ЦП:

- **Ведение журнала ACL. Трафик ведения журнала ACL состоит из пакетов, которые формируются по соответствию (разрешить или запретить) ACE, где используется ключевое слово log.**
- **Unicast RPF. В сочетании с ACL может привести к процессорной коммутации определенных пакетов.**
- **Параметры IP. Любые IP-пакеты с параметрами должны обрабатываться ЦП.**
- **Фрагментация. Любой пакет IP, который требует фрагментации, должен быть передан ЦП для обработки.**
- **Истечение времени жизни (TTL). Пакеты, которые имеют значение TTL, меньше или равное 1, требуют отправки сообщения ICMP (тип 11, код 0), что приводит к обработке ЦП.**
- **Недостижимые ICMP. Пакеты, которые требуют отправки сообщения о недоступности ICMP из-за маршрутизации, MTU или фильтрации, обрабатываются ЦП.**
- **Трафик, требующий запроса ARP. Назначения, для которых не существует записи ARP, требуют обработки ЦП.**
- **Трафик, отличный от IP. Весь трафик, не относящийся к IP, обрабатывается ЦП.**

В разделе Общая защита уровня передачи данных данного документа можно получить дополнительную информацию о защите уровня передачи данных.

Фильтрация по значению TTL

Можно использовать поддержку ACL для функции фильтрации по значению TTL, которая появилась в программном обеспечении Cisco IOS версии 12.4(2)T, в расширенном списке доступа IP для фильтрации пакетов на основе значения TTL. Эта функция может быть использована для защиты транзитного трафика, получаемого устройством, где значение TTL равно нулю или единице. Фильтрация пакетов на основе значений TTL может также гарантировать, что значение TTL не ниже диаметра сети, таким образом защищая уровень управления нисходящими устройствами, относящимися к инфраструктуре, от атак на основе TTL.

Обратите внимание, что некоторые приложения и программные средства, такие как traceroute, используют TTL для тестовых и диагностических целей. Некоторые протоколы, такие как IGMP, законным образом используют значение TTL, равное 1.

Следующий пример ACL создает политику, которая фильтрует пакеты IP со значением TTL меньше 6.

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

В материале TTL Expiry Attack Identification and Mitigation (Выявление и противодействие

атакам на основе TTL) можно получить дополнительную информацию о фильтрации пакетов на основе значения TTL.

В материале ACL Support for Filtering on TTL Value (Поддержка ACL для фильтрации по значению TTL) можно получить дополнительную информацию об этой функции.

В программном обеспечении Cisco IOS версии 12.4(4)T и более поздних версий гибкий подбор пакетов (FPM) позволяет администратору искать соответствия по произвольным битам пакета. Следующая политика FPM отбрасывает пакеты со значением TTL меньше шести.

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

В материале Flexible Packet Matching (Гибкое сопоставление пакетов) на домашней странице Cisco IOS Flexible Packet Matching можно получить дополнительную информацию об этой функции.

Фильтрация по наличию IP-параметров

В программном обеспечении Cisco IOS версии 12.3(4)T и более поздних можно использовать поддержку ACL для функции фильтрации IP-параметров в именованном, расширенном списке доступа IP для фильтрации IP-пакетов с присутствующими IP-параметрами. Фильтрация IP-пакетов по наличию IP-параметров может также использоваться для того, чтобы предотвратить обработку этих пакетов на уровне ЦП для уровня управления устройствами инфраструктуры.

Обратите внимание, что поддержка ACL для фильтрации по IP-параметрам может использоваться только с именованными, расширенными списками ACL. Нужно также отметить, что RSVP, Multiprotocol Label Switching Traffic Engineering, IGMP версии 2 и 3 и другие протоколы, которые используют пакеты с IP-параметрами, не смогут правильно работать, если пакеты для этих протоколов будут отбрасываться. Если эти протоколы используются в сети, то может использоваться поддержка ACL для фильтрации по IP-параметрам; однако функция выборочного отбрасывания параметров IP ACL будет отбрасывать этот трафик, и эти протоколы не смогут правильно работать. Если нет протоколов, которым требуются IP-параметры, то функция выборочного отбрасывания параметров IP ACL является предпочтительным методом для отбрасывания этих пакетов.

Следующий пример ACL создает политику для фильтрации IP-пакетов, которые содержат IP-параметры:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Следующий пример ACL демонстрирует политику, которая фильтрует IP-пакеты с пятью определенными IP-параметрами. Пакеты, содержащие эти параметры, запрещаются:

- 0 End of Options List (eool)
- 7 Record Route (record-route)
- 68 Time Stamp (timestamp)
- 131 - Loose Source Route (lsr)

- 137 Strict Source Route (ssr)

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

В разделе Общая защита уровня передачи данных данного документа можно получить дополнительную информацию о функции выборочного отбрасывания параметров IP ACL.

Для получения дополнительной информации см. "Транзитные списки контроля доступа: В разделе «Фильтрация на периферии сети» можно получить дополнительную информацию о фильтрации транзитного и граничного трафика.

Еще одной функцией программного обеспечения Cisco IOS, которая может использоваться для фильтрации пакетов с IP-параметрами, является CoPP. В программном обеспечении Cisco IOS версии 12.3(4)T и более поздних версий CoPP позволяет администратору фильтровать поток трафика для пакетов уровня управления. Устройство, которое поддерживает CoPP и поддержку ACL для фильтрации IP-параметров, которое появилось в программном обеспечении Cisco IOS версии 12.3(4)T, может использовать политику списков доступа для фильтрации пакетов, которые содержат IP-параметры.

Эта политика CoPP отбрасывает полученные устройством транзитные пакеты, если присутствуют какие-либо IP-параметры:

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Политика CoPP отбрасывает транзитные пакеты, полученные устройством, если присутствуют следующие IP-параметры:

- 0 End of Options List (eool)
- 7 Record Route (record-route)
- 68 Time Stamp (timestamp)
- 131 - Loose Source Route (lsr)
- 137 Strict Source Route (ssr)

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

В предыдущих политиках CoPP записи списка управления доступом (ACE), которые совпадают с пакетами со значением permit action, приводят к отбрасыванию этих пакетов функцией policy-map drop, тогда как пакеты со значением deny action (не показаны) не подпадали под действие этой функции.

В разделе Deploying Control Plane Policing (Развертывание политик уровня управления) можно получить дополнительную информацию о функции CoPP.

Защита уровня управления

В программном обеспечении Cisco IOS версии 12.4(4)T и позже может использоваться

защита уровня управления (CPPr) для ограничения или определения политики трафика уровня управления процессором устройства Cisco IOS. Будучи похожим на CoPP, CPPr имеет способность ограничивать или определять политику трафика с большей степенью детализации, чем CoPP. CPPr делит объединенный уровень управления на три отдельные категории, которые называются подынтерфейсами: Существуют подынтерфейсы хоста, транзита и исключения CEF.

Следующая политика CPPr отбрасывает транзитные пакеты, полученные устройством, где значение TTL меньше 6, и транзитные или нетранзитные пакеты, полученные устройством, где значение TTL равно 0 или 1. Политика CPPr также отбрасывает пакеты с избранными IP-параметрами, полученные устройством.

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

В предыдущей политике CPPr записи списка управления доступом, которые совпадали с пакетами со значением permit action, приводили к тому, что эти пакеты отбрасывались функцией policy-map drop, тогда как на пакеты со значением deny action (не показаны), эта функция не действовала.

В материалах Understanding Control Plane Protection (Общие сведения о защите уровня управления) и Control Plane Protection (Защита уровня управления) можно получить дополнительную информацию о функции CPPr.

Идентификация и обратная трассировка трафика

Иногда необходимо быстро определить и выполнить обратную трассировку сетевого трафика, особенно во время расследования инцидента или низкой производительности сети. NetFlow и списки ACL для классификации являются двумя основными методами для выполнения этой задачи с помощью программного обеспечения Cisco IOS. NetFlow обеспечивает видимость всего трафика в сети. Кроме того, NetFlow можно внедрить с коллекторами, которые способны показывать долгосрочные тренды и автоматизировать анализ. Списки ACL для классификации являются компонентами ACL и требуют предварительного планирования для указания определенного трафика и ручного вмешательства во время анализа. Следующие разделы содержат краткий обзор каждой функции.

NetFlow

NetFlow выявляет аномалии и сетевую активность, связанную с безопасностью, отслеживая сетевые потоки. Данные NetFlow можно просматривать и анализировать через интерфейс командной строки, либо можно экспортировать данные в коммерческий или бесплатный сборщик данных NetFlow для агрегации и анализа. Сборщики данных NetFlow через построение долгосрочных трендов способны выполнять анализ использования и поведение сети. NetFlow выполняет анализ по определенным атрибутам в IP-пакетах и созданию потоков. Версия 5 является наиболее часто используемой версией NetFlow, однако версия 9 обладает большей расширяемостью. Потоки NetFlow могут создаваться с выборками данных трафика в средах большого объема.

CEF, или распределенный CEF, является предварительным условием для включения NetFlow. NetFlow можно настроить на маршрутизаторах и коммутаторах.

Данный пример иллюстрирует базовую конфигурацию этой функции. **В предыдущих версиях**

программного обеспечения Cisco IOS для включения NetFlow на интерфейсе использовалась команда ip route-cache flow вместо ip flow {ingress | egress}.

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Ниже приведен пример выходных данных NetFlow из командной строки. Атрибут SrcIf может быть полезен при обратной трассировке.

```
router#show ip cache flow
IP packet size distribution (26662860 total packets):
1-32 64 96 128 160 192 224 256 288 320 352 384 416 448 480
.741 .124 .047 .006 .005 .005 .002 .008 .000 .000 .003 .000 .001 .000 .000

512 544 576 1024 1536 2048 2560 3072 3584 4096 4608
.000 .000 .001 .007 .039 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
55 active, 65481 inactive, 1014683 added
41000680 ager polls, 0 flow alloc failures
Active flows timeout in 2 minutes
Inactive flows timeout in 60 seconds
IP Sub Flow Cache, 336520 bytes
110 active, 16274 inactive, 2029366 added, 1014683 added to flow
0 alloc failures, 0 force free
1 chunk, 15 chunks added
last clearing of statistics never
Protocol Total Flows Packets Bytes Packets Active(Sec) Idle(Sec)
-------- Flows /Sec /Flow /Pkt /Sec /Flow /Flow
TCP-Telnet 11512 0.0 15 42 0.2 33.8 44.8
TCP-FTP 5606 0.0 3 45 0.0 59.5 47.1
TCP-FTPD 1075 0.0 13 52 0.0 1.2 61.1
TCP-WWW 77155 0.0 11 530 1.0 13.9 31.5
TCP-SMTP 8913 0.0 2 43 0.0 74.2 44.4
TCP-X 351 0.0 2 40 0.0 0.0 60.8
TCP-BGP 114 0.0 1 40 0.0 0.0 62.4
TCP-NNTP 120 0.0 1 42 0.0 0.7 61.4
TCP-other 556070 0.6 8 318 6.0 8.2 38.3
UDP-DNS 130909 0.1 2 55 0.3 24.0 53.1
UDP-NTP 116213 0.1 1 75 0.1 5.0 58.6
UDP-TFTP 169 0.0 3 51 0.0 15.3 64.2
UDP-Frag 1 0.0 1 1405 0.0 0.0 86.8
UDP-other 86247 0.1 226 29 24.0 31.4 54.3
ICMP 19989 0.0 37 33 0.9 26.0 53.9
IP-other 193 0.0 1 22 0.0 3.0 78.2
Total: 1014637 1.2 26 99 32.8 13.8 43.9

SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts
Gi0/1 192.168.128.21 Local 192.168.128.20 11 CB2B 07AF 3
Gi0/1 192.168.150.60 Gi0/0 10.89.17.146 06 0016 101F 55
Gi0/0 10.89.17.146 Gi0/1 192.168.150.60 06 101F 0016 9
Gi0/1 192.168.150.60 Local 192.168.206.20 01 0000 0303 11
Gi0/0 10.89.17.146 Gi0/1 192.168.150.60 06 07F1 0016 1
```

В материале Cisco IOS NetFlow можно получить дополнительную информацию о возможностях NetFlow.

См. материал An Introduction to Cisco IOS NetFlow - A Technical Overview (Введение в Cisco IOS NetFlow. Технический обзор).

Списки ACL для классификации

Списки ACL для классификации обеспечивают видимость трафика, который проходит через интерфейс. Списки ACL для классификации не меняют политику безопасности сети и, как правило, создаются для классификации отдельных протоколов, адресов отправителей или получателей. Например, ACE, который разрешает весь трафик, может быть разделен по определенным протоколам или портам. Такая более детализированная классификация трафика по определенным ACE поможет обеспечить понимание сетевого трафика, так как каждая категория трафика имеет свой собственный счетчик попаданий. Администратор может также отделить неявный запрет в конце ACL на детализированные ACE, чтобы выявить типы отказанного трафика.

Администратор может ускорить реагирование на инциденты при помощи списка ACL для классификации с помощью команд show access-list и clear ip access-list counters.

Следующий пример иллюстрирует настройку ACL для классификации для определения трафика SMB до запрета по умолчанию:

```
router#show ip cache flow
IP packet size distribution (26662860 total packets):
1-32 64 96 128 160 192 224 256 288 320 352 384 416 448 480
.741 .124 .047 .006 .005 .005 .002 .008 .000 .000 .003 .000 .001 .000 .000

512 544 576 1024 1536 2048 2560 3072 3584 4096 4608
.000 .000 .001 .007 .039 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
55 active, 65481 inactive, 1014683 added
41000680 ager polls, 0 flow alloc failures
Active flows timeout in 2 minutes
Inactive flows timeout in 60 seconds
IP Sub Flow Cache, 336520 bytes
110 active, 16274 inactive, 2029366 added, 1014683 added to flow
0 alloc failures, 0 force free
1 chunk, 15 chunks added
last clearing of statistics never
Protocol Total Flows Packets Bytes Packets Active(Sec) Idle(Sec)
-------- Flows /Sec /Flow /Pkt /Sec /Flow /Flow
TCP-Telnet 11512 0.0 15 42 0.2 33.8 44.8
TCP-FTP 5606 0.0 3 45 0.0 59.5 47.1
TCP-FTPD 1075 0.0 13 52 0.0 1.2 61.1
TCP-WWW 77155 0.0 11 530 1.0 13.9 31.5
TCP-SMTP 8913 0.0 2 43 0.0 74.2 44.4
TCP-X 351 0.0 2 40 0.0 0.0 60.8
TCP-BGP 114 0.0 1 40 0.0 0.0 62.4
TCP-NNTP 120 0.0 1 42 0.0 0.7 61.4
TCP-other 556070 0.6 8 318 6.0 8.2 38.3
UDP-DNS 130909 0.1 2 55 0.3 24.0 53.1
UDP-NTP 116213 0.1 1 75 0.1 5.0 58.6
UDP-TFTP 169 0.0 3 51 0.0 15.3 64.2
UDP-Frag 1 0.0 1 1405 0.0 0.0 86.8
UDP-other 86247 0.1 226 29 24.0 31.4 54.3
ICMP 19989 0.0 37 33 0.9 26.0 53.9
IP-other 193 0.0 1 22 0.0 3.0 78.2
Total: 1014637 1.2 26 99 32.8 13.8 43.9

SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts
Gi0/1 192.168.128.21 Local 192.168.128.20 11 CB2B 07AF 3
Gi0/1 192.168.150.60 Gi0/0 10.89.17.146 06 0016 101F 55
Gi0/0 10.89.17.146 Gi0/1 192.168.150.60 06 101F 0016 9
Gi0/1 192.168.150.60 Local 192.168.206.20 01 0000 0303 11
```

```
Gi0/0 10.89.17.146 Gi0/1 192.168.150.60 06 07F1 0016 1
```

Для определения трафика, который использует ACL для классификации, используйте команду show access-listacl-name. Счетчики ACL можно очистить с помощью EXEC-команды clear ip access-list counters .

```
router#show access-list ACL-SMB-CLASSIFY
Extended IP access list ACL-SMB-CLASSIFY
10 deny tcp any any eq 139 (10 matches)
20 deny tcp any any eq 445 (9 matches)
30 deny ip any any (184 matches)
```

В материале Understanding Access Control List Logging (Общие сведения о ведении журналов списка управления доступом) можно получить дополнительную информацию о возможностях ведения журналов в ACL.

Контроль доступа со схемами VLAN и списками управления доступом портов

Списки управления доступом VLAN (VACL) или схемы VLAN и ACL портов (PACL) дают возможность принудительно включить управление доступом на немаршрутизируемом трафике, который ближе к оконечным устройствам, чем списки управления доступом, которые применяются к маршрутизируемым интерфейсам.

Следующие разделы содержат обзор функций, преимуществ и сценариев возможного использования VACL и PACL.

Контроль доступа с помощью списков доступа VLAN

VACL или схемы VLAN, которые применяются ко всем пакетам, входящим в VLAN, дают возможность принудительно включить управление доступом на внутреннем трафике VLAN. Это невозможно со списками ACL на маршрутизируемых интерфейсах. Например, схема VLAN может использоваться для того, чтобы хосты, находящиеся в той же VLAN, не могли обмениваться данными друг с другом, что уменьшает возможности локальных атак и распространения червей в том же сегменте сети. Для того чтобы запретить пакетам использовать схему VLAN, можно создать список управления доступом (ACL), который совпадает с трафиком и, согласно схеме VLAN, задает действие отбрасывания. Как только схема VLAN настроена, все пакеты, которые поступают в LAN, последовательно оцениваются по настроенной карте VLAN. Карты доступа VLAN поддерживают списки доступа MAC и IPv4; однако они не поддерживают ACL IPv6 и ведение журналов.

В следующем примере используется расширенный именованный список доступа, который иллюстрирует настройку этой функции:

```
router#show access-list ACL-SMB-CLASSIFY
Extended IP access list ACL-SMB-CLASSIFY
10 deny tcp any any eq 139 (10 matches)
20 deny tcp any any eq 445 (9 matches)
30 deny ip any any (184 matches)
```

Следующий пример демонстрирует использование схемы VLAN для запрета портов TCP 139 и 445, а также протокола vines-ip:

```
router#show access-list ACL-SMB-CLASSIFY
Extended IP access list ACL-SMB-CLASSIFY
```

```
10 deny tcp any any eq 139 (10 matches)
20 deny tcp any any eq 445 (9 matches)
30 deny ip any any (184 matches)
```

В материале Configuring Network Security with ACLs (Настройка сетевой безопасности с помощью списков ACL) можно получить дополнительную информацию о конфигурации схем VLAN.

Контроль доступа с помощью PACL

PACL могут быть применены только к входящему направлению на физических интерфейсах уровня 2 коммутатора. PACL подобен схемам VLAN, но обеспечивает управление доступом для трафика уровня 2 или без маршрутизации. Синтаксис для создания PACL, который имеет приоритет над схемами VLAN и списками управления доступом к маршрутизатору, совпадает со списками управления доступом к маршрутизатору. Если ACL применен к интерфейсу 2-го уровня, то он называется PACL. Конфигурация включает создание IPv4, IPv6 или MAC ACL и его применение к интерфейсу 2-го уровня.

В данном примере используется расширенный именованный список доступа, иллюстрирующий настройку этой функции:

```
router#show access-list ACL-SMB-CLASSIFY
Extended IP access list ACL-SMB-CLASSIFY
10 deny tcp any any eq 139 (10 matches)
20 deny tcp any any eq 445 (9 matches)
30 deny ip any any (184 matches)
```

В разделе ACL порта документа Configuring Network Security with ACLs (Настройка сетевой безопасности с помощью ACL) можно получить дополнительную информацию о настройке PACL.

Контроль доступа с помощью MAC

Списки управления доступом MAC или расширенные списки применяются к IP-сети с использованием следующей команды в режиме конфигурации интерфейса:

```
Cat6K-IOS(config-if)#mac packet-classify
```

> **Примечание. Это необходимо для классификации пакетов уровня 3 как пакетов уровня 2.** Команда поддерживается в программном обеспечении Cisco IOS версии 12.2(18)SXD (для SUP 720) и Cisco IOS 12.2 (33) SRA или более поздних.

Эта интерфейсная команда должна быть применена к входящему интерфейсу и указывает механизму пересылки, что не нужно просматривать заголовок IP. Результат заключается в том, что можно использовать список доступа MAC в среде IP.

Использование частных VLAN

Частные VLAN (PVLAN) являются компонентом безопасности уровня 2, который ограничивает соединение между рабочими станциями или серверами в VLAN. Без PVLAN все устройства VLAN уровня 2 могут свободно обмениваться данными. Существуют

сетевые ситуации, когда можно повысить безопасность путем ограничения соединений между устройствами в рамках одной VLAN. Например, PVLAN часто используются для запрещения обмена данными между серверами в общедоступной подсети. Если одиночный сервер скомпрометирован, то отсутствие возможности подключения к другим серверам благодаря PVLAN поможет ограничить компрометацию одним сервером.

Существует три типа частных VLAN: изолированные VLAN, VLAN сообщества и основные VLAN. Конфигурация PVLAN использует основные и вторичные VLAN. Основная VLAN содержит все порты неизбирательного режима, которые описаны ниже, и включает одну или несколько вторичных VLAN, которые могут быть либо изолированными, либо VLAN сообществ.

Изолированные VLAN

Конфигурация вторичной VLAN как изолированной полностью блокирует связь между устройствами во вторичной VLAN. Может быть только одна изолированная VLAN на основную VLAN, и только порты неизбирательного режима могут обмениваться данными с портами в изолированной VLAN. Изолированные VLAN должны использоваться в сетях без доверия, например в сетях для гостевой поддержки.

Следующий пример конфигурации настраивает VLAN 11 как изолированную и привязывает ее к основной VLAN 20. Следующий пример также настраивает интерфейс FastEthernet 1/1 как изолированный порт в VLAN 11:

```
Cat6K-IOS(config-if)#mac packet-classify
```

VLAN сообщества

Вторичная VLAN, настроенная как VLAN сообщества, обеспечивает обмен данными между участниками VLAN, а также с любыми портами неизбирательного режима основной VLAN. Однако обмен данных невозможен ни между двумя VLAN сообщества, ни между VLAN сообщества и изолированной VLAN. VLAN сообщества должны использоваться для группирования серверов, которым необходим обмен данными друг с другом, но не требуется подключение ко всем остальным устройствам VLAN. Этот сценарий имеет распространение в общедоступной сети или в случаях, когда серверы должны предоставлять контент ненадежным клиентам.

В следующем примере настраивается одна VLAN сообщества и порт коммутатора FastEthernet 1/2 в качестве участника для этой VLAN. VLAN сообщества (VLAN 12) является вторичной VLAN по отношению к основной VLAN 20.

```
Cat6K-IOS(config-if)#mac packet-classify
```

Порты неизбирательного режима

Порты коммутатора, которые размещены в основной VLAN, называются портами неизбирательного режима. Порты неизбирательного режима могут обмениваться данными со всеми другими портами в основных и вторичных VLAN. Маршрутизатор или интерфейсы межсетевого экрана являются наиболее распространенными устройствами, которые

находятся в этих VLAN.

Следующий пример конфигурации сочетает предыдущие примеры изолированных VLAN и VLAN сообщества и добавляет конфигурацию interface FastEthernet 1/12 в качестве порта неизбирательного режима:

```
Cat6K-IOS(config-if)#mac packet-classify
```

При реализации PVLAN важно гарантировать, что конфигурация уровня 3 на месте поддерживает ограничения, которые вводит PVLAN, и не позволяет обойти конфигурацию PVLAN. Фильтрация уровня 3 с ACL маршрутизатора или межсетевым экраном может предотвратить обход конфигурации PVLAN.

В разделе Private VLANs (PVLANs) - Promiscuous, Isolated, Community (Частные VLAN: произвольные, изолированные, сообщества) на домашней странице Безопасность локальных сетей можно получить дополнительную информацию об использовании и конфигурации частных VLAN.

Заключение

Этот документ содержит широкий обзор методов, которые могут использоваться для обеспечения устройств Cisco IOS. Защита устройств повышает общую безопасность сетей, которыми вы управляете. В этом обзоре обсуждается защита уровней управления, администрирования и передачи данных, а также приведены рекомендации по настройке. Где это возможно, приведены подробные сведения, достаточные для настройки соответствующей функции. Но во всех случаях приведены полные справочники, где можно почерпнуть информацию для дальнейшего исследования.

Благодарность

Некоторые описания функций в этом документе были написаны командами разработки информации Cisco.

Приложение: Контрольный список защиты устройства Cisco IOS

В контрольном списке перечислены все шаги защиты, которые представлены в этом руководстве. Администраторы могут использовать его в качестве справочника по всем функциям защиты, которые использовались или рассматривались как кандидаты для использования на устройствах Cisco IOS, даже если функция не была реализована, поскольку она оказалась неприменимой. Администратору рекомендуется оценить каждую функцию на предмет потенциального риска, прежде чем внедрять эту функцию.

Уровень администрирования

- Пароли

  Включите хеширование MD5 (секретная опция) для использования локальных паролей

пользователейНастройте блокировку подбора пароляОтключите восстановление пароля (обдумайте риск),

- Отключение неиспользуемых служб
- Настройте проверку активности TCP для сеансов администрирования
- Задайте уведомления о пороговых значениях ЦП и памяти
- Настройка

  Уведомления о пороговых значениях ЦП и памятиРезервная память для доступа к консолиДетектор утечек памятиОбнаружение переполнения буфераРасширенный сбор информации о сбоях
- Используйте iACL для ограничения доступа администрирования
- Фильтрация (обдумайте риск),

  Пакеты ICMPIP-фрагментыПараметры IPЗначение TTL в пакетах
- Защита уровня управления

  Настройте фильтрацию портовНастройте пороговые значения очереди
- Доступ управления

  Используйте защиту уровня администрирования для ограничения интерфейсов администрированияЗадайте тайм-аут EXECИспользуйте зашифрованный транспортный протокол (например, SSH) для доступа к командной строкеУправление транспортом для линий tty и vty (опция класса доступа),Использование предупреждающих баннеров
- Аутентификация (AAA)

  Используйте AAA для аутентификации и откатаИспользуйте AAA (TACACS+) для авторизации командИспользуйте AAA для учетаИспользуйте резервные серверы AAA
- SNMP

  Настройте имя и пароль SNMPv2 и примените ACLНастройте SNMPv3
- Ведение журнала

  Настройте централизованное ведение журналаЗадайте уровень ведения журнала для всех соответствующих компонентовЗадайте интерфейс источника ведения журналаНастройте детализацию меток времени ведения журнала
- Управление конфигурацией

Замена и откатИсключительный доступ к изменению конфигурацииКонфигурация эластичности программного обеспеченияУведомления об изменениях конфигурации

Плоскость управления

- Отключите (обдумайте риск),

  Переадресация ICMPНедостижимые ICMPПротокол прокси-ARP

- Настройте аутентификацию NTP, если используется NTP

- Настройте защиту/политики уровня управления (фильтрация портов, пороговые значения очереди)

- Защитите протоколы маршрутизации

  BGP (TTL, MD5, максимальное число префиксов, списки префиксов, ACL системных путей)IGP (MD5, пассивный интерфейс, фильтрация маршрутов, потребление ресурсов)

- Настройте аппаратные ограничители скорости

- Защитите протоколы резервирования первого перехода (GLBP, HSRP, VRRP)

Уровень данных

- Настройте выборочное отбрасывание IP-параметров

- Отключите (обдумайте риск),

  IP-маршрутизация от источникаНаправленные широковещательные IP-рассылкиПереадресация ICMP

- Ограничение направленных широковещательных IP-рассылок

- Настройте tACL (обдумайте риск),

  Фильтрация ICMPФильтрация IP-фрагментовФильтрация параметров IPФильтрация по значению TTL

- Настройте необходимую защиту от спуфинга

  ACLЗащита от подделки IP-адреса (IP Source Guard)Динамическая проверка ARPUnicast RPFБезопасность портов

- Защита уровня управления (control-plane cef-exception)

- Настройте NetFlow и ACL для классификации для идентификации трафика
- Настройте необходимые ACL контроля доступа (схемы VLAN, PACL, MAC)
- Настройте частные VLAN