Руководство Cisco по усилению защиты устройств Cisco IOS

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Общие сведения
Безопасные операции
Cisco Security монитора информационные сообщения и ответы
Аутентификация, авторизация и учет рычагов
Централизуйте регистрационный набор и мониторинг
Используйте защищенные протоколы, когда возможно
Видимость трафика усиления с NetFlow
Управление конфигурацией
Панель управления
Укрепление плоскости общего менеджмента
Управление паролями
Enhanced Password Security
Локаут повторной попытки пароля для входа
No Service Password-Recovery
Disable Unused Services
Таймаут EXEC
Пакеты Keepalive для сеансов TCP
Использование интерфейса управления
Пороговые уведомления памяти
Уведомление пороговой обработки ЦП
Резервная память для консольного доступа
Детектор утечек памяти
Переполнение буфера: Обнаружение и исправление повреждения Redzone
Расширенный набор файла crashinfo
Протокол NTP (Network Time Protocol, протокол сетевого времени)
Отключите умную установку
Предельный доступ к сети с ACL инфраструктуры
Фильтрация пакета ICMP
IP - фрагменты фильтра
Поддержка ACL IP - режимов фильтрации
Поддержка ACL для фильтрации на значении TTL
Защитите интерактивные сеансы управления
Защита панели управления
Защита уровня управления

Зашифруйте сеансы управления
SSHv2
Усовершенствования SSHv2 для ключей RSA
Консоль и порты AUX
VTY контроля и Линии tty
Транспорт контроля для VTY и Линий tty
Предупреждающие сообщения
Аутентификация, авторизация и учет
Аутентификация TACACS+
Authentication Fallback
Использование паролей типа 7
Авторизация TACACS+ Command
TACACS + учет команды
Избыточные AAA-серверы
Укрепите простой протокол управления сетью
Строки имени и пароля SNMP
Строки имени и пароля SNMP с ACL
Инфраструктурные списки ACL
Представления SNMP
Протокол SNMP версии 3
Защита панели управления
Оптимальные методы Регистрации
Передайте журналы к центральному месту расположения
Уровень регистрации
Не регистрируйте к консоли или сеансам монитора
Используйте буферизированную Регистрацию
Настройте исходный интерфейс Регистрации
Настройте метки времени регистрации
Менеджмент конфигурации программного обеспечения Cisco IOS
Замена конфигурации и откат конфигурации
Исключительный доступ изменения конфигурации
Программное обеспечение Cisco IOS эластичная конфигурация
Снабженное цифровой подписью программное обеспечение Cisco
Уведомление изменения конфигурации и Регистрация
Плоскость управления
Общее укрепление уровня управления
Переадресации ICMP IP
Недостижимый ICMP
Протокол прокси-ARP
Ограничьте влияние на ЦП трафика уровня управления
Поймите трафик уровня управления
Инфраструктурные списки ACL
Списки ACL для входящего трафика
CoPP
Защита уровня управления

Аппаратные ограничители скорости
Безопасный BGP
Основанные на TTL средства обеспечения безопасности
Аутентификация однорангового соединения по протоколу BGP с MD5
Настройте максимальное число префиксов
Префиксы BGP фильтра со списками префиксов
Префиксы BGP фильтра со списками доступа пути автономной системы
Безопасные протоколы внутреннего шлюза
Аутентификация протокола маршрутизации и проверка с профилем сообщения 5
Команды Passive-Interface
Фильтрование маршрутов
Потребление ресурсов процесса маршрутизации
Защитите первые протоколы резервирования переходов
Плоскость данных
Укрепление плоскости общих данных
IP - режимы выборочное отбрасывание
Отключите маршрутизацию источника IP
Отключите переадресации ICMP
Отключите или ограничьте направленные широковещательные IP - рассылки
Транзитный трафик фильтра с транзитными ACL
Фильтрация пакета ICMP
IP - фрагменты фильтра
Поддержка ACL IP - режимов фильтрации
Меры защиты антиспуфинга
RPF индивидуальной рассылки
Защита от подделки IP-адреса (IP Source Guard)
Безопасность портов
Динамическая проверка ARP
Антиспуфинговые ACL
Ограничьте влияние на ЦП трафика плоскости данных
Функции и Типы трафика, который Влияние ЦП
Фильтр на значении TTL
Фильтр на присутствии IP - режимов
Защита уровня управления
Идентификация трафика и обратная трассировка
NetFlow
ACL классификации
Управление доступом со СХЕМАМИ VLAN и портом списки контроля доступа
Управление доступом со СХЕМАМИ VLAN
Управление доступом с PACL
Управление доступом с MAC
Частное VLAN использование
Выделенные VLAN
VLAN сообщества
Случайные порты

[Заключение](#)
[Подтверждения](#)
[Приложение: стабилизирующий чек-лист устройства Cisco IOS](#)
[Панель управления](#)
[Плоскость управления](#)
[Плоскость данных](#)

Введение

Этот документ описывает информацию, чтобы помочь вам защищать свои системные устройства Cisco IOS®, который увеличивает общую безопасность вашей сети. Структурированный вокруг этих трех плоскостей, в которые могут быть категоризированы функции сетевого устройства, этот документ предоставляет обзор каждой включенной функции и ссылок на связанную 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 плоскости сети, панели управления, уровня управления и плоскости данных, каждый предоставляет другую функциональность, которая должна быть защищена.

- **Панель управления** - панель управления управляет трафиком, который передается устройству Cisco IOS и составлен из приложений и протоколов, таких как Secure Shell (SSH) и Протокол SNMP.

- **Уровень управления** - уровень управления сетевого устройства обрабатывает трафик, который является главным для поддержания функциональности инфраструктуры сети. Уровень управления состоит из приложений и протоколов между сетевыми устройствами, который включает Протокол BGP, а также Протоколы внутреннего шлюза (IGPs), такие как Протокол EIGRP и Протокол OSPF.

- **Плоскость данных** - плоскость данных передает данные через сетевое устройство.

Плоскость данных не включает трафик, который передается устройству IOS локального Cisco.

Покрытие характеристик безопасности в этом документе часто предоставляет достаточно подробности для вас для настройки функции. Однако в случаях, где это не делает, функция объяснена таким способом, которым можно оценить, требуется ли дополнительное внимание к функции. Где возможный и соответствующий, этот документ содержит рекомендации, что, если внедрено, справка защищает сеть.

Безопасные операции

Операции защищенной сети являются существенной темой. Несмотря на то, что большая часть этого документа посвящена безопасной конфигурации устройства Cisco IOS, одни только конфигурации не делают абсолютно безопасный сеть. Рабочие процедуры в использовании в сети способствуют так же безопасности как конфигурация базовых устройств.

Эти темы содержат в рабочем состоянии рекомендации, которые вам рекомендуют внедрить. Эти темы выделяют определенные критические области функционирований сети и не являются всесторонними.

Cisco Security монитора информационные сообщения и ответы

Команда расследования инцидента, связанного с безопасностью продукта Cisco (PSIRT) создает и поддерживает публикации, обычно называемые Информационными сообщениями PSIRT, для связанных с безопасностью проблем в продуктах Cisco. Метод, используемый для связи менее серьезных проблем, является Cisco Security Ответ. Рекомендации по вопросам безопасности и ответы доступны в http://www. cisco . com/go/psirt.

Дополнительные сведения об этих механизмах связи доступны в Политике Уязвимости Cisco Security.

Для поддержания защищенной сети необходимо знать об информационных сообщениях Безопасности Cisco и ответах, которые были освобождены. Необходимо ознакомиться с уязвимостью перед угрозой, которую она может представить сети, может быть оценен. См. Медицинскую сортировку Риска для Объявлений Уязвимости безопасности для помощи этот процесс оценки.

Аутентификация, авторизация и учет рычагов

Платформа Аутентификации, авторизации и учета (AAA) жизненно важна для устройств защищенной сети. Инфраструктура AAA предоставляет аутентификацию сеансов управления и может также ограничить пользователей определенными, определенными администраторами командами и регистрировать все команды, введенные всеми пользователями. Посмотрите раздел Аутентификации, авторизации и учета этого документа для получения дополнительной информации о том, как усилить AAA.

Централизуйте регистрационный набор и мониторинг

Для получения знания о существующем, появлении и исторических событиях, отнесенных к случаям нарушения безопасности, организация должна иметь унифицированную стратегию

регистрации событий и корреляции. Эта стратегия должна усилить регистрацию от всех сетевых устройств и использование предварительно упакованные и настраиваемые возможности корреляции.

После того, как централизовано регистрация внедрена, необходимо разработать структурированный подход для регистрации анализа и отслеживания инцидента. На основе потребностей вашей организации этот подход может колебаться от простого прилежного анализа данных журнала к усовершенствованному основанному на правилах анализу.

Посмотрите раздел Оптимальных методов Регистрации этого документа для получения дополнительной информации о том, как внедрить входящий в систему устройства Cisco IOS network.

Используйте защищенные протоколы, когда возможно

Много протоколов используются для переноса чувствительных данных управления сетью. Необходимо использовать защищенные протоколы, когда это возможно. Выбор защищенного протокола включает использование SSH вместо Telnet так, чтобы были зашифрованы и данные проверки подлинности и данные для управления. Кроме того, необходимо использовать безопасные протоколы передачи файлов при копировании данных о конфигурации. Примером является использование протокола SCP вместо FTP или TFTP.

Посмотрите Безопасный Интерактивный раздел Сеансов управления этого документа для получения дополнительной информации о безопасном управлении устройств Cisco IOS.

Видимость трафика усиления с NetFlow

NetFlow позволяет вам контролировать трафики в сети. Первоначально предназначенный для экспортирования информации о потоке данных в приложения для управления сетью NetFlow может также использоваться для показа сведений о потоках на маршрутизаторе. Эта возможность позволяет вам видеть, какой трафик пересекает сеть в режиме реального времени. Независимо от того, экспортируются ли сведения о потоках в удаленный коллектор, вам рекомендуют настроить сетевые устройства для NetFlow так, чтобы это могло использоваться реактивным образом в случае необходимости.

Дополнительные сведения об этой функции доступны в разделе Идентификации и Обратной трассировки Трафика этого документа и в http://www. cisco . com/движение/netflow (только зарегистрированные клиенты).

Управление конфигурацией

Управление конфигурацией является процессом, которым изменения конфигурации предложены, рассмотрены, утверждены и развернуты. В контексте конфигурации устройства Cisco IOS два дополнительных аспекта управления конфигурацией важны: архивация конфигурации и безопасность.

Можно использовать архивные конфигурации для отката изменений, которые внесены в сетевые устройства. В контексте безопасности архивные конфигурации могут также использоваться для определения, какие изменения безопасности были сделаны и когда произошли эти изменения. В сочетании с данными журнала AAA эта информация может

помочь в аудите безопасности сетевых устройств.

Конфигурация устройства Cisco IOS содержит много чувствительных подробных данных. Имена пользователей, пароли и содержание списков контроля доступа являются примерами этого типа информации. Репозиторий, который вы используете для архивации конфигураций устройства Cisco IOS должен быть защищен. Опасный доступ к этой информации может подорвать безопасность всей сети.

Панель управления

Панель управления состоит из функций, которые достигают целей управления сети. Это включает интерактивные сеансы управления, которые используют SSH, а также сбор статистики с SNMP или NetFlow. Когда вы рассматриваете безопасность сетевого устройства, важно, что защищена панель управления. Если случай нарушения безопасности в состоянии подорвать функции панели управления, для вас может быть невозможно восстановить или стабилизировать сеть.

Эти разделы этого документа детализируют характеристики безопасности и конфигурации, доступные в программном обеспечении Cisco IOS, что справка укрепляет панель управления.

Укрепление плоскости общего менеджмента

Панель управления используется, чтобы обратиться, настроить, и управлять устройством, а также контролировать его операции и сеть, в которой она развернута. Панель управления является плоскостью, которая получает и передает трафик за использованием этих функций. Необходимо защитить и панель управления и уровень управления устройства, потому что использование уровня управления непосредственно влияет на использование панели управления. Этот список протоколов используется панелью управления:

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

- Системный журнал

Шаги должны быть сделаны для обеспечения выживания управления и уровней управления во время случаев нарушения безопасности. Если одна из этих плоскостей успешно использована, все плоскости могут поставиться под угрозу.

Управление паролями

Пароли управляют доступом к ресурсам или устройствам. Это выполнено через определение пароль или тайна, которая используется для аутентификации запросов. Когда запрос получен для доступа к ресурсу или устройству, запросу бросают вызов для проверки пароля и идентичности, и доступ может быть предоставлен, запрещен или ограничен на основе результата. Как оптимальный метод безопасности, паролями нужно управлять с TACACS + или Сервер проверки подлинности RADIUS. Однако обратите внимание, что локально настроенный пароль для привилегированного адреса все еще необходим в случае сбоя TACACS + или Сервисы RADIUS. Устройство может также иметь другой подарок сведений о пароле в своей конфигурации, такой как ключ NTP, Строка имени и пароля SNMP или ключ Протокола маршрутизации.

Команда enable secret используется для установки пароля, который предоставляет привилегированный административный доступ системе Cisco IOS. **Команда enable secret** должна использоваться, а не более старая **команда enable password**. **Команда enable password использует слабый алгоритм шифрования.**

Если никакой enable secret не установлен, и пароль настроен для консольной линии tty, пароль консоли может использоваться для получения привилегированного адреса, даже от удаленного действительного tty (VTY) сеанс. Это действие почти наверняка нежелательно и является другой причиной гарантировать конфигурацию enable secret.

Команда глобальной кофигурации **шифрования служебного пароля** направляет программное обеспечение Cisco IOS для шифрования паролей, тайн Протокола аутентификации по квитированию вызова (CHAP) и подобных данных, которые сохранены в его файле конфигурации. Такое шифрование полезно, чтобы препятствовать тому, чтобы случайные наблюдатели читали пароли, такой как тогда, когда они посмотрели на экран по осмотру администратора. Однако алгоритм, используемый командой **шифрования служебного пароля**, является простым шифром ре Vigen. Алгоритм не разработан для защиты файлов конфигурации против серьезного анализа даже немного сложными атакующими и не должен использоваться для этой цели. Любой Файл конфигурации Cisco IOS, который содержит зашифрованные пароли, должен рассматриваться с той же осторожностью, которая используется для незашифрованного списка тех тех же паролей.

В то время как этот слабый алгоритм шифрования не используется **командой enable secret**, он используется командой глобальной кофигурации **enable password**, а также командой конфигурации с командной строки **пароля**. Пароли этого типа должны быть устранены и **команда enable secret**, или функция Enhanced Password Security должна быть использована.

Команда enable secret и функция Enhanced Password Security используют алгоритм представления сообщения в краткой форме 5 (MD5) для хеширования пароля. Этот алгоритм имел значительную общественную оценку и, как известно, не обратим. Однако алгоритм подвергается подборам пароля по словарю. В подборе пароля по словарю атакующий пробует каждое слово в словаре или другом списке паролей кандидата для обнаружения соответствия. Поэтому файлы конфигурации должны быть надежно

сохранены и только разделены с доверяемыми частными лицами.

Enhanced Password Security

Enhanced Password Security функции, представленный в программном обеспечении Cisco IOS версии 12.2(8)T, позволяет администратору настраивать хеширование MD5 паролей для команды **имени пользователя**. До этой функции было два типа паролей: Тип 0, который является нешифрованным паролем и Типом 7, который использует алгоритм от шифра ре Vigen. Функция Enhanced Password Security не может быть использована с протоколами, которые требуют, чтобы нешифрованный пароль был восстановим, таков как CHAP.

Для шифрования пароля пользователя с хешированием MD5 выполните команду глобальной кофигурации **username secret**.

```
!

username <name> secret <password>

!
```

См. Enhanced Password Security для получения дополнительной информации об этой функции.

Локаут повторной попытки пароля для входа

Опция Локаута Повторной попытки Пароля для входа, добавленная в программном обеспечении Cisco IOS версии 12.3(14)T, позволяет вам блокировать учетную запись локального пользователя после настроенного номера неуспешных попыток входа. Как только пользователь заблокирован, их учетная запись блокирована, пока вы не разблокировали ее. Авторизованный пользователь, который настроен с уровнем привилегий 15, не может быть заблокирован с этой функцией. Количество пользователей с уровнем привилегий 15 должно быть сведено к минимуму.

Если количество неуспешных попыток входа достигнуто, Обратите внимание на то, что авторизованные пользователи могут блокировать себя из устройства. Кроме того, злонамеренный пользователь может создать условие отказа в обслуживании (DoS) с повторными попытками аутентифицироваться с допустимым именем пользователя.

Данный пример показывает, как активировать опцию Локаута Повторной попытки 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 также применяется к методам аутентификации, таким как CHAP и Протокол аутентификации пароля (PAP).

No Service Password-Recovery

В программном обеспечении Cisco IOS версии 12.3(14)T и позже, функция Password-Recovery No Service не позволяет никому с консольным доступом неуверенно обращаться к конфигурации устройства и очищать пароль. Это также не позволяет злонамеренным пользователям изменять значение регистра конфигурации и обращаться к NVRAM.

```
!

no service password-recovery

!
```

Программное обеспечение Cisco IOS предоставляет процедуру восстановления пароля, которая полагается на доступ к Режиму монитора ПЗУ (ROMMON) с помощью Ключа прерывания во время запуска системы. В ROMMON программное обеспечение устройства может быть повторно загружено для запроса новой конфигурации системы, которая включает новый пароль.

Процедура восстановления текущего пароля позволяет любому с консольным доступом обратиться к устройству и его сети. Функция Password-Recovery No Service предотвращает завершение Последовательности нажатий клавиш для прерывания и ввод ROMMON во время запуска системы.

Если **password-recovery no service** включен на устройстве, рекомендуется, чтобы была сохранена офлайновая копия конфигурации устройства и что внедрено решение для архивирования конфигурации. Если необходимо восстановить пароль устройства Cisco IOS, как только эта опция активирована, полная конфигурация удалена.

См. Безопасный Пример конфигурации ROMMON для получения дополнительной информации об этой функции.

Disable Unused Services

Как оптимальный метод безопасности, должен быть отключен любой ненужный сервис. Эти ненужные сервисы, особенно те, которые используют Протокол UDP, нечасто используются для обоснованных целей, но могут использоваться для запуска DoS и других атак, которые иначе предотвращены фильтрацией пакетов.

TCP и UDP маленькие сервисы должны быть отключены. Эти сервисы включают:

- эхо (номер порта 7)
- сброс (номер порта 9)
- дневное время (номер порта 13)
- chargen (номер порта 19)

Несмотря на то, что злоупотребления маленькими сервисами могут избежать или сделать менее опасного списки доступа с функцией антиспуфинга, сервисы должны быть отключены на любом устройстве, доступном в сети. В Cisco IOS начиная с версии 12.0 и выше все малые службы отключены по умолчанию. В более ранних версиях ПО **маленькие серверы tcp no service** и команды глобальной кофигурации **udp-small-servers no service** могут быть

выполнены для отключения их.

Это - список дополнительных сервисов, которые должны быть отключены если не в использовании:

- Не выполните команду глобальной кофигурации **ip finger** для отключения Сервиса Finger. Cisco IOS Software Release позже, чем 12.1 (5) и 12.1 (5) T отключают этот сервис по умолчанию.

- Выполните команду глобальной кофигурации **no ip bootp server** для отключения Протокола начального загрузки (BOOTP).

- В Cisco IOS Software Release 12.2 (8) T и позднее, выполняют **команда ip dhcp bootp ignore** в режиме глобальной конфигурации для отключения BOOTP. Это уезжает, сервисы Протокола DHCP (динамического конфигурирования узла) включили.

- Если сервисы ретрансляции DHCP не требуются, сервисы DHCP могут быть отключены. Выполните команду **no service dhcp** в режиме глобальной конфигурации.

- Не выполните **команду mop enabled** в режиме конфигурации интерфейса для отключения сервиса Протокола отладки (MOP).

- Выполните команду глобальной кофигурации **no ip domain lookup** для отключения сервисов разрешения Системы доменных имен (DNS).

- Выполните команду **no service pad** в режиме глобальной конфигурации для отключения сервиса Компоновщик/декомпоновщика пакетов (PAD), который используется для сетей X.25.

- Сервер HTTP может быть отключен с командой **no ip http server** в режиме глобальной конфигурации и Безопасным HTTP (HTTPS), сервер может быть отключен с командой глобальной кофигурации **no ip http secure-server**.

- Пока устройства Cisco IOS не получают конфигурации из сети во время запуска, команда глобальной кофигурации **no service config** должна использоваться. Это предотвращает устройство Cisco IOS от попытки определить местоположение файла конфигурации в сети с TFTP.

- Протокол CDP является сетевым протоколом, который используется для обнаружения других устройств с поддержкой CDP для соседства и топологии сети. CDP может использоваться Системами управления сетью (NMS) или во время устранения проблем. CDP должен быть отключен на всех интерфейсах, которые связаны с сетями без доверия. Это не выполнено ни с **какой** командой интерфейса **cdp enable**. Также CDP не может быть отключен глобально ни с **какой** командой глобальной кофигурации **cdp run**. Обратите внимание на то, что CDP может использоваться злонамеренным пользователем для разведки и сетевого сопоставления.

- Протокол LLDP является протоколом IEEE, который определен в 802.1AB. LLDP

подобен CDP. Однако этот протокол позволяет совместимость между другими устройствами, которые не поддерживают CDP. LLDP должен рассматриваться таким же образом как CDP и отключаться на всех интерфейсах то подключение к сетям без доверия. Для выполнения этого не выполните **передачу lldp**, и **никакой lldp не получает** команды настройки интерфейса. Не выполните **lldp выполненная** команда глобальной кофигурации для отключения LLDP глобально. LLDP может также использоваться злонамеренным пользователем для разведки и сетевого сопоставления.

Таймаут EXEC

Для установки интервала, что интерпретатор команд EXEC ждет ввода пользователя, прежде чем это завершит сеанс, выполните команду конфигурации с командной строки **exec-timeout**. **Команда exec-timeout** должна использоваться, чтобы выйти из системы сеансы на VTY или линиях tty, которые оставляют простаивающими. По умолчанию сеансы разъединены после десяти минут бездействия.

```
!

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

Пакеты Keepalive для сеансов TCP

Service tcp-keepalives-in и команды глобальной кофигурации **service tcp-keepalives-out** позволяют устройству передать TCP keepalife за сеансами TCP. Эта конфигурация должна использоваться для включения TCP keepalife на входящих подключениях к устройству и исходящих соединениях от устройства. Это гарантирует, что устройство на удаленном конце соединения все еще доступно и что полуоткрытые или осиротевшие соединения удалены из устройства IOS локального Cisco.

```
!

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

Использование интерфейса управления

К панели управления устройства обращаются внутриполосная или внеполосная на медосмотре или Logical Management Interface. Идеально, и внутриполосный доступ и доступ управления при нестандартном подключении существуют для каждого сетевого устройства так, чтобы к панели управления можно было обратиться во время выходов сети из строя.

Один из наиболее распространенных интерфейсов, который используется для внутриполосного доступа к устройству, является логическим интерфейсом обратной связи. Интерфейсы обратной связи подключены всегда, тогда как физические интерфейсы могут изменить состояние, и интерфейс не может потенциально быть доступным. Рекомендуется добавить интерфейс обратной связи к каждому устройству как интерфейс управления и что это используется исключительно для панели управления. Это позволяет администратору применять политику всюду по сети для панели управления. Как только интерфейс обратной связи настроен на устройстве, он может использоваться протоколами панели управления,

такими как SSH, SNMP и системный журнал, чтобы передать и получить трафик.

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

Пороговые уведомления памяти

Пороговое Уведомление Памяти функции, добавленное в программном обеспечении Cisco IOS версии 12.3(4)T, позволяет вам смягчать нехватки памяти на устройстве. Эта функция использует два метода для выполнения этого: Пороговое Уведомление Памяти и Резервирование Памяти.

Пороговое Уведомление памяти генерирует сообщение журнала, чтобы указать, что доступная память на устройстве упала ниже, чем настроенный порог. Этот пример конфигурации показывает, как активировать эту опцию с командой глобальной кофигурации **memory free low-watermark**. Это позволяет устройству генерировать уведомление, когда доступная доступная память падает ниже, чем заданная пороговая величина, и снова когда доступная доступная память повышается к на пять процентов выше, чем заданная пороговая величина.

```
!

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

Резервирование памяти используется так, чтобы достаточно памяти были доступны для важных уведомлений. Этот пример конфигурации демонстрирует, как активировать эту опцию. Это гарантирует, что процессы управления продолжают функционировать, когда исчерпана память об устройстве.

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

См. Пороговые Уведомления Памяти для получения дополнительной информации об этой функции.

Уведомление пороговой обработки ЦП

Когда Загрузка ЦПУ на устройстве пересекает настроенный порог, представленный в программном обеспечении Cisco IOS версии 12.3(4)T, функция Уведомления Пороговой обработки ЦП позволяет вам обнаруживать и уведомляться. Когда порог скрещен, устройство генерирует и передает сообщение прерывания SNMP. Два метода задания порога загрузки ЦПУ поддерживаются на программном обеспечении Cisco IOS: Верхний порог и Нижний порог.

Конфигурация данного примера показывает, как включить Повышение и Нижние пороги, которые инициируют сообщение с уведомлением порогового значения ЦПУ:

```
!

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>]
!
```

См. Уведомление Пороговой обработки ЦП для получения дополнительной информации об этой функции.

&

Резервная память для консольного доступа

В программном обеспечении Cisco IOS версии 12.4(15)T и позже, Резервная Память для функции Консольного доступа может использоваться для резервирования достаточной памяти для обеспечения консольного доступа устройству Cisco IOS для административного и целей устранения проблем. Когда устройство испытывает нехватку памяти, эта функция особенно выгодна. Можно выполнить **резерв памяти консольная** команда глобальной кофигурации для активации этой опции. Данный пример настраивает устройство Cisco IOS для резервирования 4096 килобайтов для этой цели.

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

См. Резервную Память для Консольного доступа для получения дополнительной информации об этой функции.

Детектор утечек памяти

Представленный в программном обеспечении Cisco IOS версии 12.3 (8) T1, функция Детектора Утечки памяти позволяет вам обнаруживать утечки памяти на устройстве. Детектор Утечки памяти в состоянии найти 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 фокусируется на распределениях памяти, которые являются динамичными. Можно использовать команду EXEC **show memory debug leaks**, чтобы обнаружить, если существует утечка памяти.

Переполнение буфера: Обнаружение и исправление повреждения Redzone

В программном обеспечении Cisco IOS версии 12.3(7)T и позже, Переполнение буфера: Обнаружением и исправлением функции Повреждения Redzone можно включить на устройстве, чтобы обнаружить и исправить переполнение блока памяти и продолжать операции.

Эти команды глобальной кофигурации могут использоваться для активации этой опции. После того, как настроенный, команда **переполнения show memory** может использоваться для отображения статистики обнаружения и исправления переполнения буфера.

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

Расширенный набор файла crashinfo

Расширенная функция Набора Файла crashinfo автоматически удаляет старые файлы crashinfo. Когда устройство завершается катастрофическим отказом, эта опция, добавленная в программном обеспечении Cisco IOS версии 12.3(11)T, позволяет устройству исправлять пространство для создания новых файлов crashinfo. Эта функция также позволяет конфигурации количества файлов crashinfo быть сохраненной.

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

Протокол NTP (Network Time Protocol, протокол сетевого времени)

Протокол NTP не является особенно опасным сервисом, но любой ненужный сервис может представлять вектор атаки. Если NTP используется, важно явно настроить доверяемый источник времени и использовать правильную проверку подлинности. Точное и надежное время требуется в целях системного журнала, такой как во время судебных расследований потенциальных атак, а также для успешной возможности VPN - подключения когда в зависимости от сертификатов для аутентификации Фазы 1.

- **Часовой пояс NTP** - при настройке NTP, часовой пояс должен быть настроен так, чтобы могли быть точно коррелированы метки времени. Обычно существует два подхода для настройки часового пояса для устройств в сети с глобальным присутствием. Один метод должен настроить все сетевые устройства с Согласованным текущим временем (UTC) (ранее Время по Гринвичу (GMT)). Другой подход должен настроить сетевые устройства с местным часовым поясом. Дополнительные сведения об этой функции могут быть найдены в “часовом поясе” в Документации продукта Cisco.

- **Аутентификация NTP** - при настройке Аутентификации NTP она предоставляет обеспечение, что сообщениями NTP обмениваются между доверяемым Ntp peer.

Пример конфигурации с помощью 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
```

Отключите умную установку

Оптимальные методы безопасности вокруг Cisco Умная Установка (S I), функция зависит от того, как функция использована в определенном пользовательском окружении. Cisco дифференцирует эти варианты использования:

- Клиенты, которые не используют Умную функцию Установки.
- Клиенты, которые усиливают Умную функцию Установки только нулевых сенсорных развертываний.
- Клиенты, которые усиливают Умную функцию Установки больше, чем нулевых

сенсорных развертываний (конфигурация и управление изображением).

Эти разделы описывают каждый сценарий подробно:

- Клиенты, которые не используют Умную функцию Установки.
- Клиенты, которые не используют Cisco Умная функция Установки и выполняют выпуск Cisco IOS и программного обеспечения Cisco IOS XE, где команда доступна, должны отключить Умную опцию Установки ни с **какой vstack** командой.

Примечание: vstack команда была представлена в Cisco IOS Release 12.2 (55) SE03.

Это - пример выходных данных от **показа vstack** команда на коммутаторе Cisco Catalyst с Умной отключенной характеристикой клиента Установки:

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

Клиенты, которые усиливают умную функцию установки только нулевых сенсорных развертываний

Отключите Умную функциональность клиента Установки после того, как нулевая сенсорная установка завершена, или не используйте **vstack** команду.

Для распространения **vstack** команды в сеть используйте один из этих методов:

- Войдите **никакая vstack** команда на всем клиенте не переключается или вручную или со сценарием.
- Не добавьте **vstack** команду как часть Конфигурации Cisco IOS, которая выдвинута в каждого Умного клиента Установки как часть нулевой сенсорной установки.
- В версиях, которые не поддерживают **vstack** команду (Cisco IOS Release 12.2 (55) SE02 и более ранние релизы), примените список контроля доступа (ACL) на клиентские коммутаторы для блокирования трафика на порте TCP 4786.

Для включения Умной функциональности клиента Установки позже, войдите**, vstack** команда на всем клиенте переключается или вручную или со сценарием.

Клиенты, которые усиливают умную функцию установки больше, чем нулевых сенсорных развертываний

В дизайне Умной архитектуры Установки меры должны быть приняты таким образом, что пространство IP-адресов инфраструктуры не доступно для недоверяемых сторон. В версиях, которые не поддерживают **vstack** команду, гарантируйте, что только у Умного управляющего узла Установки есть подключение TCP всем Умным клиентам Установки на порту 4786.

Администраторы могут использовать эти оптимальные методы безопасности для Cisco Умные развертывания Установки на устройствах, на которые влияют:

- Интерфейсные ACL
- Контроль уровня управления (CoPP). Эта функция не доступна во всех Cisco IOS Software Release.

Данный пример показывает интерфейсный ACL с Умным управляющим узлом Установки IP-адрес как 10.10.10.1 и Умный IP-адрес клиента Установки как 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. Когда коммутаторы сначала развернуты, это может также быть выдвинуто через управляющий узел.

Для дальнейшего ограничения доступа ко всем клиентам в инфраструктуре администраторы могут использовать эти оптимальные методы безопасности на других устройствах в сети:

- Списки контроля доступа инфраструктуры (iACLs)
- Списки контроля доступом VLAN (VACL)

Предельный доступ к сети с ACL инфраструктуры

Созданный для предотвращения неавторизованного прямого соединения к сетевым устройствам списки контроля доступа инфраструктуры (iACLs) являются одним из самых важных управлений безопасностью, которые могут быть внедрены в сетях. ACL инфраструктуры усиливают идею, что почти весь сетевой трафик пересекает сеть и не предназначен к самой сети.

iACL создан и применен для определения соединений от хостов или сетей, которые должны быть позволены сетевым устройствам. Общими примерами этих типов соединений является eBGP, SSH и SNMP. После того, как соответствующие соединения были разрешены, весь другой трафик к инфраструктуре явно запрещен. Весь транзитный трафик, который пересекает сеть и не предназначен к устройствам, относящимся к инфраструктуре, тогда явно разрешен.

Защиты, обеспеченные iACLs, относятся к управлению и для уровням управления. Реализация iACLs может быть сделана легче с помощью отдельной адресации для устройств сетевой инфраструктуры. *См.* Безопасность Ориентированный Подход к IP-адресации для получения дополнительной информации о последствиях для системы безопасности IP-адресации.

Данный пример iACL конфигурация иллюстрирует структуру, которая должна использоваться в качестве отправной точки, когда вы начинаете iACL процесс внедрения:

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

После того, как созданный, iACL должен быть применен ко всем интерфейсам та поверхность неустройства, относящиеся к инфраструктуре. Это включает интерфейсы, которые соединяются с другими организациями, сегментами удаленного доступа, пользовательскими сегментами и сегментами в ЦОД.

Для получения дополнительной информации см. раздел "Защита ядра: Списки контроля доступа Защиты инфраструктуры для получения дополнительной информации о ACL Инфраструктуры.

Фильтрация пакета ICMP

Протокол ICMP разработан как протокол управления IP. Также, сообщения, которые это передает, могут иметь далеко идущие ограничения к TCP и Протоколам "IP" в целом. В то время как сетевой **эхо-запрос** средств устранения проблем и ICMP использования **traceroute**, внешнее подключение ICMP редко необходимо для правильной работы сети.

Программное обеспечение Cisco IOS предоставляет функциональность для специфической фильтрации сообщений ICMP по имени или типа и кода. ACL данного примера, который должен использоваться с записями управления доступом (ACE) от предыдущих примеров, позволяет эхо-запросы от доверяемых 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
```

IP - фрагменты фильтра

Процесс фильтра для фрагментированных пакетов IP может поставить проблему к устройствам безопасности. Это вызвано тем, что информация уровня 4, которая используется для фильтрации TCP и пакетов UDP только присутствует в начальном фрагменте. Программное обеспечение Cisco IOS использует определенный метод для проверки неначальный фрагментов против списков настроенного адреса. Программное обеспечение Cisco IOS оценивает эти неначальный фрагменты против ACL и игнорирует любую отфильтрованную информацию Уровня 4. Это заставляет неначальный фрагменты быть оцененными исключительно на части Уровня 3 любого настроенного ACE.

В конфигурации данного примера, если пакет TCP, предназначенный к **192.168.1.1** на **порту 22**, фрагментирован в пути, начальный фрагмент отброшен как ожидалось вторым ACE на основе информации уровня 4 в пакете. Однако весь остающийся (неначальные) фрагменты позволены первым ACE, основанным полностью на информации сетевого уровня 3 в пакете и ACE. Этот сценарий показывают в этой конфигурации:

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

Из-за неинтуитивной природы обработки фрагмента, IP - фрагменты часто непреднамеренно разрешаются ACL. Фрагментация также часто используется в попытках уклониться от обнаружения Intrusion Detection Systems. Именно по этим причинам IP - фрагменты часто используются в атаках, и почему они должны явно фильтроваться наверху любого, настроил iACLs. ACL данного примера включает всестороннюю фильтрацию IP - фрагментов. Функциональность от 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
```

См. Списки контроля доступа и IP - фрагменты для получения дополнительной информации о том, как ACL обрабатывает фрагментированные пакеты IP.

Поддержка ACL IP - режимов фильтрации

Программное обеспечение Cisco IOS версии 12.3(4)T добавило поддержку использования ACL для фильтрации пакетов IP на основе IP - режимов, которые содержатся в пакете. IP - режимы представляют проблему безопасности для сетевых устройств, потому что эти опции

должны быть обработаны как пакеты исключения. Это требует уровня усилия по ЦП, которое не требуется для типичных пакетов, которые пересекают сеть. Присутствие IP - режимов в пакете может также указать на попытку ниспровергать управления безопасностью в сети или иначе изменить транзитные характеристики пакета. Именно по этим причинам пакеты с IP - режимами должны фильтроваться в краю сети.

Данный пример должен использоваться с ACE от предыдущих примеров для включения завершенной фильтрации пакетов IP, которые содержат IP - режимы:

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

Поддержка ACL для фильтрации на значении TTL

Программное обеспечение Cisco IOS версии 12.4(2)T добавило поддержку ACL для фильтрации пакетов IP на основе значения Времени жизни (TTL). Значение TTL дейтаграммы IP постепенно уменьшено каждым сетевым устройством как потоки пакетов от источника до назначения. Несмотря на то, что начальные значения варьируются операционной системой, когда TTL пакета достигает нуля, пакет должен быть отброшен. Устройство, которое постепенно уменьшает TTL для обнуления, и поэтому отбрасывает пакет, требуется, чтобы генерировать и передать Time Exceeded Message ICMP к источнику пакета.

Генерация и передача этих сообщений являются процессом исключения. Маршрутизаторы могут выполнить эту функцию, когда количество пакетов IP, которые должны истечь, низко, но если количество пакетов, должных истечь, высоко, генерация и передача этих сообщений могут использовать все доступные ресурсы ЦПУ. Это представляет вектор атаки DoS. Именно по этой причине устройства должны быть укреплены против атак DoS, которые используют высокую скорость пакетов IP, которые должны истечь.

Рекомендуется, чтобы организации фильтровали пакеты IP с низкими значениями TTL в краю сети. Полностью фильтрование пакетов со значениями TTL, недостаточными для пересечения сети, смягчает угрозу основанных на TTL атак.

ACL данного примера фильтрует пакеты со значениями TTL меньше чем шесть. Это обеспечивает защиту против атак истечения TTL для сетей до пяти переходов по ширине.

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

> **Примечание:** Некоторые протоколы делают легитимное использование пакетов с низкими значениями TTL. eBGP является одним таким протоколом. См. Идентификацию Атаки Истечения TTL и Смягчение для получения дополнительной информации о смягчении TTL основанные на истечении атаки.

См. Поддержку ACL фильтрации на Значении TTL для получения дополнительной информации об этой функциональности.

Защитите интерактивные сеансы управления

Сеансы управления к устройствам позволяют вам способность просмотреть и собрать информацию об устройстве и его операциях. Если эта информация раскрыта

злонамеренному пользователю, устройство может стать целью атаки, поставившей под угрозу и используемой для выполнения дополнительных атак. У любого с привилегированным адресом к устройству есть возможность полного административного контроля того устройства. Обязательно защитить сеансы управления для предотвращения информационного раскрытия и неавторизованный доступа.

Защита панели управления

В программном обеспечении Cisco IOS версии 12.4(6)T и позже, Защита панели управления (MPP) функции позволяет администратору ограничивать, на котором трафик управления интерфейсов может быть получен устройством. Это позволяет администратору дополнительный контроль над устройством и как обращаются к устройству.

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

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

См. Защиту Панели управления для получения дополнительной информации о MPP.

Защита уровня управления

Защита Уровня управления (CPPr) основывается на функциональности Контроля уровня управления, чтобы ограничить и определить политику трафика уровня управления, который предназначен к процессору маршрута устройства IOS. CPPr, добавленный в программном обеспечении Cisco IOS версии 12.4(4)T, делит уровень управления на отдельные категории уровня управления, которые известны как подинтерфейсы. Существуют три подинтерфейса уровня управления: Хост, Транзит и Исключение CEF. Кроме того, CPPr включает эти дополнительные защитные функции уровня управления:

- **Функция фильтрации порта -** Эта функция обеспечивает применение политик или отбрасывание пакетов, которые переходят к закрытому или неслушающему TCP и портам UDP.

- **Функция применения политик порога очереди** - Эта функция ограничивает количество пакетов для указанного протокола, которые позволены во входной очереди IP уровня управления.

CPPr позволяет администратору классифицировать, определять политику, и ограничивать трафик, который передается устройству для целей управления с подинтерфейсом хоста. Примеры пакетов, которые классифицированы для категории подинтерфейса хоста, включают трафик управления, такой как SSH или Telnet и протоколы маршрутизации.

> **Примечание:** CPPr не поддерживает IPv6 и ограничен путем ввода IPv4.

См. Руководство Защитной функции Уровня управления - 12.4T и Понимание Защиты Уровня управления для получения дополнительной информации о Cisco функция CPPr.

Зашифруйте сеансы управления

Поскольку информация может быть раскрыта на интерактивном сеансе управления, этот трафик должен быть зашифрован так, чтобы злонамеренный пользователь не мог получить доступ к данным, которые переданы. Шифрование трафика позволяет безопасное соединение удаленного доступа с устройством. Если трафик для сеанса управления передается по сети в открытом тексте, атакующий может получить уязвимые данные об устройстве и сети.

Администратор в состоянии установить зашифрованное и безопасное подключение управления удаленного доступа к устройству с SSH или HTTPS (Протокол защищенной передачи гипертекста) функции. Программное обеспечение Cisco IOS поддерживает Версию SSH 1.0 (SSHv1), Версию SSH 2.0 (SSHv2) и HTTPS, который использует Уровень защищенных сокетов (SSL) и Transport Layer Security (TLS) для аутентификации и шифрования данных. SSHv1 и SSHv2 не совместимы. SSHv1 неуверен и не стандартизированный, таким образом, не рекомендуется, если SSHv2 является опцией.

Программное обеспечение Cisco IOS также поддерживает протокол SCP, который позволяет зашифрованное и безопасное соединение для копирования конфигураций устройства или образов программного обеспечения. SCP полагается на SSH. Конфигурация данного примера включает SSH на устройстве Cisco IOS:

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

Этот пример конфигурации включает сервисы SCP:

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

Это - пример конфигурации для сервисов HTTPS:

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

См. Configuring Secure Shell на маршрутизаторах и Коммутаторах Рабочая Cisco IOS и часто задаваемые вопросы Secure Shell (SSH) для получения дополнительной информации о функции SSH программного обеспечения Cisco IOS.

SSHv2

Функция поддержки SSHv2, представленная в программном обеспечении Cisco IOS версии 12.3(4)T, позволяет пользователю настраивать SSHv2. (Поддержка SSHv1 была внедрена в более раннем релизе программного обеспечения Cisco IOS.) SSH выполняется поверх уровня надежности передачи и предоставляет строгую проверку подлинности и возможности шифрования. Единственная надежность передачи, которая определена для SSH, является TCP. SSH предоставляет средство надежно обратиться и надежно выполнить команды на другом компьютере или устройстве по сети. Функция протокола SCP, которая туннелирована по SSH, обеспечивает безопасную передачу файлов.

Если **команда verson 2 ip ssh** явно не настроена, то Cisco IOS включает Версию SSH 1.99. Версия SSH 1.99 позволяет и SSHv1 и соединения SSHv2. SSHv1, как полагают, неуверен и может иметь негативные эффекты на систему. Если SSH включен, рекомендуется отключить SSHv1 при помощи **ip ssh version 2** команды.

Конфигурация данного примера 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
```

См. Поддержку Версии 2 Secure Shell для получения дополнительной информации об использовании SSHv2.

Усовершенствования SSHv2 для ключей RSA

Cisco IOS SSHv2 поддерживает интерактивные клавиатурой и основанные на пароле методы аутентификации. Усовершенствования SSHv2 для функции Ключей RSA также поддерживают основанную на RSA аутентификацию с открытым ключом для клиента и сервера.

Для проверки подлинности пользователя основанная на RSA проверка подлинности пользователя использует частное / пару открытых ключей, привязанную к каждому пользователю для аутентификации. Пользователь должен генерировать частное / пару открытых ключей на клиенте и настроить открытый ключ на сервере SSH Cisco IOS для завершения аутентификации.

Пользователь SSH, который пытается установить учетные данные, предоставляет зашифрованной подписи секретный ключ. Подпись и открытый ключ пользователя передаются серверу SSH для аутентификации. Сервер SSH вычисляет хэш по открытому ключу, предоставленному пользователем. Хэш используется, чтобы определить, имеет ли сервер запись, которая совпадает. Если соответствие найдено, основанная на RSA проверка сообщения выполнена с открытым ключом. Следовательно, пользователь аутентифицируется или запрещенный доступ на основе зашифрованной подписи.

Для проверки подлинности сервера Клиент SSH Cisco IOS должен назначить ключ хоста для каждого сервера. Когда клиент пытается установить Сеанс SSH с сервером, это получает подпись сервера как часть сообщения обмена ключами. Если строгий флаг проверки ключа хоста включен на клиенте, клиентские проверки, имеет ли он запись ключа хоста, которая соответствует предварительно сконфигурированному серверу. Если соответствие найдено, клиент пытается проверить подпись с ключом сервера. Если сервер успешно аутентифицируется, установка сеанса продолжается; иначе это завершено и отображает **Сообщение об ошибках Проверки подлинности сервера**.

Конфигурация данного примера включает 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
```

См. Усовершенствования Версии 2 Secure Shell для Ключей RSA для получения дополнительной информации об использовании ключей RSA с SSHv2.

Конфигурация данного примера позволяет серверу SSH Cisco IOS выполнить основанную на RSA проверку подлинности пользователя. Если открытый ключ RSA, сохраненный на сервере, проверен с общественностью или парой с закрытым ключом, сохраненной на клиенте, проверка подлинности пользователя успешна.

```
!
! 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.)
!
```

См. Настройку Сервер SSH Cisco IOS для Выполнения Основанной на RSA Проверки подлинности пользователя для получения дополнительной информации об использовании ключей RSA с SSHv2.

Конфигурация данного примера позволяет Клиенту SSH Cisco IOS выполнить основанную на RSA проверку подлинности сервера.

```
!
!

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
!
```

См. Настройку Клиент SSH Cisco IOS для Выполнения Основанной на RSA Проверки подлинности сервера для получения дополнительной информации об использовании ключей RSA с SSHv2.

Консоль и порты AUX

В устройствах Cisco IOS консоль 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 выполнения восстановления пароля у не прошедшего поверку подлинности атакующего должен был бы быть доступ к консольному порту и способности прервать питание к устройству или заставить устройство завершаться катастрофическим отказом.

Любой метод, используемый для доступа к консольному порту устройства, должен быть защищен способом, который равен безопасности, которая принуждена для привилегированного адреса к устройству. Методы использовали, чтобы к безопасному доступу должен включать использование AAA, exec-timeout и паролей модема, если модем присоединен к консоли.

Если восстановление пароля не требуется, то администратор может удалить способность выполнить процедуру восстановления пароля с помощью команды глобальной кофигурации **password-recovery no service**; однако, как только **команда no service password-recovery** была включена, администратор больше не может выполнять восстановление пароля на устройстве.

В большинстве ситуаций Порт AUX устройства должен быть отключен для предотвращения неавторизованный доступа. Порт AUX может быть отключен с этими 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
!
```

VTY контроля и Линии tty

Интерактивные сеансы управления в программном обеспечении Cisco IOS используют tty или действительный tty (VTY). Tty является локальной асинхронной линией, к которой терминал может быть подключен для локального доступа к устройству или к модему для удаленного доступа к устройству. Обратите внимание на то, что tty могут использоваться для соединений с консольными портами других устройств. Эта функция позволяет устройству с линиями tty действовать как сервер консоли, где соединения могут быть установлены по сети к консольным портам устройств, связанных с линиями tty. Линии tty для этих обратных подключений по сети должны также управляться.

Линия VTY используется для всех других удаленных сетевых соединений, поддерживаемых устройством, независимо от протокола (SSH, SCP, или Telnet является примерами). Чтобы гарантировать, что к устройству можно обратиться через локальный или удаленный сеанс управления, надлежащие средства управления должны быть принуждены и на VTY и на линиях tty. Устройства Cisco IOS имеют ограниченное число линий VTY; количество доступных линий может быть определено с командой EXEC выставочного подвида. Когда все линии VTY используются, новые сеансы управления не могут быть установлены, который создает условие DoS для доступа к устройству.

Самая простая форма управления доступом к VTY или tty устройства с помощью аутентификации на всех линиях независимо от размещения устройства в сети. Это важно для линий VTY, потому что они доступны через сеть. Линия tty, которая связана с модемом, который используется для удаленного доступа к устройству, или линия tty, которая связана с консольным портом других устройств, также доступна через сеть. Если вы применяете списки доступа к интерфейсам на устройстве, другие формы VTY и управлений доступом tty могут быть принуждены с transport input или командами настройки access-class с использованием CoPP и функций CPPr, или.

Аутентификация может быть принуждена с помощью AAA, который является рекомендуемым методом для аутентифицируемого доступа к устройству с использованием базы локальных пользователей, или простой проверкой подлинности пароля, настроенной непосредственно на линии tty или VTY.

Команда exec-timeout должна использоваться, чтобы выйти из системы сеансы на VTY или линиях tty, которые оставляют простаивающими. Команда service tcp-keepalives-in должна

также использоваться для включения TCP keepalife на входящих соединениях к устройству. Это гарантирует, что устройство на удаленном конце соединения все еще доступно и что полуоткрытые или осиротевшие соединения удалены из локального устройства IOS.

Транспорт контроля для VTY и Линий tty

VTY и tty должны быть настроены, чтобы принять только зашифрованный и защитить подключения управления удаленного доступа к устройству или через устройство, если это используется в качестве сервера консоли. Этот раздел обращается к tty, потому что такие линии могут быть связаны с консольными портами на других устройствах, которые позволяют tty быть доступным по сети. Чтобы предотвратить информационное раскрытие или неавторизованный доступ к данным, которые переданы между администратором и устройством, **transport input ssh** должен использоваться вместо протоколов открытого текста, таких как Telnet и rlogin. Конфигурация **transport input none** может быть включена на tty, который в действительности отключает использование линии tty для обратных консольных соединений.

И VTY и линии tty позволяют администратору соединяться с другими устройствами. Для ограничения типа транспорта, который администратор может использовать для исходящих соединений, использовать команду конфигурации с командной строки **transport output**. Если исходящие соединения не необходимы, то **transport output ни один** не должен использоваться. Однако, если исходящие соединения позволены, то зашифрованный и безопасный метод удаленного доступа для соединения должен быть принужден с помощью **ssh transport output**.

> **Примечание:** IPSec может использоваться для зашифрованных и безопасных соединений удаленного доступа с устройством, если поддерживается. При использовании IPSec он также добавляет дополнительные служебные данные ЦПУ к устройству. Однако SSH должен все еще быть принужден как транспорт, даже когда используется IPSec.

Предупреждающие сообщения

В некоторой юридической юрисдикции может быть невозможно преследовать по суду и недопустимый для мониторинга злонамеренных пользователей, пока они не были уведомлены, что им не разрешают использовать систему. Один метод для обеспечения этого уведомления должен разместить эту информацию в сообщение баннера, которое настроено с командой banner login программного обеспечения Cisco IOS.

Юридические требования сложны, варьируются юрисдикцией и ситуацией, и должны быть обсуждены с юрисконсультом. Даже в юрисдикции, юридические заключения могут отличаться. В сотрудничестве с адвокатом баннер может предоставить некоторых или всю эту информацию:

- Заметьте, что в систему должны войти или использовать только в частности авторизованный персонал и возможно информация о том, кто может авторизовать использование.
- Заметьте, что любое неавторизованное использование системы незаконно и может подвергнуться гражданско-правовым санкциям и уголовным наказаниям.

- Заметьте, что любое использование системы может быть зарегистрировано или проверено без дополнительного замечания и что результирующие журналы могут использоваться в качестве доказательства в суде.

- Определенные предупреждения требуются местными законодательствами.

От точки зрения безопасности, а не законный, баннер входа в систему не должен содержать определенную информацию об имени маршрутизатора, модели, программном обеспечении или владении. Этой информацией могут злоупотребить злонамеренные пользователи.

Аутентификация, авторизация и учет

Платформа Аутентификации, авторизации и учета (AAA) важна для обеспечения интерактивного доступа к сетевым устройствам. Инфраструктура AAA предоставляет высоконастраиваемую среду, которая может быть адаптирована на основе потребностей сети.

Аутентификация TACACS+

TACACS + является протоколом аутентификации, который устройства Cisco IOS могут использовать для аутентификации пользовательских интерфейсов управления против удаленного AAA-сервера. Эти пользовательские интерфейсы управления могут обратиться к устройству IOS через SSH, HTTPS, telnet или HTTP.

TACACS + аутентификация, или более широко аутентификация AAA (проверка подлинности, авторизация и учет), предоставляет способность использовать учетные записи отдельного пользователя на каждого администратора сети. Когда вы не зависите от одиночного совместно используемого пароля, безопасность сети улучшена, и ваша отслеживаемость усилена.

RADIUS является протоколом, подобным в цели к TACACS +; однако, это только шифрует пароль, передаваемый по сети. Напротив, TACACS + шифрует все Содержимое tcp, которое включает обоих имя пользователя и пароль. Когда TACACS + поддерживается AAA-сервером, поэтому TACACS + должен использоваться в предпочтении к RADIUS. См. TACACS + и Сравнение RADIUS для более подробного сравнения этих двух протоколов.

TACACS + аутентификация может быть включен на устройстве Cisco IOS с конфигурацией, подобной данному примеру:

```
!
!

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 специфичного для организации шаблона аутентификации AAA (проверка подлинности, авторизация и учет). См. Аутентификацию, авторизацию и учет для получения дополнительной информации о конфигурации AAA.

Список методов является последовательным списком, который описывает методы аутентификации, которые будут делать запрос, для аутентификации пользователя. Списки методов позволяют вам определять один или несколько протоколов безопасности использоваться для аутентификации, и таким образом гарантировать резервную систему для аутентификации в случае, если отказывает начальный метод. Программное обеспечение Cisco IOS использует первый перечисленный метод, который успешно принимает или отклоняет пользователя. Последующие методы только предприняты в случаях, где более ранние методы отказывают из-за недоступности сервера или некорректной конфигурации.

См. Именованные Списки методов для Аутентификации для получения дополнительной информации о конфигурации Именованных Списков методов.

Authentication Fallback

Если весь настроенный TACACS + серверы становятся недоступными, то устройство Cisco IOS может полагаться на протоколы вспомогательной проверки подлинности. Если все настроенные TACACS + серверы недоступны, типичные конфигурации включают использование локальной переменной или включают аутентификацию.

Полный список опций для на Устройстве аутентификации включает, включают, локальный, и линия. Каждая из этих опций имеет преимущества. Использование enable secret предпочтено, потому что тайна хеширована с односторонним алгоритмом, который по сути более безопасен, чем алгоритм шифрования, который используется с паролями Типа 7 для линии или локальной проверки подлинности.

Однако на Cisco IOS Software Release, которые поддерживают использование секретных паролей для локально определенных пользователей, нейтрализация к локальной проверке подлинности может быть выбираемой. Это обеспечивает локально определенного пользователя, чтобы быть созданным для одного или более администраторов сети. Если TACACS + должны были стать абсолютно недоступными, каждый администратор может

использовать их локальное имя пользователя и пароль. Несмотря на то, что это действие действительно улучшает отслеживаемость администраторов сети в TACACS + простои, это значительно увеличивает административные накладные расходы, потому что должны быть поддержаны учетные записи локального пользователя на всех сетевых устройствах.

Этот пример конфигурации полагается на предыдущий TACACS + пример аутентификации для включения аутентификации нейтрализации в пароль, который настроен локально с **командой 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
!
```

См. Аутентификацию Настройки для получения дополнительной информации об использовании аутентификации нейтрализации с AAA.

Использование паролей типа 7

Первоначально разработанный для разрешения быстрой расшифровки сохраненных паролей, пароли Типа 7 не являются безопасной формой хранения пароля. Существует много программных средств, доступных, который может легко дешифровать эти пароли. Использования паролей Типа 7 нужно избежать, пока не требуется функцией, которая используется на устройстве Cisco IOS.

Удаление паролей этого типа может быть упрощено посредством аутентификации AAA (проверка подлинности, авторизация и учет) и использования функции Enhanced Password Security, которая позволяет секретным паролям использоваться с пользователями, которые

локально определены через команду глобальной кофигурации **имени пользователя**. Если вы не можете полностью предотвратить использование паролей Типа 7, считайте эти пароли запутываемыми, не зашифрованный.

Посмотрите, что Плоскость Общего менеджмента Укрепляет раздел этого документа для получения дополнительной информации об удалении паролей Типа 7.

Авторизация TACACS+ Command

Авторизация для выполнения команд с TACACS + и AAA предоставляет механизм, который разрешает или запрещает каждую команду, которая введена административным пользователем. Когда пользователь вводит команды EXEC, Cisco IOS передает каждую команду к настроенному AAA-серверу. AAA-сервер тогда использует свою настроенную политику для permit or deny команды для того индивидуального пользователя.

Эта конфигурация может быть добавлена к предыдущему примеру аутентификации AAA (проверка подлинности, авторизация и учет) для реализации авторизации для 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
!
```

См. Авторизацию Настройки для получения дополнительной информации об авторизации для выполнения команд.

TACACS + учет команды

Когда настроено, учет команды AAA передает информацию о каждой команде EXEC, которая введена в настроенный TACACS + серверы. Информация передала к TACACS +, сервер включает выполняемую команду, дата, это выполнялось, и имя пользователя пользователя, который вводит команду. Учет команды не поддерживается с RADIUS.

Конфигурация данного примера включает команду AAA, составляющую команды EXEC, введенные в нуль уровней привилегий, один, и 15. Эта конфигурация полагается на предыдущие примеры, которые включают 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
!
```

См. Настройку, Составляющую дополнительные сведения о конфигурации учета AAA.

Избыточные AAA-серверы

AAA-серверы, которые усилены в среде, должны быть избыточными и развернуты отказоустойчивым способом. Это помогает гарантировать, что интерактивный управляющий доступ, такой как SSH, возможен, если AAA-сервер недоступен.

Когда вы разработаете или внедрите избыточное решение для AAA-сервера, помните эти факторы:

- Доступность AAA-серверов во время сбоев потенциальной сети
- Географически рассеянное размещение AAA-серверов

- Загрузка на отдельных AAA-серверах в установившемся и неисправных состояниях
- Задержка сети между Серверами доступа к сети и AAA-серверами
- Синхронизация баз данных AAA-сервера

См. Развертывают Access Control Server для получения дополнительной информации.

Укрепите простой протокол управления сетью

Этот раздел выделяет несколько методов, которые могут использоваться для обеспечения развертываний SNMP в устройствах IOS. Важно, что SNMP должным образом защищен для защиты конфиденциальности, целостности и доступности и сетевых данных и сетевых устройств, через которые передают транзитом эти данные. SNMP предоставляет вам полную информацию на состоянии сетевых устройств. Эта информация должна быть защищена от злонамеренных пользователей, которые хотят усилить эти данные для выполнения атак на сеть.

Строки имени и пароля SNMP

Строки имени и пароля являются паролями, которые применены к устройству IOS для ограничения доступа, и только для чтения и доступ для чтения-записи, к данным SNMP на устройстве. Эти строки имени и пароля, как со всеми паролями, должны быть тщательно выбраны, чтобы гарантировать, что они не тривиальны. Строки имени и пароля должны быть изменены через определенные промежутки времени и в соответствии с политикой сетевой безопасности. Например, когда администратор сети изменяет роли или покидает компанию, строки должны быть изменены.

Эти строки настройки настраивают строку имени и пароля только для чтения READONLY и строку имени и пароля для чтения и записи ЧТЕНИЯ-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 строки имени и пароля были выбраны для ясного объяснения использования этих строк. Для производственных сред строки имени и пароля должны быть выбраны с осторожностью и должны состоять из серии алфавитных, числовых, и неалфавитно-цифровых символов. См. Рекомендации для Создания Стойких паролей для получения дополнительной информации о выборе нетривиальных паролей.

См. Справочник по командам SNMP IOS для получения дополнительной информации об этой функции.

Строки имени и пароля SNMP с ACL

В дополнение к строке имени и пароля ACL должен быть применен, который далее ограничивает доступ SNMP к избранной группе IP - адресов источника. Эта конфигурация ограничивает доступ только на чтение SNMP устройствами конечного хоста, которые находятся в 192.168.100.0/24 адресном пространстве, и ограничивает доступ для чтения-записи SNMP только устройством конечного хоста в 192.168.100.1.

> **Примечание:** Устройства, которые разрешены этими ACL, требуют надлежащей строки имени и пароля для доступа к запрошенным сведениям 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
!
```

См. snmp-server community в Ссылке Команды управления Cisco IOS network для получения дополнительной информации об этой функции.

Инфраструктурные списки ACL

ACL инфраструктуры (iACLs) могут быть развернуты, чтобы гарантировать, что только конечные хосты с доверяемыми IP-адресами могут передать трафик SNMP к устройству IOS. iACL должен содержать политику, которая запрещает неавторизованные Пакеты snmp на порту 161 UDP.

Посмотрите Ограничивающий Доступ к Сети с разделом ACL Инфраструктуры этого документа для получения дополнительной информации об использовании iACLs.

Представления SNMP

Представления SNMP являются характеристикой безопасности, которая может permit or deny доступ к определенным SNMP MIB. Как только представление создано и применено к строка имени и пароля с **snmp-server community** команды глобальной кофигурации представления community-string при доступе к данным базы управляющей информации (MIB) вы ограничены разрешениями, которые определены представлением. Когда соответствующий, вам рекомендуют использовать представления для ограничения пользователей SNMP к данным, которых они требуют.

Этот пример конфигурации ограничивает доступ SNMP со строкой имени и пароля LIMITED к данным базы управляющей информации (MIB), которые расположены 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
!
```

См. Поддержку SNMP Настройки для получения дополнительной информации.

Протокол SNMP версии 3

SNMP Version 3 (SNMPv3) определен RFC3410, RFC3411, RFC3412, RFC3413, RFC3414 и RFC3415 и является протоколом на основе стандартов взаимодействия для управления сетью. SNMPv3 предоставляет безопасный доступ устройствам, потому что это аутентифицирует и дополнительно шифрует пакеты по сети. Где поддерживается, когда вы развертываете SNMP, SNMPv3 может использоваться для добавления другого уровня безопасности. SNMPv3 состоит из трех основных параметров конфигурации:

- **никакая аутентификация** - Этот режим не требует никакой аутентификации, ни любого шифрования Пакетов snmp
- **auth** - Этот режим требует аутентификации Пакета snmp без шифрования
- **priv** - Этот режим требует и аутентификации и шифрования (конфиденциальность) каждого Пакета snmp

Авторитетный идентификатор ядра должен существовать для использования механизмов обеспечения безопасности SNMPv3 - аутентификации или аутентификации и шифрования - для обработки Пакетов snmp; по умолчанию идентификатор ядра генерируется локально. Идентификатор ядра может быть отображен с **командой show snmp engineID** как показано в данном примере:

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

> **Примечание:** Если engineID изменен, все учетные записи пользователя SNMP должны быть реконфигурированы.

Следующий шаг должен настроить группу SNMPv3. Эта команда настраивает устройство Cisco IOS для SNMPv3 с группой сервера SNMP AUTHGROUP и включает только аутентификацию для этой группы с **подлинным** ключевым словом:

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

Эта команда настраивает устройство Cisco IOS для SNMPv3 с группой сервера SNMP PRIVGROUP и включает и 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 паролем Аутентификации MD5 **authpassword** и паролем шифрования 3DES **privpassword**:

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

Обратите внимание на то, что команды настройки **snmp-server user** не отображены в выходных данных конфигурации устройства как требуется RFC 3414; поэтому, пароль пользователя не доступен для просмотра от конфигурации. Для просмотра настроенных пользователей введите **команду show snmp user** как показано в данный пример:

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

См. Поддержку SNMP Настройки для получения дополнительной информации об этой функции.

Защита панели управления

Функция Защиты панели управления (MPP) в программном обеспечении Cisco IOS может быть использована, чтобы помочь защищать SNMP, потому что это ограничивает интерфейсы, через которые трафик SNMP может завершиться на устройстве. Функция MPP позволяет администратору определять один или несколько интерфейсов как интерфейсы управления. Трафику управления разрешают ввести устройство только через эти интерфейсы управления. После того, как MPP включен, никакие интерфейсы кроме определяемых интерфейсов управления не принимают трафик при управлении сетью, который предназначен к устройству.

Обратите внимание на то, что MPP является подмножеством функции CPPr и требует версии IOS, которая поддерживает CPPr. См. Понимание Защиты Уровня управления для получения дополнительной информации о CPPr.

В данном примере MPP используется для ограничения SNMP и доступа SSH к только интерфейсу FastEthernet 0/0:

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

См. Руководство Защитной функции Панели управления для получения дополнительной информации.

Оптимальные методы Регистрации

Регистрация событий предоставляет вас видимость в использование устройства Cisco IOS и сети, в которую это развернуто. Программное обеспечение Cisco IOS предоставляет несколько гибких параметров регистрации, которые могут помочь достигать управления сетью и целей видимости организации.

Эти разделы предоставляют некоторые основные оптимальные методы регистрации, которые могут помочь рычагам администратора, регистрирующим успешно при уменьшении влияния входа устройства Cisco IOS.

Передайте журналы к центральному месту расположения

Рекомендуется передать регистрационную информацию к удаленному серверу системного журнала. Это позволяет коррелировать и аудит сети и события связанное с безопасностью через сетевые устройства эффективнее. Обратите внимание на то, что сообщения системного журнала переданы ненадежно UDP и в открытом тексте. Поэтому любые меры защиты, которые сеть предоставляет трафику управления (например, шифрование или внеполосный доступ) должны быть расширены для включения трафика системного журнала.

Этот пример конфигурации настраивает устройство Cisco IOS для передачи регистрационной информации к удаленному серверу системного журнала:

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

См. Определение Инцидентов Использование Межсетевого экрана и Событий системного журнала (syslog) Маршрутизатора IOS для получения дополнительной информации о регистрационной корреляции.

Интегрированный в 12.4 (15) T и первоначально представленный в 12.0 (26) S, Регистрация к Локальной Энергонезависимой памяти (Диск ATA) функция позволяет сообщениям регистрации системы быть сохраненными на флэш диске прикрепления передовой технологии (ATA). Сообщения экономили на дисководе ATA, сохраняются после того, как маршрутизатор перезагружен.

Это строки настройки настраивает 134,217,728 байтов (128 МБ) сообщений регистрации к каталогу системного журнала флэш-памяти ATA (disk0), задавая размер файла 16,384 байтов:

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

Если существует достаточный объем свободной памяти на диске, прежде чем сообщения регистрации записаны в файл на диске ATA, проверки программного обеспечения Cisco IOS. В противном случае самый старый файл сообщений регистрации (меткой времени) удален, и текущий файл сохранен. Формат имени файла является **log_month:day:year::**

время.

> **Примечание:** Флэш-накопитель ATA ограничил дисковое пространство и таким образом должен быть поддержан, чтобы избежать перезаписывать Сохраненные данные.

Данный пример показывает, как скопировать сообщения регистрации от флэш диска ATA маршрутизатора до внешнего диска на сервере FTP 192.168.1.129 как часть процедур технического обслуживания:

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

См. Регистрацию к Локальной Энергонезависимой памяти (Диск ATA) для получения дополнительной информации об этой функции.

Уровень регистрации

Каждому сообщению журнала, которое генерируется устройством Cisco IOS, назначают одна из восьми степеней серьезности ошибки, которые колеблются от уровня 0, Аварийных ситуаций, через уровень 7, Отладку. Пока в частности не требуется, вам рекомендуют избежать регистрировать на уровне 7. Регистрация на уровне 7 производит поднятую Загрузку ЦПУ на устройстве, которое может привести к устройству и нестабильной работе сети.

Уровень прерывания регистрации команды глобальной кофигурации используется для определения, какие сообщения регистрации передаются удаленным серверам системного журнала. Заданный уровень указывает на самое низкое сообщение степеней серьезности ошибки, которое передается. Для буферизированной регистрации используется команда уровня **logging buffered**.

Этот пример конфигурации ограничивает сообщения журнала, которые передаются удаленным серверам системного журнала и локальному буферу журнала к степеням серьезности ошибки 6 (информационные) до 0 (аварийные ситуации):

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

См. Устранение проблем, Защиту от ошибок и неисправностей и Регистрацию для получения дополнительной информации.

Не регистрируйте к консоли или сеансам монитора

С программным обеспечением Cisco IOS возможно передать сообщения журнала к сеансам монитора - сеансы монитора являются интерактивными сеансами управления, на которых **команда terminal monitor** EXEC была выполнена - и к консоли. Однако это может поднять Загрузку ЦПУ устройства IOS и поэтому не рекомендуется. Вместо этого вам рекомендуют передать регистрационную информацию к локальному буферу журнала, который может быть просмотрен с **командой show logging**.

Используйте **консоль никакой регистрации** команд глобальной кофигурации и **no logging monitor** для отключения регистрации к консоли и сеансам монитора. Этот пример конфигурации показывает использование этих команд:

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

См. Ссылку Команды управления Cisco IOS network для получения дополнительной информации о командах глобальной кофигурации.

Используйте буферизированную Регистрацию

Программное обеспечение Cisco IOS поддерживает использование локального буфера журнала так, чтобы администратор мог просмотреть локально сообщения созданного журнала. Использование буферизированной регистрации настоятельно рекомендовано по сравнению с регистрацией или к консоли или к сеансам монитора.

Существует два параметра конфигурации, которые релевантны, когда настройка буферизовала регистрацию: размер буфера журнала и важность сообщения, который сохранен в буфере. Размер **буфера журнала** настроен с размером **logging buffered** команды глобальной кофигурации. Самые низкие степени серьезности ошибки, включенные в буфер, настроены с командой severity logging buffered. Администратор в состоянии просмотреть содержание буфера журнала посредством **команды show logging EXEC**.

Этот пример конфигурации включает конфигурацию буфера журнала 16384 байтов, а также степеней серьезности ошибки 6, информационный, который указывает, что хранятся сообщения на уровнях 0 (аварийные ситуации) до 6 (информационный):

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

См. Ссылку Команды управления Cisco IOS network для получения дополнительной информации о буферизированной регистрации.

Настройте исходный интерфейс Регистрации

Для обеспечения увеличенного уровня непротиворечивости, когда вы собираете и рассматриваете сообщения журнала, вам рекомендуют статически настроить исходный интерфейс регистрации. Выполненный через команду интерфейса **logging source-interface**, статически настраивая исходный интерфейс регистрации гарантирует, что тот же IP-адрес появляется во всех сообщениях регистрации, которые передаются от отдельного устройства Cisco IOS. Для добавленной устойчивости вам рекомендуют использовать интерфейс обратной связи в качестве источника регистрации.

Этот пример конфигурации иллюстрирует использование команды глобальной кофигурации интерфейса **logging source-interface**, чтобы указать что IP-адрес loopback 0 интерфейсов использоваться для всех сообщений журнала:

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

См. Ссылку Команды Cisco IOS для получения дополнительной информации.

Настройте метки времени регистрации

Конфигурация меток времени регистрации помогает вам коррелировать события через сетевые устройства. Важно внедрить корректную и последовательную конфигурацию метки времени регистрации, чтобы гарантировать, что вы в состоянии сопоставить данные регистрации. Метки времени регистрации должны быть настроены, чтобы включать дату и времю с точностью миллисекунды и включать часовой пояс в использование на устройстве.

Данный пример включает конфигурацию меток времени регистрации с точностью

миллисекунды в течение Согласованного текущего времени (UTC) зона:

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

Если вы предпочитаете не регистрировать времена относительно UTC, можно настроить определенный местный часовой пояс и настроить ту информацию для присутствования в сообщениях созданного журнала. Данный пример показывает конфигурацию устройства для зоны Тихоокеанского времени (PST):

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

Менеджмент конфигурации программного обеспечения Cisco IOS

Программное обеспечение Cisco IOS включает несколько функций, которые могут включить форму управления конфигурацией на устройстве Cisco IOS. Такие функции включают функциональность, чтобы заархивировать конфигурации и откатывать конфигурацию к предыдущей версии, а также создать журнал изменений подробной конфигурации.

Замена конфигурации и откат конфигурации

В программном обеспечении Cisco IOS версии 12.3(7)T и позже, функции Замены и Отката конфигурации Конфигурации позволяют вам архивировать конфигурацию устройства Cisco IOS на устройстве. Сохраненный вручную или автоматически, конфигурации в этом архиве могут использоваться для замены текущей рабочей конфигурации командой имени файла **configure replace**. Это в отличие от **команды running-config** имени файла **копии**. Команда имени файла **configure replace** заменяет рабочую конфигурацию в противоположность слиянию, выполненному командой **копии**.

Рекомендуется активировать эту опцию на всех устройствах Cisco IOS в сети. После того, как включенный, администратор может заставить текущую рабочую конфигурацию быть добавленной к архиву с командой EXEC **archive config**, которой дают привилегию. Заархивированные конфигурации могут быть просмотрены с командой EXEC **show archive**.

Данный пример иллюстрирует конфигурацию архивации автоматической конфигурации. Данный пример дает устройству Cisco IOS команду хранить заархивированные конфигурации как файлы, названные archived-config-N на disk0: файловая система, чтобы поддержать максимум 14 резервных копий и заархивировать один раз в день (1440 минут) и когда администратор выполняет команду EXEC **write memory**.

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

Несмотря на то, что функциональность архивной конфигурации может сохранить до 14 резервных копирований конфигурации, вам рекомендуют рассмотреть требования к пространству перед использованием **максимальной** команды.

Исключительный доступ изменения конфигурации

Добавленный к программному обеспечению Cisco IOS версии 12.3(14)T, Исключительное Свойство доступа Изменения конфигурации гарантирует, что только один администратор изменяет конфигурацию устройства Cisco IOS в установленный срок. Эта функция помогает устранять нежелательное воздействие одновременных изменений, внесенных в компоненты связанной конфигурации. Эта функция настроена с режимом **configuration mode exclusive** команды глобальной кофигурации и работает в одном из двух режимов: автоматический и ручной. Когда администратор выполняет команду EXEC **configure terminal,** в автоматическом режиме конфигурация автоматически блокирует. В ручном режиме администратор

использует команду **блокировки configure terminal** для блокировки конфигурации, когда это вводит режим конфигурации.

Данный пример иллюстрирует конфигурацию этой функции блокировки автоматической конфигурации:

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

Программное обеспечение Cisco IOS эластичная конфигурация

Добавленный в программном обеспечении Cisco IOS версии 12.3(8)T, Эластичная функция Конфигурации позволяет надежно сохранить копию Образа ПО Cisco IOS и конфигурации устройства, которая в настоящее время используется устройством Cisco IOS. Когда эта опция активирована, не возможно изменить или удалить эти резервные файлы. Рекомендуется активировать эту опцию для предотвращения и непреднамеренных и злонамеренных попыток удалить эти файлы.

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

Как только эта опция активирована, возможно восстановить удаленную конфигурацию или Образ ПО Cisco IOS. Текущее активное состояние этой функции может быть отображено с **показом безопасная загрузочная** команда EXEC.

Снабженное цифровой подписью программное обеспечение Cisco

Добавленный в программном обеспечении Cisco IOS версии 15.0(1)M для Cisco 1900, 2900 и маршрутизаторах серии 3900, Снабженная цифровой подписью функция Программного обеспечения Cisco упрощает использование программного обеспечения Cisco IOS, которое снабжают цифровой подписью и таким образом доверяют с использованием безопасных, асимметричных (общий ключ) криптография.

Снабженный цифровой подписью образ несет зашифрованный (с секретным ключом) хэш себя. На проверку устройство дешифрует хэш с соответствующим открытым ключом от ключей, которые это имеет в его базе ключей и также вычисляет свой собственный хэш образа. Если дешифрованный хэш совпадает с расчетным хэшем образа, в образ не вмешались и можно доверять.

Снабженные цифровой подписью ключи Программного обеспечения Cisco определены типом и версией ключа. Ключ может быть специальным предложением, производством или типом ключа одновременного нажатия клавиш. Производство и специальные ключевые типы имеют связанную ключевую версию, которая инкрементно увеличивается в алфавитном порядке каждый раз, когда ключ отозван и заменен. Когда вы используете Снабженную цифровой подписью функцию Программного обеспечения Cisco, ROMMON и обычные Образы Cisco IOS оба подписаны со специальным ключом или производственным ключом. Образ ROMMON обновляем и должен быть подписан с тем же ключом как специальное предложение или производственный образ, который загружен.

Эта команда проверяет целостность образа c3900-universalk9-mz. SSA во флэш-памяти с ключами в базе 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 3.1.0 Cisco IOS XE. SG для Cisco Catalyst Коммутаторы серии E 4500.

См. Снабженное цифровой подписью Программное обеспечение Cisco для получения дополнительной информации об этой функции.

В программном обеспечении Cisco IOS версии 15.1(1)T и позже, была представлена Ключевая Замена для Снабженного цифровой подписью Программного обеспечения Cisco. Ключевая замена и аннулирование заменяют и удаляют ключ, который используется для Снабженной цифровой подписью проверки Программного обеспечения Cisco от хранения ключей платформы. Только особенный и производственные ключи может быть отозван в случае ключевого компромисса.

Новое (особенный или производство) ключ для (особенный или производство) образ входит (производство или аннулирование) образ, который используется для отмены предыдущего специального предложения или производственного ключа. Целостность образа аннулирования проверена с ключом одновременного нажатия клавиш, который прибывает предварительно сохраненный в платформу. Ключ одновременного нажатия клавиш не изменяется. При отмене производственного ключа после того, как образ аннулирования загружен, новый ключ, который он несет, добавлен к базе ключей, и соответствующий старый ключ может быть отозван, пока Образ ROMMON обновлен, и новый производственный образ загружен. При отмене специального ключа производственный образ загружен. Этот образ добавляет новый специальный ключ и может отозвать старый специальный ключ. После вас upgrade ROMMON может быть загружен новый специальный образ.

Данный пример описывает аннулирование специального ключа. Эти команды добавляют новый специальный ключ к базе ключей от текущего производственного образа, копируют новый Образ ROMMON (C3900_rom-monitor.srec. SSB) к области хранения (usbflash0:), обновите файл ROMMON и отзовите старый специальный ключ:

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

Новый специальный образ (c3900-universalk9-mz. SSB), может тогда быть скопирован к флэш-памяти, которая будет загружена, и подпись образа проверена с недавно добавленным специальным ключом (.SSB):

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

Ключевое аннулирование и замена не поддерживаются на Catalyst 4500 Коммутаторы Серии E, которые выполняют программное обеспечение Cisco IOS XE, невзирая на то, что эти коммутаторы действительно поддерживают Снабженную цифровой подписью функцию Программного обеспечения Cisco.

См. Снабженный цифровой подписью раздел Аннулирования и Замены Ключа Программного обеспечения Cisco Снабженного цифровой подписью Программного обеспечения Cisco ведут для получения дополнительной информации об этой функции.

Уведомление изменения конфигурации и Регистрация

Уведомление Изменения конфигурации и Характеристика входа в систему, добавленная в программном обеспечении Cisco IOS версии 12.3(4)T, позволяют регистрировать изменения конфигурации, сделанные к устройству Cisco IOS. Журнал поддержан на устройстве Cisco IOS и содержит сведения о пользователе частного лица, которое внесло изменение, команда настройки введенный, и время, когда было внесено изменение. Эта функциональность добавлена с командой режима конфигурации регистратора изменения конфигурации **logging enable**. **Hidekeys** дополнительных команд и записи **logging size**

используются для улучшения конфигурации по умолчанию becuase, они предотвращают регистрацию данных пароля и увеличивают длину журнала изменений.

Рекомендуется добавить эту функциональность так, чтобы история изменения конфигурации устройства Cisco IOS могла быть более понятной. Когда изменение конфигурации сделано, Кроме того, вам рекомендуют использовать команду настройки **notify syslog** для включения генерации сообщений системного журнала.

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

После Уведомления Изменения конфигурации и Характеристики входа в систему был включен, **config архивации журналов privileged EXEC command show, все** могут использоваться для просмотра журнала конфигурации.

Плоскость управления

Функции уровня управления состоят из протоколов и процессов, которые связываются между сетевыми устройствами для перемещения данных от источника до назначения. Это включает протоколы маршрутизации, такие как Border Gateway Protocol, а также протоколы как ICMP и Протокол RSVP.

Важно, чтобы события в управлении и плоскостях данных не оказывали негативное влияние на уровень управления. Если событие плоскости данных, такое как влияние атаки DoS уровень управления, вся сеть может стать нестабильной. Эта информация о функциях ПО Cisco IOS и конфигурациях может помочь гарантировать упругость уровня управления.

Общее укрепление уровня управления

Защита уровня управления сетевого устройства важна, потому что уровень управления гарантирует, что управление и плоскости данных поддержаны и в рабочем состоянии. Если уровень управления должен был стать нестабильным во время случая нарушения безопасности, для вас может быть невозможно восстановить устойчивость сети.

Во многих случаях можно отключить прием и передачу определенных типов сообщений на интерфейсе для уменьшения суммы Загрузки ЦПУ, которая требуется, чтобы обрабатывать ненужные пакеты.

Переадресации ICMP IP

Когда пакет получен и передан на том же интерфейсе, сообщение переадресации ICMP может генерироваться маршрутизатором. В этой ситуации маршрутизатор передает пакет и передает сообщение переадресации ICMP обратно в отправителя оригинального пакета. Это поведение позволяет отправителю обходить маршрутизатор и прямые последующие пакеты непосредственно назначению (или к маршрутизатору ближе назначению). В должным образом функционирующем IP - сети маршрутизатор передает перенаправления только к хостам на его собственных локальных подсетях. Другими словами, переадресации ICMP никогда не должны идти вне границы Уровня 3.

Существует два типа сообщений переадресации ICMP: перенаправление для адреса узла и перенаправление для подсети в целом. Злонамеренный пользователь может использовать способность маршрутизатора передать переадресации ICMP путем непрерывного передавания пакеты маршрутизатору, который вынуждает маршрутизатор ответить

сообщениями переадресации ICMP и результатами в неблагоприятном воздействии на ЦП и производительности маршрутизатора. Чтобы препятствовать тому, чтобы маршрутизатор передал переадресации ICMP, не используйте **IP** команду настройки интерфейса **перенаправлений**.

Недостижимый ICMP

Фильтрация со списком доступа к интерфейсам выявляет передачу сообщений о недоступности ICMP назад к источнику отфильтрованного трафика. Генерация этих сообщений может увеличить загрузку ЦПУ на устройстве. В программном обеспечении Cisco IOS генерация сообщения о недоступности ICMP ограничена одним пакетом каждые 500 миллисекунд по умолчанию. Генерация сообщения о недоступности ICMP может быть отключена с командой настройки интерфейса **никакой недостижимый ip**. Ограничение скорости сообщения о недоступности ICMP может быть изменено от по умолчанию с **rate-limit icmp команды глобальной конфигурации IP недостижимый** интервал в мс.

Протокол прокси-ARP

Прокси - протокол преобразования адресов является способом, в котором 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 к использованию прокси - протокола преобразования адресов. Это может привести к увеличению суммы трафика ARP на сегменте сети и истощения ресурсов и атак по перехвату и возможному изменению передаваемых данных. Прокси - протокол преобразования адресов представляет вектор атаки истощения ресурсов, потому что каждый проксированный запрос ARP использует малую величину памяти. Атакующий может быть в состоянии исчерпать всю доступную память, если она передает большое число запросов ARP.

Атаки по перехвату и возможному изменению передаваемых данных позволяют хосту в сети имитировать MAC-адрес маршрутизатора, который приводит к не подозревающим хостам, передающим трафик атакующему. Прокси - протокол преобразования адресов может быть отключен с **no ip proxy-arp** команды настройки интерфейса.

См. Включение Прокси - протокола преобразования адресов для получения дополнительной информации об этой функции.

Ограничьте влияние на ЦП трафика уровня управления

Защита уровня управления важна. Поскольку производительность приложения и производительность конечного пользователя могут пострадать без присутствия данных и трафика управления, жизнеспособность уровня управления гарантирует, что другие две плоскости поддержаны и в рабочем состоянии.

Поймите трафик уровня управления

Для надлежащей защиты уровня управления устройства Cisco IOS важно понять типы трафика, который является процессом, коммутированным ЦП. Обработайте коммутируемый трафик, обычно состоит из двух различных типов трафика. Первый тип трафика направлен к устройству Cisco IOS и должен быть обработан непосредственно ЦП устройства Cisco IOS. Этот трафик состоит из *Получить категории трафика смежности*. Этот трафик содержит запись в Таблице Cisco Expressorwarding (CEF), посредством чего следующий транзитный участок является самим устройством, которое обозначено условием, получают в выходных данных CLI **show ip cef**. Эта индикация имеет место для любого IP-адреса, который требует прямой обработки ЦП устройства Cisco IOS, который включает IP-адреса интерфейса, пространство адреса групповой адресации и пространство широковещательного адреса.

Второй тип трафика, который обрабатывается ЦП, является трафиком плоскости данных - трафиком с назначением вне самого устройства Cisco IOS - который требует специальной обработки ЦП. Несмотря на то, что не полный список ЦП, влияющего на трафик плоскости данных, эти типы трафика, является коммутированным процессом и может поэтому влиять на использование уровня управления:

- **Регистрация Списка контроля доступа** - трафик Регистрации ACL состоит из любых пакетов, которые генерируются из-за соответствия (permit or deny) ACE, на котором используется регистрационное ключевое слово.

- **Одноадресная пересылка по обратному пути (RPF Индивидуальной рассылки)** - RPF Индивидуальной рассылки, используемый в сочетании с ACL, может привести к коммутации в контексте процесса определенных пакетов.

- **IP - режимы** - Любые пакеты IP с включенными опциями должны быть обработаны ЦП.

- **Фрагментация** - Любой пакет IP, который требует фрагментации, нужно передать к ЦП для обработки.

- **Истечение времени существования (TTL)** - Пакеты, которые имеют значение TTL, меньше чем или равное, каждый требует, чтобы Превышенное Время Internet Control Message Protocol (ТИП ICMP 11, Код 0) сообщения было передано, который приводит к Обработке ЦПУ.

- **Недостижимый ICMP** - Пакеты, которые приводят к сообщениям о недоступности ICMP из-за маршрутизации, MTU или фильтрации, обработан ЦП.

- **Трафик, Требующий Запроса ARP** - Назначения, для которых не существует Запись ARP, требует обработки ЦП.

- **Не-IP трафик** - Весь не-IP трафик обработан ЦП.

Этот список подробно излагает несколько методов для определения, какие типы трафика обрабатываются ЦП устройства Cisco IOS:

- **Команда show ip cef** предоставляет информацию о следующем переходе для каждого префикса IP, который содержится в таблице CEF. Как обозначено ранее, записи, которые содержат, получают, поскольку "Следующий переход" рассматривают, получают смежности и указывают, что трафик должен быть передан непосредственно

ЦП.

- Команда **show interface switching** предоставляет сведения о количестве пакетов, которые являются процессом, коммутированным устройством.

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

  с локальным назначением (т.е. получите трафик смежности),с опциямиэто требует фрагментацииэто передается пространству широковещательного адресаэто передается пространству адреса групповой адресации

- Получите трафик смежности, может быть определен с помощью **команды show ip cache flow**. Любые потоки, которые предназначены к устройству Cisco IOS, имеют Интерфейс назначения (DstIf) локальной переменной.

- **Контроль уровня управления** может использоваться для определения типа и скорости трафика, который достигает уровня управления устройства Cisco IOS. Контроль уровня управления может быть выполнен с помощью разграниченной классификации ACL, регистрация и использование **команды show policy-map control-plane**.

Инфраструктурные списки ACL

ACL инфраструктуры (iACLs) ограничивают внешнюю связь устройствами сети. ACL инфраструктуры экстенсивно покрыты Предельным Доступом к Сети с разделом ACL Инфраструктуры этого документа.

Рекомендуется внедрить iACLs для защиты уровня управления всех сетевых устройств.

Списки ACL для входящего трафика

Для распределенных платформ Получите ACL (rACL), может быть опция для Cisco IOS Software Release 12.0 (21) S2 для 12000 (GSR), 12.0 (24) S для этих 7500, и 12.0 (31) S для 10720. RACL защищает устройство от вредного трафика, прежде чем трафик повлияет на процессор маршрута. Получите ACL, разработаны, чтобы только защитить устройство, на котором это настроено, и на транзитный трафик не влияет rACL. В результате IP - адрес назначения любой, который используется в записях ACL в качестве примера ниже только, обращается к медосмотру или виртуальным IP - адресам маршрутизатора. Получите ACL, также считаются оптимальным методом сетевой безопасности и должен быть рассмотрен как долгосрочное добавление к хорошей сетевой безопасности.

Это - ACL тракта приема, который записан для разрешения SSH (порт TCP 22) трафик от надежных хостов в 192.168.100.0/24 сети:

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

См. GSR: Получите Списки контроля доступа, чтобы помочь определять и позволять легальный трафик устройству и запрещать все нежелательные пакеты.

CoPP

Функция CoPP может также быть использована для ограничения пакетов IP, которые предназначены к устройству, относящемуся к инфраструктуре. В данном примере только трафику SSH от надежных хостов разрешают достигнуть ЦП устройства Cisco IOS.

> **Примечание:** Отбрасывание трафика от неизвестных или недоверяемых IP-адресов может предотвратить хосты с динамично-назначенными-IP-адресами с соединения на устройство Cisco IOS.

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

В предыдущем примере CoPP, записи ACL, которые совпадают с несанкционированными пакетами с результатом действия разрешения в сбросе этих пакетов функцией отбрасывания policy-map, в то время как на пакеты, которые совпадают с запрещать действием, не влияет функция отбрасывания policy-map.

CoPP доступен в Cisco IOS Software Release Train 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, и 12.4T.

См. Развертывающийся Контроль уровня управления для получения дополнительной информации о конфигурации и использовании функции CoPP.

Защита уровня управления

Защита Уровня управления (CPPr), представленный в программном обеспечении Cisco IOS версии 12.4(4)T, может использоваться, чтобы ограничить или определить политику трафика уровня управления, который предназначен к ЦП устройства Cisco IOS. В то время как подобный CoPP, CPPr имеет способность ограничить трафик с большой степенью детализации. CPPr делит составной уровень управления на три отдельных категории уровня управления, известные как подинтерфейсы. Подинтерфейсы существуют для Хоста, Транзита и категорий трафика Исключения CEF. Кроме того, CPPr включает эти защитные функции уровня управления:

- **Функция фильтрации порта -** Эта функция обеспечивает применение политик и отбрасывание пакетов, которые переданы к закрытому или неслушающему TCP или портам UDP.

- **Функция пороговой обработки очереди** - Эта функция ограничивает количество пакетов для указанного протокола, которые позволены во входной очереди IP уровня управления.

См. Защиту Уровня управления и Понимание Защиты Уровня управления (CPPr) для получения дополнительной информации о конфигурации и использовании функции CPPr.

Аппаратные ограничители скорости

Cisco Catalyst Supervisor Engine серии 6500 32 и поддержка модуля управления Supervisor Engine 720 определяемые платформой, аппаратные ограничители скорости (HWRLs) для специальных сетевых сценариев. Эти аппаратные ограничители скорости упоминаются как ограничители скорости особого случая, потому что они покрывают определенный предопределенный набор IPv4, IPv6, индивидуальной рассылки, и передают сценарии DoS в многоадресном режиме. HWRLs может защитить устройство Cisco IOS от множества атак, которые требуют, чтобы пакеты были обработаны ЦП.

Существует несколько HWRLs, которые включены по умолчанию. См. PFC3 Аппаратные Настройки по умолчанию Ограничителя Скорости для получения дополнительной информации.

См. Аппаратные Ограничители Скорости на PFC3 для получения дополнительной информации о HWRLs.

Безопасный BGP

Протокол BGP является основой маршрутизации Интернета. Также, любая организация с больше, чем скромными требованиями подключения часто использует BGP. BGP часто предназначается атакующими из-за его повсеместности и *набора, и забудьте* природу BGP - конфигураций в меньших организациях. Однако существует много специфичных для BGP характеристик безопасности, которые могут быть усилены для увеличения безопасности BGP - конфигурации.

Это предоставляет обзор самых важных характеристик безопасности BGP. Где это необходимо, рекомендации по конфигурации сделаны.

Основанные на TTL средства обеспечения безопасности

Каждый пакет IP содержит 1-байтовое поле, известное как Время жизни (TTL). Каждое устройство, что пакет IP пересекает декременты это значение одним. Начальное значение варьируется операционной системой и, как правило, колеблется от 64 до 255. Когда его значение TTL достигает нуля, пакет отброшен.

Известный и как Обобщенный основанный на TTL механизм обеспечения безопасности (GTSM) и как Взлом безопасности TTL BGP (BTSH), основанное на TTL средство обеспечения безопасности усиливает значение TTL пакетов IP, чтобы гарантировать, что пакеты BGP, которые получены, от непосредственно связанного узла. Эта функция часто требует координации от маршрутизаторов равноправного информационного обмена; однако, когда-то включенный, это может полностью победить, многие на основе TCP нападают против BGP.

GTSM для BGP включен с **опцией ttl-security** для **соседней** команды настройки маршрутизатора под управлением BGP. Данный пример иллюстрирует конфигурацию этой функции:

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

Поскольку пакеты BGP получены, значение TTL проверено и должно быть больше, чем или равным 255 минус заданное число переходов.

Аутентификация однорангового соединения по протоколу BGP с MD5

Аутентификация однорангового узла с MD5 создает дайджест MD5 каждого пакета, переданного как часть сеанса BGP. В частности части IP и заголовков TCP, Содержимого tcp и секретного ключа используются для генерации дайджеста.

Созданный дайджест тогда сохранен в Виде параметра TCP 19, который был создан в частности для этой цели RFC 2385 . Динамик BGP получения использует тот же алгоритм и секретный ключ для регенерации профиля сообщения. Если полученные и вычисленные

дайджесты не идентичны, от пакета сбрасывают.

Аутентификация однорангового узла с MD5 настроена с **параметром пароля** к **соседней** команде настройки маршрутизатора под управлением BGP. Использование этой команды проиллюстрировано следующим образом:

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

См. Аутентификацию Соседнего маршрутизатора для получения дополнительной информации об аутентификации Однорангового соединения по протоколу BGP с MD5.

Настройте максимальное число префиксов

Префиксы BGP сохранены маршрутизатором в памяти. Чем больше префиксов, которые должен держать маршрутизатор, тем большая память, которую должен использовать BGP. В некоторых конфигурациях подмножество всех интернет-префиксов может быть сохранено, такой как в конфигурациях, которые усиливают только маршрут по умолчанию или маршруты для сетей заказчика поставщика.

Для предотвращения исчерпания памяти важно настроить максимальное число префиксов, которое принято на основе на узел. Рекомендуется, чтобы предел был настроен для каждого Однорангового соединения по протоколу BGP.

При настройке этой функции с командой настройки маршрутизатора под управлением BGP **neighbor maximum-prefix** один аргумент требуется: максимальное число префиксов, которые приняты перед узлом, является завершением. Дополнительно, номер от 1 до 100 может также быть введен. Этот номер представляет процент от значения максимального числа префиксов в этот момент, сообщение журнала передается.

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

См. Настройку Характеристика получения максимального префикса BGP для получения дополнительной информации о максимальном числе префиксов на узел.

Префиксы BGP фильтра со списками префиксов

Списки префиксов позволяют администратору сети permit or deny определенные префиксы, которые переданы или получены через BGP. Списки префиксов должны использоваться, куда возможный для обеспечения сетевой трафик передается по намеченным путям. Списки префиксов должны быть применены к каждому узлу eBGP и во входящем и в исходящих направлениях.

Настроенные списки префиксов ограничивают префиксы, которые переданы или получены к в частности разрешенным политикой маршрутизации сети. Если это не происходит из-за большого числа полученных префиксов, список префиксов должен быть настроен для специфического блокирования известных плохих префиксов. Эти известные плохие префиксы включают освобожденное пространство IP-адресов и сети, которые зарезервированы для внутреннего или целей тестирования RFC 3330. Исходящие списки префиксов должны быть настроены для специфического разрешения только префиксов, которые организация намеревается объявить.

Этот пример конфигурации использует списки префиксов для ограничения маршрутов, которые изучены и объявлены. В частности только маршрут по умолчанию позволен входящий списком префиксов BGP-PL-INBOUND, и префикс 192.168.2.0/24 является

единственным маршрутом, позволенным быть объявленным BGP-PL-OUTBOUND.

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

См. Соединение с Поставщиком услуг Использование Внешнего BGP для полного обзора фильтрации префикса BGP.

Префиксы BGP фильтра со списками доступа пути автономной системы

Списки доступа пути автономной системы (AS) BGP позволяют пользователю фильтровать полученные и объявленные префиксы на основе атрибута AS-path префикса. Это может использоваться в сочетании со списками префиксов для установления устойчивого набора фильтров.

Этот пример конфигурации использует списки доступа пути AS для ограничения входящих префиксов инициируемыми удаленным AS и исходящими префиксами к инициируемым локальной автономной системой. Префиксы, которые получены от всех других автономных систем, фильтруются и не устанавливаются в таблице маршрутизации.

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

Безопасные протоколы внутреннего шлюза

Способность сети должным образом передать трафик и восстановиться с изменений топологии или отказов зависит от точного отображения топологии. Можно часто работать, Протокол IGP в заказе предоставляют это представление. По умолчанию IGPs являются динамичными и обнаруживают дополнительные маршрутизаторы, которые связываются с определенным IGP в использовании. IGPs также обнаруживают маршруты, которые могут использоваться во время сбоя соединения сети.

Эти подразделы предоставляют обзор самых важных характеристик безопасности IGP. Рекомендации и примеры, которые покрывают Версию 2 (RIPv2) Протокола RIP (Routing Information Protocol), Протокол EIGRP и Протокол OSPF, предоставлены в надлежащих случаях.

Аутентификация протокола маршрутизации и проверка с профилем сообщения 5

Сбой для обеспечения обмена сведениями о маршрутизации позволяет атакующему вводить ложные сведения о маршрутизации в сеть. При помощи проверки подлинности с помощью пароля с протоколами маршрутизации между маршрутизаторами можно помочь безопасности сети. Однако, потому что эта аутентификация передается как открытый текст, может быть просто для атакующего ниспровергать это управление безопасностью.

Путем добавления возможностей хэша MD5 к процессу проверки подлинности обновления маршрута больше не содержат нешифрованные пароли, и все содержание обновления маршрута является более стойким к вмешательству. Если слабые пароли выбраны, Однако Аутентификация MD5 все еще восприимчива к грубой силе и подборам пароля по словарю. Рекомендуется использовать пароли с достаточной рандомизацией. Когда по сравнению с проверкой подлинности с помощью пароля, эти примеры являются определенными для Аутентификации MD5, так как Аутентификация MD5 намного более безопасна. IPSec может также использоваться, чтобы проверить и защитить протоколы маршрутизации, но эти примеры не детализируют его использование.

EIGRP и RIPv2 используют Цепочки ключей как часть конфигурации. *См.* ключ для получения дополнительной информации о конфигурации и использовании Цепочек ключей.

Это - пример конфигурации для аутентификации маршрутизатора EIGRP использование MD5:

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

Это - конфигурация проверки подлинности маршрутизатора MD5 в качестве примера для RIPv2. RIPv1 не поддерживает аутентификацию.

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

Это - пример конфигурации для аутентификации маршрутизатора OSPF использование MD5. OSPF не использует Цепочки ключей.

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

См. OSPF Настройки для получения дополнительной информации.

Команды Passive-Interface

Информационные утечки или введение ложной информации в IGP, могут быть смягчены посредством использования **команды passive-interface**, которая помогает в управлении рекламой сведений о маршрутизации. Рекомендуется не объявить любую информацию к сетям, которые являются вне 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, что вы представляете ложные сведения о маршрутизации в сети, необходимо использовать Фильтрацию маршрута. В отличие от команды конфигурации маршрутизатора **passive-interface**, маршрутизация происходит на интерфейсах, как только фильтрация маршрута включена, но ограничена информация, которая объявлена или обработана.

Для EIGRP и RIP, использования **команды distribute-list** с ключевое слово ограничивает, какая информация объявлена, в то время как использование **в** ключевом слове ограничивает, какие обновления обработаны. **Команда distribute-list** доступна для OSPF, но это не препятствует тому, чтобы маршрутизатор распространился фильтруемые маршруты. Вместо этого **команда area filter-list** может использоваться.

Этот пример EIGRP фильтрует исходящие рекламные объявления с **командой distribute-list** и списком префиксов:

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

Этот пример EIGRP фильтрует входящие обновления со списком префиксов:

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

См. Настройку Независимые от протокола IP - маршрутизация Функции для получения дополнительной информации о том, как управлять объявлением и обработкой обновлений маршрута.

Этот 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 сохранены маршрутизатором в памяти и увеличениями потребления ресурсов с дополнительными префиксами, которые должен держать маршрутизатор. Для предотвращения истощения ресурсов важно настроить протокол маршрутизации для ограничения потребления ресурсов. При использовании функцию Защиты от перегрузок Базы данных Состояния канала, это возможно с OSPF.

Данный пример демонстрирует конфигурацию функции Защиты от перегрузок Базы данных состояний каналов OSPF:

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

См. Ограничение Количества Самогенерации LSA для Процесса OSPF для получения дополнительной информации о Защите от перегрузок Базы данных состояний каналов OSPF.

Защитите первые протоколы резервирования переходов

Первые Протоколы Резервирования переходов (FHRPs) предоставляют упругость и резервирование для устройств то действие как шлюзы по умолчанию. Эта ситуация и эти протоколы являются банальными в средах, где пара приборов слоя 3 предоставляет 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 всем FHRPs. По умолчанию эти протоколы связываются с не прошедшей поверку подлинности связью. Этот вид связи может позволить атакующему изображать из себя FHRP-говорящее устройство для принятия роли шлюза по умолчанию в сети. Это поглощение позволило бы атакующему выполнять атаку по перехвату и возможному изменению передаваемых данных и перехватывать весь трафик пользователя, который выходит из сети.

Для предотвращения этого типа атаки все FHRPs, которые поддерживаются программным обеспечением Cisco IOS, включают возможность аутентификации или с MD5 или с текстовыми строками. Из-за угрозы, представленной не прошедшим поверку подлинности FHRPs, рекомендуется, чтобы экземпляры этих протоколов использовали Аутентификацию MD5. Этот пример конфигурации демонстрирует использование GLBP, HSRP и Аутентификации MD5 VRRP:

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

Плоскость данных

Несмотря на то, что плоскость данных ответственна за движущиеся данные от источника до назначения в контексте безопасности, плоскость данных наименее важна из этих трех плоскостей. Именно по этой причине важно защитить управление и уровни управления в предпочтении по плоскости данных при обеспечении сетевого устройства.

Однако в самой плоскости данных, существует много функций и параметров конфигурации, которые могут помочь защищать трафик. Эти разделы детализируют эти функции и опции, таким образом, что можно более легко защитить сеть.

Укрепление плоскости общих данных

Большая часть трафика плоскости данных течет по сети, как определено настройкой маршрутизации сети. Однако функциональность IP - сети существует для изменения пути пакетов по сети. Функции, такие как IP - режимы, в частности параметр исходной маршрутизации, формируют проблему безопасности в сегодняшних сетях.

Использование Транзитных ACL также относится к укреплению плоскости данных.

Посмотрите Транзитный трафик Фильтра с Транзитным разделом ACL этого документа для получения дополнительной информации.

IP - режимы выборочное отбрасывание

Существует две проблемы безопасности, представленные IP - режимами. Трафик, который содержит IP - режимы, должен быть процессной коммутацией устройствами Cisco IOS, которые могут привести к поднятой Загрузке ЦПУ. IP - режимы также включают функциональность для изменения пути, который трафик берет через сеть, которая потенциально позволяет ему ниспровергать управления безопасностью.

Из-за этих проблем, **опции команды глобальной конфигурации IP {отбрасывание | игнорирует}**, был добавлен к Cisco IOS Software Release 12.3 (4) T, 12.0 (22) S, и 12.2 (25) S. В первой форме этой команды, **IP отбрасывания опций**, отброшены все пакеты IP, которые содержат IP - режимы, которые получены устройством Cisco IOS. Это предотвращает и поднятую Загрузку ЦПУ и возможную подрывную деятельность управлений безопасностью, которые могут включить IP - режимы.

Вторая форма этой команды, **IP опции игнорируют**, настраивает устройство Cisco IOS для игнорирования IP - режимов, которые содержатся в полученных пакетах. В то время как это действительно смягчает угрозы, отнесенные к IP - режимам для локального устройства, возможно, что на нисходящие устройства могло влиять присутствие IP - режимов. Именно по этой причине форма **отбрасывания** этой команды настоятельно рекомендована. Это продемонстрировано в примере конфигурации:

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

Обратите внимание на то, что некоторые протоколы, например RSVP, делают легитимное использование IP - режимов. На функциональность этих протоколов влияет эта команда.

Однажды IP - режимы Выборочное Отбрасывание было включено, команда EXEC **show ip traffic** может использоваться для определения количества пакетов, которые отброшены из-за присутствия IP - режимов. Эта информация присутствует в принудительном счетчике сбросов.

См. IP - режимы ACL Выборочное Отбрасывание для получения дополнительной информации об этой функции.

Отключите маршрутизацию источника IP

Источник IP, направляющий, усиливает Свободный Исходный маршрут и Параметры записи маршрута в тандеме или Строгий Исходный маршрут наряду с Параметром записи маршрута, чтобы позволить источнику дейтаграммы IP задать сетевой путь, который берет пакет. Эта функциональность может использоваться в попытках направить трафик вокруг управлений безопасностью в сети.

Если IP - режимы не были полностью отключены через IP - режимы Выборочная функция Отбрасывания, важно, чтобы была отключена маршрутизация Источника IP. Маршрутизация источника IP, которая включена по умолчанию во всех Cisco IOS Software Release, отключена через команду глобальной кофигурации **no ip source-route**. Этот пример конфигурации иллюстрирует использование этой команды:

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

Отключите переадресации ICMP

Переадресации ICMP используются для информирования сетевого устройства лучшего пути к IP - адресу назначения. По умолчанию программное обеспечение Cisco IOS передает перенаправление, если оно получает пакет, который должен маршрутизироваться через интерфейс, оно было получено.

В некоторых ситуациях для атакующего могло бы быть возможно заставить устройство Cisco IOS передавать много сообщений переадресации ICMP, который приводит к поднятой Загрузке ЦПУ. Поэтому рекомендуется, чтобы была отключена передача переадресаций ICMP. Переадресации ICMP отключены с **командой no ip redirects** конфигурации интерфейса, как показано в примере конфигурации:

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

Отключите или ограничьте направленные широковещательные IP - рассылки

Направленные широковещательные IP - рассылки позволяют передать пакет IP - трансляции к удаленной IP-подсети. Как только это достигает удаленной сети, передающий IP - устройство передает пакет как широковещание Уровня 2 ко всем станциям на подсети. Эта функциональность адресной трансляции была усилена, поскольку усиление и отражение способствуют нескольким атакам, включая smurf-атаку.

Текущим версиям программного обеспечения Cisco IOS отключили эту функциональность по умолчанию; однако, это может быть включено через команду настройки интерфейса **ip directed-broadcast**. Версиям программного обеспечения Cisco IOS до 12.0 включили эту функциональность по умолчанию.

Если сеть абсолютно требует функциональности адресной трансляции, ее использование должно управляться. Это возможно с использованием списка контроля доступа как опция к **команде ip directed-broadcast**. Этот пример конфигурации ограничивает адресные трансляции теми пакетами UDP, которые происходят в надежной сети, 192.168.1.0/24:

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

Транзитный трафик фильтра с транзитными ACL

Возможно управлять тем, какой трафик передает транзитом сеть с использованием транзитных ACL (tACLs). Это в отличие от ACL инфраструктуры, которые ищут на трафик фильтрации, который предназначен к самой сети. Фильтрация, предоставленная tACLs, выгодна, когда это выбираемо к трафику фильтрации к конкретной группе устройств или

трафика, который передает транзитом сеть.

Этот тип фильтрации традиционно выполнен межсетевыми экранами. Однако существуют экземпляры, где это может быть выгодно для выполнения этой фильтрации на устройстве Cisco IOS в сети, например, где фильтрация должна быть выполнена, но не присутствует никакой межсетевой экран.

Транзитные ACL являются также соответствующим местом, в котором можно внедрить статические меры защиты антиспуфинга.

Посмотрите раздел Мер защиты Антиспуфинга этого документа для получения дополнительной информации.

Для получения дополнительной информации см. "Транзитные списки контроля доступа: Фильтрация в Вашем Краю для получения дополнительной информации о tACLs.

Фильтрация пакета ICMP

Протокол ICMP был разработан как протокол управления для IP. Также, сообщения, которые это передает, могут иметь далеко достигающие ограничения на TCP и Протоколах "IP" в целом. ICMP используется сетевым **эхо-запросом** средств устранения проблем и **traceroute**, а также Обнаружением MTU-маршрута; однако, внешнее подключение ICMP редко необходимо для правильной работы сети.

Программное обеспечение Cisco IOS предоставляет функциональность для специфической фильтрации сообщений ICMP по имени или типа и кода. ACL данного примера позволяет ICMP от надежных сетей, в то время как это блокирует все пакеты ICMP из других источников:

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

IP - фрагменты фильтра

Как детализировано ранее на Предельном Доступе к Сети с разделом ACL Инфраструктуры этого документа, фильтрация фрагментированных пакетов IP может поставить проблему к устройствам безопасности.

Из-за неинтуитивной природы обработки фрагмента IP - фрагменты часто непреднамеренно разрешаются ACL. Фрагментация также часто используется в попытках уклониться от обнаружения Intrusion Detection Systems. Именно по этим причинам IP - фрагменты часто используются в атаках и должны явно фильтроваться наверху любого, настроил tACLs. ACL ниже включает всестороннюю фильтрацию IP - фрагментов. Функциональность, проиллюстрированная в данном примере, должна использоваться в сочетании с функциональностью предыдущих примеров:

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

См. Списки контроля доступа и IP - фрагменты для получения дополнительной информации об обработке ACL фрагментированных пакетов IP.

Поддержка ACL IP - режимов фильтрации

В программном обеспечении Cisco IOS версии 12.3(4)T и позже, программное обеспечение

Cisco IOS поддерживает использование ACL для фильтрации пакетов IP на основе IP - режимов, которые содержатся в пакете. Присутствие IP - режимов в пакете могло бы указать на попытку ниспровергать управления безопасностью в сети или иначе изменить транзитные характеристики пакета. Именно по этим причинам пакеты с IP - режимами должны фильтроваться в краю сети.

Данный пример должен использоваться с содержанием от предыдущих примеров для включения завершенной фильтрации пакетов IP, которые содержат IP - режимы:

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

Меры защиты антиспуфинга

Много атак используют спуфинг IP - адреса источника, чтобы быть эффективными или скрыть истинный источник атаки и препятствовать точной обратной трассировке. Программное обеспечение Cisco IOS предоставляет RPF Индивидуальной рассылки и Защиту IP-источника (IPSG) для удерживания атак, которые полагаются на спуфинг IP - адреса источника. Кроме того, ACL и пустая маршрутизация часто развертываются как ручное средство спуфинга предотвращения.

Защита IP-источника работает для уменьшения спуфинга для сетей, которые находятся под прямым административным контролем путем выполнения порта коммутатора, MAC-адреса и проверки адреса источника. RPF индивидуальной рассылки предоставляет проверку исходной сети и может уменьшить имитировавшие атаки от сетей, которые не находятся под прямым административным контролем. Защита на уровне порта может использоваться для проверки MAC-адресов в уровне доступа. Протокол Разрешения динамических адресов (ARP), Контроль (DAI) смягчает векторы атаки, которые используют отравление ARP на локальных сегментах.

RPF индивидуальной рассылки

RPF индивидуальной рассылки позволяет устройству проверить, что адрес источника переданного пакета может быть достигнут через интерфейс, который получил пакет. Вы не должны полагаться на RPF Индивидуальной рассылки как на единственную защиту от спуфинга. Если соответствующий маршрут return к IP - адресу источника существует, поддельные пакеты могли ввести сеть через Индивидуальную рассылку поддерживающий RPF интерфейс. RPF индивидуальной рассылки полагается на вас для включения скоростной маршрутизации Cisco на каждом устройстве и настроен на поинтерфейсной основе.

RPF индивидуальной рассылки может быть настроен в одном из двух режимов: свободный или строгий. В случаях, где существует асимметричная маршрутизация, предпочтен свободный режим, потому что строгий режим, как известно, отбрасывает пакеты в этих ситуациях. Во время конфигурации **ip проверяют** команду настройки интерфейса, ключевое слово**, любой** настраивает свободный режим, в то время как **rx** ключевого слова настраивает строгий режим.

Данный пример иллюстрирует конфигурацию этой функции:

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

См. Понимание Одноадресной пересылки по обратному пути для получения дополнительной информации о конфигурации и использовании RPF Индивидуальной рассылки.

Защита от подделки IP-адреса (IP Source Guard)

Защита IP-источника является эффективными средствами спуфинга предотвращения, которое может использоваться, если вы управляете Интерфейсами 2 уровня. Защита IP-источника использует информацию от DHCP, snooping для динамичной настройки списка контроля доступа порта (PACL) на Интерфейсе 2 уровня, запрещая любой трафик от IP-адресов, которые не привязаны в таблице IP source binding.

Защита IP-источника может быть применена к Интерфейсам 2 уровня, принадлежащим DHCP поддерживающие отслеживание VLAN. Эти команды включают отслеживание DHCP:

```
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 командой настройки интерфейса **защиты на уровне порта ip verify source**. Это требует **dhcp команды глобальной конфигурации IP, snooping параметр данных**; дополнительно, сервер DHCP должен поддержать параметр DHCP 82.

См. функции DHCP Настройки и Защиту IP-источника для получения дополнительной информации об этой функции.

Безопасность портов

Защита на уровне порта используется для смягчения спуфинга MAC-адреса в интерфейсе доступа. Защита на уровне порта может использовать динамично изученные (sticky) MAC-адреса для упрощения в начальной конфигурации. Как только защита на уровне порта определила нарушение MAC, она может использовать один из четырех режимов нарушения. Эти режимы, защищают, ограничивают, завершают работу, и shutdown VLAN. В экземплярах, когда порт только предоставляет доступ для одной рабочей станции с использованием стандартных протоколов, максимальным числом, можно быть достаточным. Протоколы, которые усиливают виртуальные MAC - адреса, такие как HSRP, не функционируют, когда максимальное число установлено в одно.

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

См. Защиту на уровне порта Настройки для получения дополнительной информации о Защите на уровне порта confuration.

Динамическая проверка ARP

Динамическая проверка ARP (DAI) может использоваться для смягчения атак отравления ARP на локальные сегменты. Атака отравления ARP является методом, в котором атакующий передает сфальсифицированную информацию о ARP к локальному сегменту. Эта информация разработана для повреждения кэша ARP других устройств. Часто атакующий использует отравление ARP для выполнения атаки по перехвату и возможному изменению передаваемых данных.

DAI перехватывает и проверяет отношение IP К MAC-АДРЕСУ всех пакетов ARP на ненадежных портах. В средах DHCP DAI использует данные, которые генерируются DHCP, snooping функция. Пакеты ARP, которые получены на доверяемых интерфейсах, не

проверены, и от недопустимых пакетов на ненадежных интерфейсах сбрасывают. В средах не-DHCP требуется использование ACL ARP.

Эти команды включают отслеживание DHCP:

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

Как только отслеживание DHCP было включено, эти команды включают DAI:

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

В средах DHCP non ACL ARP требуются, чтобы включать DAI. Данный пример демонстрирует базовую конфигурацию DAI с ACL ARP:

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

См. Настройку Динамическая Проверка ARP для получения дополнительной информации о том, как настроить DAI.

Антиспуфинговые ACL

Вручную настроенные ACL могут обеспечить статическую защиту антиспуфинга против атак, которые используют известное неиспользованное и недоверяемое адресное пространство. Обычно, эти антиспуфинговые ACL применены к входному трафику в границах сети как компонент большего ACL. Антиспуфинговые ACL требуют обычного мониторинга, потому что они могут часто изменяться. Спуфинг может быть минимизирован в трафике, который происходит из локальной сети, если вы применяете исходящие ACL, которые ограничивают трафик допустимыми локальный адресами.

Данный пример демонстрирует, как ACL могут использоваться для ограничения IP-спуфинга. Этот ACL применен входящий на необходимом интерфейсе. ACE, которые составляют этот ACL, не являются всесторонними. Если вы настраиваете эти типы ACL, ищете актуальную ссылку, которая окончательна.

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

См. Настройку Обычно Используемые ACL IP для получения дополнительной информации о том, как настроить Списки контроля доступа.

Официальный список невыделенных интернет-адресов ведется Командой Cymru. Дополнительные сведения о фильтрации неиспользуемых адресов доступны в Ссылочной Странице Bogon .

Ограничьте влияние на ЦП трафика плоскости данных

Первичная цель маршрутизаторов и коммутаторов к передачам пакетов и кадрам через устройство вперед к конечным назначениям. Эти пакеты, которые передают транзитом устройства, развернутые всюду по сети, могут повлиять на использование ЦП устройства. Плоскость данных, которая состоит из трафика, который передает транзитом сетевое устройство, должна быть защищена для обеспечения использования управления и уровней управления. Если транзитный трафик может заставить устройство обрабатывать трафик коммутатора, на уровень управления устройства можно влиять, который может привести к в рабочем состоянии разрушению.

Функции и Типы трафика, который Влияние ЦП

Несмотря на то, что не исчерпывающий, этот список включает типы трафика плоскости данных, которые требуют специальной Обработки ЦПУ и являются процессом, коммутированным ЦП:

- **Регистрация ACL** - трафик Регистрации ACL состоит из любых пакетов, которые генерируются из-за соответствия (permit or deny) ACE, на котором используется **регистрационное** ключевое слово.
- **RPF индивидуальной рассылки** - RPF Индивидуальной рассылки, используемый в сочетании с ACL, мог бы привести к коммутации в контексте процесса определенных пакетов.
- **IP - режимы** - Любые пакеты IP с включенными опциями должны быть обработаны ЦП.
- **Фрагментация** - Любой пакет IP, который требует фрагментации, нужно передать к ЦП для обработки.
- **Истечение времени существования (TTL)** - Пакеты, которые имеют значение TTL, меньше чем или равное 1, требуют, чтобы Превышенное Время Internet Control Message Protocol (ТИП ICMP 11, Код 0) сообщения было передано, который приводит к Обработке ЦПУ.
- **Недостижимый ICMP** - Пакеты, которые приводят к сообщениям о недоступности ICMP из-за маршрутизации, MTU или фильтрации, обработан ЦП.
- **Трафик, Требующий Запроса ARP** - Назначения, для которых не существует Запись ARP, требует обработки ЦП.
- **Не-IP трафик** - Весь не-IP трафик обработан ЦП.

Посмотрите, что Плоскость Общих данных Укрепляет раздел этого документа для получения дополнительной информации об Укреплении Плоскости Данных.

Фильтр на значении TTL

Можно использовать Поддержку ACL фильтрации на функции Значения TTL, представленной 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 получения устройства, где значение TTL является нулем или один. Фильтрование пакетов на основе значений TTL может также использоваться, чтобы гарантировать, что значение TTL не ниже, чем диаметр сети, таким образом защищая уровень управления нисходящих устройств, относящихся к инфраструктуре от атак истечения TTL.

Обратите внимание на то, что некоторые приложения и программные средства, такие как пакеты истечения TTL использования **traceroute** для тестирования и диагностических назначений. Некоторые протоколы, такие как IGMP, законно используют значение TTL одного.

Этот пример ACL создает политику, которая фильтрует пакеты IP, где значение TTL -

меньше чем 6.

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

См. Идентификацию Атаки Истечения TTL и Смягчение для получения дополнительной информации о фильтровании пакетов на основе значения TTL.

См. Поддержку ACL фильтрации на Значении TTL для получения дополнительной информации об этой функции.

В программном обеспечении Cisco IOS версии 12.4(4)T и позже, Гибкое пакетное соответствие (FPM) позволяет администратору совпадать на произвольных битах пакета. Эта политика FPM пакеты отбрасываний с TTL оценивает меньше чем шесть.

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

См. Гибкое Пакетное Соответствие, расположенное на Cisco IOS Гибкий Пакет Соответствующая домашняя страница, для получения дополнительной информации о функции.

Фильтр на присутствии IP - режимов

В программном обеспечении Cisco IOS версии 12.3(4)T и позже, можно использовать Поддержку ACL функции IP - режимов фильтрации в именованном, расширенном списке доступа IP для фильтрации пакетов IP с подарком IP - режимов. Пакеты IP фильтрации, которые основываются на присутствии IP - режимов, могут также использоваться, чтобы препятствовать тому, чтобы уровень управления устройств, относящихся к инфраструктуре имел для обработки этих пакетов на уровне процессоров.

Обратите внимание на то, что Поддержка ACL функции IP - режимов фильтрации может использоваться только с именованным, расширенными списками ACL. Нужно также обратить внимание, что RSVP, Multiprotocol Label Switching Traffic Engineering, Версии IGMP 2 и 3 и другие протоколы, которые используют пакеты IP - режимов, не могли бы быть в состоянии функционировать должным образом, если отброшены пакеты для этих протоколов. Если эти протоколы используются в сети, то Поддержка ACL IP - режимов фильтрации может использоваться; однако, IP - режимы ACL, Выборочная функция Отбрасывания могла отбросить этот трафик и эти протоколы, не могли бы функционировать должным образом. Если нет никаких протоколов в использовании, которые требуют IP - режимов, IP - режимы ACL, Выборочное Отбрасывание является предпочтительным способом для отбрасывания этих пакетов.

Этот пример ACL создает политику, которая фильтрует пакеты IP, которые содержат любые IP - режимы:

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

ACL данного примера демонстрирует политику, которая фильтрует пакеты IP с пятью определенными IP - режимами. Запрещены пакеты, которые содержат эти опции:

- 0 концов списка опций (eool)
- 7 рекордных маршрутов (record-route)
- 68 штампов времени (метка времени)

- 131 - Свободный исходный маршрут (lsr)
- 137 - Строгий исходный маршрут (ssr)

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

Посмотрите, что Плоскость Общих данных Укрепляет раздел этого документа для получения дополнительной информации о IP - режимах ACL Выборочное Отбрасывание.

Для получения дополнительной информации см. "Транзитные списки контроля доступа: Фильтрация в Вашем Краю для получения дополнительной информации о фильтрации транзита и граничного трафика.

Другой функцией в программном обеспечении Cisco IOS, которое может использоваться для фильтрации пакетов с IP - режимами является CoPP. В программном обеспечении Cisco IOS версии 12.3(4)T и позже, CoPP позволяет администратору фильтровать трафик пакетов уровня управления. Устройство, которое поддерживает CoPP и Поддержку ACL IP - режимов фильтрации, представленных в программном обеспечении Cisco IOS версии 12.3(4)T, может использовать политику списка доступа для фильтрации пакетов, которые содержат IP - режимы.

Эта политика CoPP отбрасывает транзитные пакеты, которые получены устройством, когда присутствуют любые IP - режимы:

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

Когда эти IP - режимы присутствуют, эта политика CoPP отбрасывает транзитные пакеты, полученные устройством:

- 0 концов списка опций (eool)
- 7 рекордных маршрутов (record-route)
- 68 штампов времени (метка времени)
- 131 свободный исходный маршрут (lsr)
- 137 строгих исходных маршрутов (ssr)

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

В предыдущей политике CoPP, записи списка контроля доступа (ACE), которые совпадают с пакетами с результатом действия разрешения в этих пакетах, сбрасываемых функцией отбрасывания policy-map, в то время как на пакеты, которые совпадают с запрещать действием (не показанный) не влияет функция отбрасывания policy-map.

См. Развертывающийся Контроль уровня управления для получения дополнительной информации о функции CoPP.

Защита уровня управления

В программном обеспечении Cisco IOS версии 12.4(4)T и позже, может использоваться Защита Уровня управления (CPPr), чтобы ограничить или определить политику трафика уровня управления ЦП устройства Cisco IOS. В то время как подобный CoPP, CPPr имеет

способность ограничить или определить политику трафика с помощью большой степени детализации, чем CoPP. CPPr делит составной уровень управления на три отдельных категории уровня управления, известные как подинтерфейсы: Хост, Транзит и подинтерфейсы Исключения CEF существуют.

Эта политика CPPr отбрасывает транзитные пакеты, полученные устройством, где значение TTL - меньше чем 6 и транзит или нетранзитные пакеты, полученные устройством, где значение TTL является нулем или один. Политика CPPr также отбрасывает пакеты с выбранными IP - режимами, полученными устройством.

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

В предыдущей политике CPPr, записи списка контроля доступа, которые совпадают с пакетами с результатом действия разрешения в этих пакетах, сбрасываемых функцией отбрасывания policy-map, в то время как на пакеты, которые совпадают с запрещать действием (не показанный) не влияет функция отбрасывания policy-map.

См. Понимание Защиты Уровня управления и Защиты Уровня управления для получения дополнительной информации о функции CPPr.

Идентификация трафика и обратная трассировка

Время от времени можно должны быть быстро определить и сетевой трафик обратной трассировки, особенно во время реагирования на инциденты или плохой производительности сети. NetFlow и ACL Классификации являются этими двумя основными методами для выполнения этого с программным обеспечением Cisco IOS. NetFlow может предоставить видимость в весь трафик в сети. Кроме того, NetFlow может быть внедрен с коллекторами, которые могут предоставить долгосрочное отклонение и автоматизированный анализ. ACL классификации являются компонентом ACL и требуют предварительное планирование определить определенный трафик и ручное вмешательство во время анализа. Эти разделы предоставляют краткий обзор каждой функции.

NetFlow

NetFlow определяет аномальную и связанную с безопасностью активность сети путем отслеживания сетевых потоков. Данные NetFlow могут быть просмотрены и проанализированы через CLI, или данные могут быть экспортированы в коммерческий Сборщик данных в режиме NetFlow или бесплатный Сборщик данных в режиме NetFlow для агрегации и анализа. Сборщики данных в режиме NetFlow, посредством долгосрочного отклонения, могут предоставить анализ использования и поведение сети. NetFlow функционирует путем выполнения анализа определенных атрибутов в пакетах IP и создания потоков. Версия 5 является обычно используемой версией NetFlow, однако, версия 9 более расширяема. Потоки NetFlow могут быть созданы с выбранными данными трафика в средах большого объема.

CEF или распределенный CEF, является предпосылкой к включению NetFlow. NetFlow может быть настроен на маршрутизаторах и коммутаторах.

Данный пример иллюстрирует базовую конфигурацию этой функции. В предыдущих версиях программного обеспечения Cisco IOS команда для включения NetFlow на интерфейсе является **ip route-cache flow** вместо **ip flow {вход | выход}**.

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

Это - пример выходных данных NetFlow от CLI. Атрибут SrcIf может способствовать 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
```

См. Cisco IOS NetFlow для получения дополнительной информации о возможностях NetFlow.

См. Введение к Cisco IOS NetFlow - Технический обзор для технического обзора NetFlow.

ACL классификации

ACL классификации предоставляют видимость в трафик, который пересекает интерфейс. ACL классификации не изменяют политику безопасности сети и, как правило, создаются для классификации отдельных протоколов, адресов источника или назначений. Например, ACE, который разрешает весь трафик, мог быть разделен на определенные протоколы или порты. Это больше разграниченной классификации трафика в определенные ACE может помочь предоставлять понимание сетевого трафика, потому что каждая категория трафика

имеет свой собственный счетчик попаданий. Администратор мог бы также отделиться, неявные запрещают в конце ACL в гранулированные ACE помогать определять типы отказа в трафике.

Администратор может ускорить реагирование на инциденты при помощи ACL классификации с командами EXEC **clear ip access-list counters** и **show access-list**.

Данный пример иллюстрирует, что конфигурация ACL классификации для определения трафика SMB до по умолчанию запрещает:

```
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 классификации, используйте команду EXEC названия acl **show access-list**. Счетчики ACL могут быть очищены с командой EXEC названия acl **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)
```

См. Понимание Регистрации Списка контроля доступа для получения дополнительной информации, о как к возможностям enable logging в ACL.

Управление доступом со СХЕМАМИ VLAN и портом списки контроля доступа

Списки контроля доступом VLAN (VACL), или схемы VLAN и порт ACL (PACL), предоставляют возможность принудить управление доступом на немаршрутизированном трафике, который ближе к оконечным устройствам, чем списки контроля доступа, которые применены к маршрутизируемым интерфейсам.

Эти разделы предоставляют обзор функций, преимуществ и сценариев возможного использования VACL и PACL.

Управление доступом со СХЕМАМИ VLAN

VACL или схемы VLAN, которые применяются ко всем пакетам, которые вводят VLAN, предоставляют возможность принудить управление доступом на внутритрафике виртуальной локальной сети (VLAN). Это не возможно с ACL на маршрутизируемых интерфейсах. Например, схема VLAN могла бы использоваться для предотвращения хостов, которые содержатся в той же VLAN от связи друг с другом, который уменьшает возможности для локальных атакующих или червей для использования хоста на том же сегменте сети. Для запрета пакетов от использования схемы VLAN можно создать список контроля доступа (ACL), который совпадает с трафиком и, в схеме VLAN, заставляет действие понижаться. Как только схема VLAN настроена, все пакеты, которые вводят LAN, последовательно оценены против карты настроенной VLAN. Карты доступа VLAN поддерживают списки доступа MAC и IPv4; однако, они не поддерживают ACL IPv6 или регистрация.

Данный пример использует расширенный Именованный список доступа, который иллюстрирует конфигурацию 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)
```

Данный пример демонстрирует использование схемы VLAN для запрета портов TCP 139 и 445, а также протокол "IP" VINES:

```
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)
```

См. Настройку Сетевой безопасности с ACL для получения дополнительной информации о конфигурации схем VLAN.

Управление доступом с PACL

PACL могут только быть применены к входящему направлению на физических интерфейсах Уровня 2 коммутатора. Подобный схемам VLAN, PACL предоставляют управление доступом

на трафике Уровня 2 или немаршрутизировавшем. Синтаксис для создания PACL, которое имеет приоритет по схемам VLAN и спискам управления доступом к маршрутизатору, совпадает со списками управления доступом к маршрутизатору. Если ACL применен к Интерфейсу 2 уровня, то он упоминается как PACL. Конфигурация включает создание IPv4, IPv6, или ACL MAC и приложения его к Интерфейсу 2 уровня.

Данный пример использует расширенный Именованный список доступа для иллюстрирования конфигурации 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)
```

См. раздел ACL порта Настройки Сетевой безопасности с ACL для получения дополнительной информации о конфигурации PACL.

Управление доступом с MAC

Списки контроля доступа MAC или расширенные списки могут быть применены на IP - сеть с использованием этой команды в режиме конфигурации интерфейса:

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

> **Примечание:** Это должно классифицировать пакеты Уровня 3 как пакеты Уровня 2. Команда поддерживается в программном обеспечении Cisco IOS версии 12.2(18)SXD (для SUP 720) и Cisco IOS Software Release 12.2 (33) SRA или позже.

Эта интерфейсная команда должна быть применена на входной интерфейс, и это дает механизму пересылки команду не осматривать IP - заголовок. Результат состоит в том, что вы в состоянии использовать список доступа MAC на среде IP.

Частное VLAN использование

Частные VLAN (PVLAN) являются функцией безопасности уровня 2, которая ограничивает подключение между рабочими станциями или серверами в VLAN. Без PVLAN все устройства на VLAN Уровня 2 могут связаться свободно. Сетевые среды существуют, где безопасности можно помочь путем ограничения связи между устройствами на одиночной VLAN. Например, PVLAN часто используются для запрещения связи между серверами в публично доступной подсети. Если одиночный сервер становится поставившим под угрозу, отсутствие подключения к другим серверам к приложению PVLAN могло бы помочь ограничивать компромисс одним сервером.

Существует три типа Частных VLAN: выделенные VLAN, VLAN сообщества и основные VLAN (виртуальная локальная сеть). Конфигурация PVLAN использует основные и вторичные VLAN. Основной VLAN (виртуальная локальная сеть) содержит все случайные порты, которые описаны позже, и включает одну или более вторичных VLAN, которые могут быть или изолированы или VLAN сообщества.

Выделенные VLAN

Конфигурация вторичного VLAN как выделенный VLAN полностью предотвращает связь

между устройствами во вторичном VLAN. Мог бы только быть один выделенный VLAN на основной VLAN (виртуальная локальная сеть), и только случайные порты могут связаться с портами в выделенном VLAN. Выделенные VLAN должны использоваться на сетях без доверия как сети та поддержка гости.

Этот пример конфигурации настраивает VLAN 11 как выделенный VLAN и привязывает его к основному VLAN (виртуальная локальная сеть), VLAN 20. Пример ниже также настраивает interface FastEthernet 1/1 как изолированный порт в VLAN 11:

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

VLAN сообщества

Вторичное VLAN, которое настроено как VLAN сообщества, позволяет связь среди участников VLAN, а также с любыми случайными портами в основном VLAN (виртуальная локальная сеть). Однако никакая связь не возможна ни между какими двумя VLAN сообщества или от VLAN сообщества до выделенного VLAN. VLAN сообщества должны использоваться для группировки серверов, которым нужно подключение друг с другом, но где не требуется подключение ко всем другим устройствам в VLAN. Этот сценарий распространен в публично доступной сети или где угодно что серверы предоставляют содержание недоверяемым клиентам.

Данный пример настраивает одиночную VLAN сообщества и настраивает порт коммутатора FastEthernet 1/2 в качестве участника той VLAN. VLAN сообщества, VLAN 12, является вторичным VLAN к основному VLAN (виртуальная локальная сеть) 20.

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

Случайные порты

Порты коммутатора, которые размещены в основной VLAN (виртуальная локальная сеть), известны как случайные порты. Случайные порты могут связаться со всеми другими портами в основных и вторичных VLAN. Маршрутизатор или интерфейсы межсетевого экрана являются наиболее распространенными устройствами, найденными на этих VLAN.

Этот пример конфигурации комбинирует изолированное предыдущее и примеры VLAN сообщества и добавляет конфигурацию interface FastEthernet 1/12 как случайный порт:

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

При реализации PVLAN важно гарантировать, что конфигурация Уровня 3 на месте поддерживает ограничения, которые введены PVLAN, и не обеспечивает Конфигурацию PVLAN, которая будет ниспровергаться. Фильтрация уровня 3 с ACL маршрутизатора или межсетевым экраном может предотвратить подрывную деятельность Конфигурации PVLAN.

См. Частные сети VLAN: разнородные, изолированные, общедоступные, расположенные на домашней странице Безопасности локальных сетей, для получения дополнительной информации об использовании и конфигурации Частных VLAN.

Заключение

Этот документ дает вам широкий обзор методов, которые могут использоваться для обеспечения системного устройства Cisco IOS. При обеспечении устройств это увеличивает общую безопасность сетей, которыми вы управляете. В этом обзоре, защите управления,

обсуждены контроль и плоскости данных, и рекомендации по конфигурации предоставлены. Где возможно, достаточная подробность предоставлена для конфигурации каждой связанной функции. Однако во всех случаях, полные справочники предоставлены для предоставления вас информацию, необходимую для дальнейшей оценки.

Подтверждения

Некоторые описания характеристики в этом документе были записаны командами разработки информации о Cisco.

Приложение: стабилизирующий чек-лист устройства Cisco IOS

Этот чек-лист является набором всех укрепляющихся шагов, которые представлены в этом руководстве. Администраторы могут использовать его в качестве напоминания всех укрепляющихся функций, использованных и продуманных для устройства Cisco IOS, даже если опция не была реализована, потому что это не применялось. Администраторам рекомендуют оценить каждую опцию для ее потенциального риска, прежде чем они внедрят опцию.

Панель управления

- Пароли

  Включите хеширование MD5 (секретная опция) для включают и пароли локального пользователяНастройте локаут повторной попытки пароляОтключите восстановление пароля (рассмотрите риск),

- Отключите неиспользованные сервисы

- Настройте TCP keepalife для сеансов управления

- Память аппарата и уведомления порогового значения ЦПУ

- Настройка

  Память и уведомления порогового значения ЦПУРезервная память для консольного доступаДетектор утечек памятиОбнаружение переполнения буфераРасширенный набор crashinfo (сведения об аварийном отказе)

- Используйте iACLs для ограничения управляющего доступ

- Фильтр (рассматривают риск),

  Пакеты ICMPIP - фрагментыIP - режимыЗначение TTL в пакетах

- Защита уровня управления

Настройте фильтрацию портаНастройте пороги очереди

- Управляющий доступ

  Используйте Защиту Панели управления для ограничения интерфейсов управленияТаймаут exec набораИспользуйте зашифрованный транспортный протокол (такой как SSH) для доступа CLITранспорт контроля для VTY и линий tty (обращаются к опции класса),Предупредите баннеры использования

- AAA

  Используйте AAA для аутентификации и нейтрализацииИспользуйте AAA (TACACS +) для авторизации для выполнения командИспользуйте AAA для учетаИспользуйте избыточные AAA-серверы

- SNMP

  Настройте сообщества SNMPv2 и примените ACLНастройте SNMPv3

- Регистрация

  Настройте централизованную регистрациюSet logging level для всех соответствующих компонентовLogging source-interface набораНастройте глубину детализации метки времени регистрации

- Управление конфигурацией

  Замена и откатИсключительный доступ изменения конфигурацииКонфигурация упругости программного обеспеченияУведомления изменения конфигурации

Плоскость управления

- Отключите (рассмотрите риск),

  Переадресация ICMPНедостижимый ICMPПротокол прокси-ARP

- Настройте Аутентификацию NTP, если используется NTP

- Настройте Контроль уровня управления / Защита (фильтрация порта, пороги очереди)

- Безопасные протоколы маршрутизации

  BGP (TTL, MD5, максимальное число префиксов, списки префиксов, ACL системного пути)IGP (MD5, пассивный интерфейс, фильтрация маршрута, потребление ресурсов)

- Настройте аппаратные ограничители скорости

- Защитите первые протоколы резервирования переходов (GLBP, HSRP, VRRP)

Плоскость данных

- Настройте IP - режимы выборочное отбрасывание
- Отключите (рассмотрите риск),

  IP-маршрутизация от источникаНаправленные широковещательные IP - рассылкиПереадресация ICMP
- Предельные направленные широковещательные IP - рассылки
- Настройте tACLs (рассмотрите риск),

  ICMP фильтраIP - фрагменты фильтраIP - режимы фильтраЗначения TTL фильтра
- Настройте требуемые меры защиты антиспуфинга

  ACLЗащита от подделки IP-адреса (IP Source Guard)Динамическая проверка ARPRPF индивидуальной рассылкиБезопасность портов
- Защита Уровня управления (исключение cef уровня управления)
- Настройте NetFlow и ACL классификации для идентификации трафика
- Настройте требуемые ACL управления доступом (схемы VLAN, PACL, MAC)
- Настройте частные VLAN