Улучшение безопасности в CSS 11000 и CSS 11500

Содержание

Введение

Этот документ предоставляет сведения о параметрах настройки Конфигурации CISCO, которые могут улучшить безопасность относительно Cisco Content Services Switch (CSS) 11000 или CSS 11500. Этот документ описывает параметры настройки базовой конфигурации, которые почти универсально применимы в IP - сетях, и покрывает несколько неожиданных моментов, о которых необходимо знать.

Этот документ не представляет полный список этих элементов, ни может информация в документе быть замененной знание со стороны администратора сети. Документ служит напоминанием элементов, о которых иногда забывают.

Этот документ упоминает только команды, которые важны в IP - сетях. Многие сервисы, которые можно включить на CSS, требуют тщательной настройки системы безопасности. Однако этот документ фокусируется на информации для сервисов, которые включены по умолчанию или которые почти всегда включаются пользователями, и это может потребовать выведения из строя или изменения конфигурации.

Некоторые настройки по умолчанию в Программном обеспечении webns Cisco существуют для статистических причин. Эти параметры настройки были применимы, когда они были выбраны, но вероятно будут другими, если новые настройки по умолчанию были выбраны сегодня. Другие настройки по умолчанию применимы для большинства систем, но могут создать угрозы безопасности, если эти настройки по умолчанию используются в устройствах, которые являются частью защиты по периметру сети. Тем не менее другие настройки по умолчанию фактически требуются стандартами, но не всегда выбираемы от точки зрения безопасности.

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.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Управление паролями

Пароли и подобная конфиденциальная информация, такие как строки имени и пароля Протокола SNMP, являются основным методом защиты против неавторизованный доступа к вашему CSS. Лучший способ управления паролями — хранить их в TACACS+ или на сервере аутентификации RADIUS. Однако почти каждый CSS все еще имеет локально настроенный пароль для привилегированного адреса. CSS может также включать другие сведения о пароле в файл конфигурации. Любой пароль, который настроен в открытом тексте, появляется в конфигурации, зашифрованной со Стандартом шифрования данных (DES).

Профили локального пользователя

Этот список описывает профили локального пользователя:

- *Администратор* — Профиль администратора включает эти привилегии:Доступ к Меню Offline Diagnostics MonitorПолный доступ к командной строкеПолный доступ к каталогуЭти параметры настройки могут быть настроены или из командной строки или из Меню Offline Diagnostics Monitor.
- *Технический специалист* — профиль Технического специалиста включает эти привилегии:Полный доступ к командной строкеПолный доступ к каталогуЭти параметры настройки могут быть настроены с использованием командной строки. Не используйте профиль Технического специалиста для административных целей CSS.
- *Суперпользователь* — профиль Суперпользователя включает эти привилегии:Полный доступ к командной строкеСпособность сохранить ограничения доступа к каталогуЭти параметры настройки могут быть настроены с использованием командной строки.
- *User* — Профиль пользователя не может изменить конфигурацию и включает ограничения доступа к каталогу. Эти параметры настройки могут быть настроены с использованием командной строки.

При запуске **команды restrict user-database** вы принуждаете ограничения доступа к каталогу на каждого пользователя. Только пользовательские уровни Администратора и Технического специалиста могут выполнить эти действия:

- Удалите **команду restrict user-database**.
- Измените команду **базы локальных пользователей**.
- Выполните **команду clear running-config**.

Контроль интерактивного доступа

Любой пользователь, который может войти к CSS, может отобразить информацию это, широкая публика должна не обязательно просмотреть. В некоторых случаях пользователь, который может войти к CSS, может использовать CSS в качестве реле для дальнейших сетевых атак. Пользователь, который получает привилегированный адрес к CSS, может реконфигурировать CSS. Для предотвращения несоответствующего доступа необходимо управлять интерактивными входами в систему к CSS.

Хотя в большинстве случаев интерактивный доступ отключен по умолчанию, некоторые возможности все-таки сохраняются. Самыми очевидными исключениями являются интерактивные сеансы от непосредственно подключенных асинхронных оконечных

устройств, таких как консольный терминал и доступ к Управлению портами Ethernet.

См. Методы Удаленного доступа CSS Настройки для получения дополнительной информации о том, как управлять интерактивным доступом к CSS.

Порты консоли

Важный элемент для запоминания - то, что консольный порт устройства Cisco имеет особые привилегии. В частности предположите, что кто-то передает ESC (Escape) символ к консольному порту, когда работает диагностика POST. После перезагрузки этот человек может легко использовать процедуру восстановления пароля для взятия под свой контроль системы. Атакующие, которые могут прервать питание или вызвать сбой системы, и у кого есть доступ к консольному порту через терминал с прямым кабельным подключением, модем, сервер терминала или некоторое другое сетевое устройство, могут взять под свой контроль систему. Эти атакующие могут взять на себя управление, даже если у них нет физического доступа к системе или способности обычно входить в систему.

Поэтому любой модем или сетевое устройство, которое предоставляет доступ к консольному порту Cisco, должны быть защищены к стандарту, который сопоставим с безопасностью, которая используется для привилегированного адреса к CSS. Как минимум любой консольный модем должен иметь тип, который может потребовать, чтобы пользователь удаленного доступа предоставил пароль для доступа, и паролем модема нужно тщательно управлять.

Основной интерактивный доступ

Существует больше способов получить интерактивные соединения к CSS, чем могут понять пользователи. Можно использовать эти методы для управления CSS:

- Telnet
- Хост Secure Shell (SSH)
- SNMP
- Консоль
- Ftp
- XML
- Управление web

Выполните **ограничить** команду, чтобы включить или отключить. CSS все еще слушает на определенном порте, но закрывает соединение. Так, чтобы пакеты не поражали эти порты, настройте пункты списка контроля доступа (ACL) для запрета пакетов.

Трудно быть уверенным, что были заблокированы все возможные режимы доступа. В большинстве случаев администраторы должны использовать своего рода механизм аутентификации, чтобы удостовериться, что управляются входы в систему на всех линиях. Администраторы должны гарантировать, что входы в систему управляются даже на машинах, которые, как предполагается, недоступны от сетей без доверия.

Контроль консольного доступа

По умолчанию консоль аутентифицируется против локально профилей настроенного пользователя. Для активации TACACS + или Проверка подлинности RADIUS, выполните

консольную опознавательную команду global и связанные опции.

Контроль VTY

По умолчанию VTY аутентифицируются против локально профилей настроенного пользователя. Для активации TACACS + или Проверка подлинности RADIUS, выполните команду global **виртуальной проверки подлинности** и связанные опции.

Поддержка SSH

Если ваше программное обеспечение поддерживает протокол зашифрованного доступа, такой как SSH, Cisco рекомендует включить только, что протокол и отключает доступ Telnet, когда вы хотите использовать сервер SSH. Чтобы включить Демону SSH (SSHD), вам нужна серверная лицензия SSHD, которая включает функцию SSHD и по Стандарту и по Расширенным версиям программного обеспечения CSS. Выполните **команды sshd**. См. Сетевые протоколы CSS Настройки для получения дополнительной информации.

Примечание: Поддержка версии SSH 1 запустилась в 4.01. Поддержка версии SSH 2 запустилась в 5.20.

RADIUS

С версии 5.00 и позже, можно настроить CSS для использования RADIUS для проверки подлинности пользователя. Для настройки CSS для Проверки подлинности RADIUS обратитесь к Профилям пользователей Настройки и Параметрам CSS.

Примечание: Пользователь/профиль группы только требует атрибутов RADIUS инженерной группы по развитию Интернета (IETF), [006] Service-Type = Административный.

Этот список определяет коды сообщения отладки:

```
PW_ACCESS_REQUEST       1
PW_ACCESS_ACCEPT        2
PW_ACCESS_REJECT        3
PW_ACCOUNTING_REQUEST   4
PW_ACCOUNTING_RESPONSE  5
PW_ACCOUNTING_STATUS    6
PW_ACCESS_CHALLENGE     11
```

Для просмотра отладок, которые привязаны к Входам RADIUS, выполняют эти команды:

```
logging subsystem radius level debug-7
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

Это - пример отладки успешной аутентификации:

```
logging subsystem radius level debug-7
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

Это - пример аутентификации, которая отказала из-за неверного имени пользователя или пароля:

```
logging subsystem radius level debug-7
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

Это - пример аутентификации, которая отказала, потому что не настроен атрибут RADIUS профиля пользователя 006 service-type:

```
logging subsystem radius level debug-7
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

TACACS +

В версии 5.03 и позже, можно настроить CSS для использования TACACS + для проверки подлинности пользователя. Для настройки CSS для TACACS + аутентификация, обратитесь к Комментариям к выпуску для Серии css 11000.

Для просмотра отладок, которые привязаны к TACACS + входы в систему, выполняют эти команды:

```
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

Это - пример отладки успешной аутентификации:

```
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

Это - пример ошибки проверки подлинности из-за неверного имени пользователя или пароля:

```
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

Предупреждающие сообщения

В некоторой юрисдикции можно значительно упростить процесс гражданской и/или уголовной ответственности взломщиков, которые входят системы, если вы предоставляете баннер, который сообщает неавторизованный пользователям, что их использование неавторизовано. Другая юрисдикция запрещает монитор действий даже неавторизованный пользователей, пока вы не предприняли шаги для уведомления пользователей намерения сделать так. Один способ предоставить это уведомление состоит в том, чтобы поместить его в сообщение баннера. Можно настроить сообщение баннера с **командой set banner** CSS. Эта команда была представлена в 5.03.

Требования к правовым уведомлениям сложны и зависят от юрисдикции и ситуации. Даже в юрисдикции, юридические заключения варьируются. Обсудите эту проблему со своим юрисконсультом. В сотрудничестве с адвокатом полагайте который из этих предупреждений помещать в ваш баннер:

- Предупреждение, которое в частности сообщает только авторизованный персонал, должно войти в систему или использовать систему и возможно информацию о том, кто может авторизовать использование.
- Уведомление о том, что любое несанкционированное использование системы является незаконным и влечет за собой гражданскую и/или уголовную ответственность.

- Уведомление о том, что любое использование системы может регистрироваться или контролироваться без дальнейшего предупреждения, и полученные записи могут использоваться в суде в качестве доказательств.
- Определенные предупреждения, которые требуются местными законодательствами.

Для безопасности (а не законный) причины, не включайте в ваш баннер входа в систему эту информацию о своем CSS:

- Name
- Модель
- Программное обеспечение, которое выполняется
- ********** OWNER **********

Стандартно настраиваемые службы управления

Много пользователей управляют своими сетями с использованием протоколов кроме интерактивной удаленной регистрации. Наиболее распространенные протоколы для этих целей – SNMP и HTTP. Самая безопасная опция не должна включать эти протоколы вообще. Однако при включении одного из протоколов защитите его, как этот раздел описывает.

SNMP

SNMP очень широко используется для мониторинга сетевого устройства и, часто, для изменений конфигурации. SNMP имеет два главных стандартных пересмотра, SNMPv1 и SNMPv2. Ваш CSS поддерживает версию SNMP 2C (SNMPv2C), который известен как основанный на сообществе SNMP. CSS генерирует trap-сообщения в формате SNMPv1.

Для управления доступом SNMP к CSS выполните **команду no restrict snmp** и **команду restrict snmp**. Доступ через SNMP включен по умолчанию. При отключении доступа через SNMP CSS все еще слушает на определенном порте 1, но закрывает соединение. Настройте выражения ACL для запрета пакетов так, чтобы пакеты не поражали порт SNMP.

К сожалению, SNMPv1 и SNMPv2C используют очень слабую схему проверки подлинности, которая основывается на строке имени и пароля. Аутентификация составляет фиксированный пароль, который передан по сети без шифрования. Если вы должны использовать SNMPv2C, стараетесь выбрать неясные строки имени и пароля (и не используйте, например, общий или частный). Если вообще возможный, избегите использования тех же строк имени и пароля для всех сетевых устройств. Для каждого устройства (или хотя бы для каждого участка сети) лучше использовать свою строку или строки сообщества. Строка, доступная только для чтения, не должна совпадать со строкой, доступной для чтения и записи. Если возможно, сделайте периодический опрос SNMPv2C со строкой имени и пароля только для чтения. Используйте строки для чтения-записи только для фактических операций записи.

SNMPv2C не подходит для использования через общедоступный Интернет по этим причинам:

- SNMPv2C использует строки проверки подлинности открытого текста.
- SNMPv2C является протоколом транзакций на основе дейтаграмм, который легко имитируется.

- В большинстве реализаций SNMP те строки отправляются неоднократно при периодических опросах.

Тщательно рассмотрите результаты перед использованием SNMPv2C через общедоступный Интернет.

В большинстве сетей правильные сообщения SNMP только прибывают из определенных станций управления. Если правильные сообщения SNMP только прибывают из определенных станций управления в вашей сети, рассматривают использование ACL, которые применены к контурам VLAN для запрета нежелательных сообщений SNMP.

Базы данных управляющих станций SNMP, содержащие информацию об аутентификации, например строки сообщества, часто имеют большой размер. Эта информация может предоставить доступ ко многим CSSs и другим сетевым устройствам. Это сосредоточение информации делает станцию управления SNMP естественной мишенью для атаки. Защитите станцию управления SNMP соответственно.

HTTP

CSS поддерживает удаленное конфигурирование с помощью HTTP - протокола с использованием Расширяемого языка разметки гипертекста (XML) (XML) документы. Если вы переходите к порту TCP 8081, в Версии WebNS 4.10 или ранее, можно достигнуть доступа к интерфейсам пользователя управления устройствами WebNS в открытом тексте. В целом доступ HTTP эквивалентен интерактивному доступу к CSS. Протокол аутентификации, который используется для HTTP, эквивалентен передаче нешифрованного пароля по сети. К сожалению, в HTTP отсутствуют эффективные методы работы с одноразовыми паролями и паролями, основанными на вызовах. Поэтому HTTP относительно рискованный выбор для использования через общедоступный Интернет.

Если вы принимаете решение использовать HTTP для управления, ограничить доступ к соответствующим IP-адресам с использованием ACL, которые применены к контурам VLAN. Для управления доступом XML HTTP к CSS выполните команду **no restrict xml** и **команду restrict xml**. В более поздних версиях WebNS команда изменилась на **состояние веб-mgt** *[отключают |, включают]*. Доступ через XML HTTP отключен по умолчанию. Для управления пользовательским HTTP WebNS доступом управления устройствами выполните **команду no restrict web-mgmt** и **команду restrict web-mgmt**. Интерфейс пользователя управления устройствами WebNS отключен по умолчанию. Необходимо настроить и команду **no restrict xml** и **команду no restrict web-mgmt** для просмотра к CSS на порту 8081.

В версии 5.00 и позже, если вы переходите HTTP к адресу канала на порту 8081, браузер перенаправлен для использования HTTPS и подключения к тому же адресу канала.

HTTPS

CSS поддерживает удаленное конфигурирование через HTTP, Безопасный (HTTPS) протокол. Этот Протокол SSL защищает передачи данных (который может включать пароли) между интерфейсом пользователя управления устройствами WebNS и вашим web-браузером.

Для управления пользовательским HTTPS WebNS доступом управления устройствами выполните **команду no restrict web-mgmt** и **команду restrict web-mgmt**. Интерфейс пользователя управления устройствами WebNS отключен по умолчанию. Если это отключено, CSS продолжает слушать на определенном порте, но закрывает соединение.

Так, чтобы пакеты не поражали порт TCP SSL 443, настройте выражения ACL для запрета пакетов.

Управление и интерактивный доступ по Интернету (и другие сети без доверия)

Много пользователей управляют своим CSSs удаленно, и иногда это выполнено по Интернету. Любой незашифрованный удаленный доступ рискован, но особенно опасен доступ через сеть общего пользования, такую как Интернет. Все удаленные схемы управления, которые включают интерактивный доступ, HTTP и SNMP, уязвимы.

Атаки, которые обсуждает этот раздел, являются относительно сложными, но они ни в коем случае не вне досягаемости взломщиков сегодня. Поставщики услуг сети общего пользования, которые берут необходимые меры безопасности, могут часто мешать этим атакующим. Оцените свой уровень доверия в измерениях безопасности, что все поставщики, которые несут ваше использование трафика управления. Даже если вы доверяете своим поставщикам, делаете, по крайней мере, некоторые шаги для защиты себя от результатов каких-либо ошибок, эти поставщики могли бы сделать.

Все внимания в отношении этого раздела применяются так же к хостам как относительно CSS. В то время как этот документ обсуждает, как защитить сеансы регистрации CSS, также изучить использование аналогичных механизмов для защиты хостов, если вы администрируете те хосты удаленно. Удаленное интернет-администрирование полезно, но оно требует особого внимания к безопасности.

Анализаторы пакетов

Взломщики часто входят в компьютеры, которыми интернет-провайдеры владеют, или в компьютеры на других больших сетях. Взломщики устанавливают программы анализатора пакетов, которые контролируют трафик, который проходит через сеть. Эти программы анализатора пакетов крадут данные, такие как пароли и Строки имени и пароля SNMP. Операторы сети начали улучшать свою безопасность, которая делает эту кражу более трудной. Однако эта кража все еще относительно распространена. В дополнение к риску от внешних злоумышленников недобросовестные сотрудники компании-провайдера могут также установить анализаторы. Любой пароль, который передается по незашифрованному каналу, находится в опасности, который включает вход в систему и enable password для вашего CSSs.

Если вы можете, избежать входить в ваш CSS с использованием какого-либо незашифрованного протокола по какой-либо сети без доверия. Если ваше программное обеспечение CSS поддерживает его, используйте протокол входа с шифрованием, такой как SSH.

Если у вас нет доступа к зашифрованному протоколу удаленного доступа, другая возможность состоит в том, чтобы использовать систему одноразовых паролей, такую как S/KEY или OPIE, вместе с TACACS + или сервер RADIUS, для управления обоими интерактивными входами в систему и привилегированным адресом к CSS. Преимущество состоит в том, что украденный пароль бесполезен. Украденный пароль сделан недопустимым тем жем сеанс, на котором он украден. Данные, которые переданы на сеансе и не отнесены к паролям, остаются доступными eavesdropper, но много программ анализатора установлены для концентрации на паролях.

Если необходимо передать сеансы Telnet паролей в открытом тексте, часто изменять ваши пароли. и обратите пристальное внимание на путь, который пересекают ваши сеансы.

Другие опасности при доступе в Интернет

В дополнение к анализаторам пакетов удаленное интернет-управление CSS представляет эти угрозы безопасности:

- Для управления CSS по Интернету необходимо разрешить, по крайней мере, некоторым Узлам Интернета иметь доступ к CSS. Эти хосты могут поставиться под угрозу, или их адреса могут имитироваться. При разрешении интерактивного доступа из Интернета вы делаете свой зависит от уровня безопасности, не только на ваших собственных мерах по антиспуфингу, но и на мерах по антиспуфингу поставщиков услуг, которые вовлечены.Можно уменьшить эти опасности при выполнении этих действий:Удостоверьтесь, что все хосты, которым разрешают войти к вашему CSS, находятся под вашим собственным контролем.Используйте протоколы входа с шифрованием со строгой проверкой подлинности.
- Иногда, доступ к незашифрованному соединению TCP (такому как сеанс Telnet) возможно получить. Кто-то, кто получает доступ к этому типу сеанса, может фактически взять на себя управление далеко от пользователя, в которого входят. Такие атаки не почти так же распространены как сниффинг простого пакета и могут быть сложны для установки. Однако такие атаки возможны, и атакующий, у которого есть ваша сеть в частности в памяти, поскольку цель может использовать их. Единственное реальное решение к проблеме незаконного использования сеанса должно использовать строго аутентифицируемый, зашифрованный протокол управления.
- Атаки отказа в обслуживании (DoS) относительно распространены в Интернете. Если ваша сеть под атакой DoS, можно быть неспособны достигнуть CSS, чтобы собрать информацию или взять действие по защите. Даже атака на сеть кого-то еще может повредить управляющего доступ к вашей собственной сети. Несмотря на то, что можно предпринять шаги для создания сети более стойкой к атакам DoS, единственная реальная защита против этого риска должна иметь отдельное, дополнительный канал управления (такой как модем коммутируемой линии передачи) для использования в аварийных ситуациях.

Регистрация

CSSs Cisco может запись данных о множестве событий, многие из которых имеют значимость защиты. Журналы могут быть неоценимыми для характеристики и ответа на случаи нарушения безопасности. Можно выполнить **команду logging subsystem** для включения входа в систему CSS. Уровень регистрации по умолчанию предупреждает 4 для всех подсистем.

Выполните эти команды для регистрации подсистемы для сбора этой информации:

- Регистрационные информации пользователя для входа
- Выходы из системы
- Аутентификация RADIUS
- Аутентификация TACACS+

```
logging subsystem radius level debug-7
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

Примечание: Команда netman subsystem покрывает TACACS + отладки.

От точки зрения безопасности самые важные события, которых обычно делает запись регистрация системы, включают эти события:

- Интерфейсные изменения статуса
- Изменяется на конфигурацию системы
- Соответствия ACL

```
logging subsystem netman level info-6
!--- Note that the default logging level is warning-4, which does !--- not appear in the configuration. logging commands enable
logging subsystem acl level debug-7
```

Удаленный мониторинг (RMON) позволяет вам удаленно контролировать и анализировать активность пакетов на Портах Ethernet CSS. RMON также позволяет конфигурацию аварийных сигналов для монитора объектов MIB и позволяет конфигурации событий уведомлять вас относительно этих условий сигнала тревоги. Событие "RMON" является действием, которое происходит, когда инициировано связанное Сигнальное оповещение "rmon". Можно настроить аварийное событие, таким образом, что, когда аварийное событие имеет место, оно генерирует один или оба из этих элементов:

- Регистрационное событие
- Trap-сообщение к станции управления сетью SNMP

Сохраните информацию журнала

По умолчанию CSS сохраняет начальную загрузку и сообщения журнала события подсистемы к файлам журнала на твердом или Флэш диске. Содержание этих файлов зарегистрировано в тексте ASCII. Можно также настроить CSS для передачи сообщений журнала к активному сеансу CSS, адресу электронной почты или другой системе хоста.

Максимальный размер локального файла журнала составляет 50 МБ для твердых находящихся на диске систем и 10 МБ для Флэша находящиеся на диске системы.

Сообщения журнала подсистемы являются событиями подсистемы, которые происходят во время использования CSS. CSS сохраняет эти сообщения в sys.log файле. CSS создает этот файл, когда первое событие подсистемы происходит, который должен быть зарегистрирован. CSS определяет который сообщения подсистемы регистрировать его настроенным уровнем регистрации.

Большинство крупных систем используют серверы "syslog". Можно выполнить **команду logging host**, чтобы передать регистрационную информацию демону системного журнала на системе хоста. Даже если у вас есть сервер системного журнала, необходимо все еще включить локальное ведение журнала к диску.

Ко всем журналам добавляют метку времени с месяцем, днем и временем к второму. При настройке источника единого времени, такого как Простой сетевой протокол синхронизации времени (SNTP) для журналов можно более легко отследить последовательность

зарегистрированных событий. Для настройки SNTP server на CSS выполните **sntp** команду. SNTP был представлен в 5.00 кодах.

Рекордные нарушения в списке доступа

При использовании ACL для трафика фильтрации, который обращается к адресам канала или правилу содержимого, виртуальному IP (VIP) адреса, можно принять решение регистрировать пакеты, которые нарушают критерии фильтра. Чтобы к enable logging на выражении ACL, выполните **пункт # регистрационная команда enable**. Кроме того, выполните **команду logging subsystem acl level debug-7**. CSS регистрирует эту информацию:

- Протокол
- Исходный порт
- Номер порта
- IP-адрес ОТПРАВИТЕЛЯ
- IP-адрес ПОЛУЧАТЕЛЯ

Попытайтесь избежать конфигурации регистрации для записей ACL, которые совпадают с очень большими числами пакетов. Эта конфигурация заставляет файлы журнала становиться чрезмерно большими и может вырезать в производительность системы.

Можно также использовать Регистрацию ACL для охарактеризования трафика, который привязан к сетевым атакам. В этом случае вы настраиваете Регистрацию ACL для регистрации подозрительного трафика. Можно охарактеризовать на маршрутизаторе Cisco на интернет-стороне CSS для обработки ACL. См. Охарактеризование и Отслеживание Переполнения пакетами Использование маршрутизаторов Cisco для получения дополнительной информации.

Примечание: ACL CSS только применены на входящие пакеты. ACL не проверяет пакеты, которые являются исходящими от интерфейса.

Защитите IP-маршрутизацию

В этом разделе рассматриваются некоторые меры по базовым мерам безопасности, которые касаются пути, которым маршрутизатор передает пакеты IP. См. Основные элементы Cisco ISP - Существенные Функции IOS Каждый интернет-провайдер Должен Рассмотреть для получения дополнительной информации об этих проблемах.

По умолчанию, конфигурация CSS:

- Ограничивает количество SYN - пакетов, которые переходят к VIP, прежде чем CSS регистрирует его как атаку DoS**Примечание:** Это поведение не может быть отключено.
- Запрещает адресные трансляции
- Запрещает пакеты с тем же IP - адресом источника и получателя
- Запрещает IP-адреса источника групповой адресации
- Запрещает порт источника или назначения 0 пакетов

Антиспуфинг

Многие сетевые атаки основаны на фальсификации, или спуфинге, взломщиком адресов источника IP-датаграмм. Некоторые атаки полагаются на спуфинг для атаки для работы.

Другие атаки намного более трудно отследить, если атакующие могут использовать адрес кого-то еще вместо их собственного адреса. Поэтому для предотвращения спуфинга везде, где это выполнимо, ценно для администраторов сети.

Антиспуфинг должен быть сделан в каждой точке в сети, где это практично. Но антиспуфинг является обычно и самым легким сделать и самый эффективный на границах между большими блоками адресов или между доменами администрирования сети. Антиспуфинг на каждом маршрутизаторе в сети обычно непрактичен, потому что, определение которого адреса источника могут законно появиться на любом данном интерфейсе, является трудным.

Если вы - интернет-провайдер (ISP), можно найти что эффективное противодействие подделке пакетов, вместе с другими эффективными мерами безопасности, причины дорогой, проблемные абоненты брать их бизнес другим поставщикам. Если вы - интернет-провайдер, особенно старайтесь применить средства управления за антиспуфингом в коммутируемых пулах и других точках подключения конечного пользователя.

Примечание: См. RFC 2267.

Администраторы корпоративных межсетевых экранов или маршрутизаторов периметра иногда устанавливают меры по антиспуфингу так, чтобы хосты в Интернете не могли принять адреса внутренних хостов. Однако внутренние хосты могут все еще принять адреса хостов в Интернете. Необходимо предотвращать спуфинг в обоих направлениях. Существует по крайней мере три достаточных основания для установки антиспуфинга в обоих направлениях в межсетевом экране организации:

- Внутренние пользователи меньше испытывают желание попытаться запустить сетевые атаки и менее вероятно успешно выполниться, если они действительно пробуют.
- Внутренние хосты, которые случайно неправильно сконфигурированы, менее вероятно, доставят неприятности удаленным узлам. Поэтому они, менее вероятно, будут генерировать неудовлетворенность клиента.
- Внешние взломщики часто вламываются в сеть как на стартовую площадку для дальнейших атак. Эти взломщики могут быть менее заинтересованы в сети с защитой от исходящего спуфинга.

Антиспуфинг с ACL

К сожалению, для простой распечатки команд, которые предоставляют соответствующую защиту от спуфинга, не практично. Конфигурация списков управления доступом (ACL) зависит слишком много от отдельной сети. Основная задача заключается в отсеивании пакетов, которые поступают на интерфейсы, маршрут к которым не является допустимым для предполагаемых исходных адресов пакетов. Например, на CSS с двумя каналами, который подключает ферму серверов с Интернетом, вы хотите сбросить от любой дейтаграммы, которая поступает в интернет-канал, но имеет поле исходного адреса, которое утверждает, что прибыло из машины на ферме серверов.

Точно так же вы хотите сбросить от любой дейтаграммы, которая поступает в интерфейс, который связан с фермой серверов, но это имеет поле исходного адреса, которое утверждает, что прибыло из машины вне фермы серверов. Если ресурсы ЦПУ позволяют, применяют антиспуфинг на какой-либо канал, где определение того, какой трафик может законно поступить, выполнимо.

Интернет-провайдеры, которые несут транзитный трафик, могли ограничить возможности настроить ACL антиспуфинга, но такие интернет-провайдеры могут обычно фильтровать внешний трафик, который утверждает, что произошел в адресном пространстве того интернет-провайдера.

В целом фильтры антиспуфинга должны быть созданы с вводами для ACL. Пакеты должны фильтроваться в каналах, через которые поступают пакеты. CSS может только применить ACL к входящим пакетам.

Когда ACL антиспуфинга существуют, они должны всегда отклонять дейтаграммы с широковещанием или адресами источника для групповой адресации. По умолчанию CSS запрещает эти дейтаграммы. ACL антиспуфинга должны также отклонить дейтаграммы, которые имеют зарезервированный адрес обратной связи как адрес источника. Кроме того, у вас должен обычно быть ACL антиспуфинга, отфильтровывают все перенаправления Протокола ICMP, независимо от адреса источника или назначения. ACL CSS не позволяет вам задавать тип ICMP для запрета. Вместо этого выполните **команду no redirects** для настройки всех IP - адресов канала для не принятия переадресаций ICMP. Это команды:

```
clause # deny any 127.0.0.0 255.0.0.0 destination any
clause # deny any 0.0.0.0 0.0.0.0 destination any
```

Примечание: Пункт # запрещает любой 0.0.0.0 0.0.0.0 назначения, любая команда отфильтровывает пакеты из многого Протокола начального загрузки (BOOTP) клиенты/DHCP. Поэтому команда не является соответствующей во всех средах.

Контроль адресных трансляций

Широко распространенные и популярные атаки DoS smurf и некоторые связанные атаки, используют направленные широковещательные IP - рассылки. По умолчанию CSS настроен с **командой no ip subnet-broadcast**, которая запрещает адресные трансляции.

Направленная широковещательная IP - рассылка является дейтаграммой, которая передается широковещательному адресу подсети, к которой непосредственно не подключен компьютер - отправитель. Адресная трансляция маршрутизируется через сеть как одноадресный пакет, пока адресная трансляция не поступает в целевую подсеть. В подсети адресная трансляция преобразована в широковещание уровня соединения. Из-за природы архитектуры IP-адресации только последний маршрутизатор или сетевое устройство Уровня 3 в цепочке могут окончательно определить адресную трансляцию. Это устройство является тем, которое связано непосредственно с целевой подсетью. Направленные рассылки иногда осуществляются для законных целей, но такое использование — редкость вне сферы финансовых услуг.

При атаке смарф злоумышленник, использующий сфальсифицированный адрес отправителя, отправляет эхо-запросы ICMP на адрес прямой широковещательной рассылки. В результате все хосты на целевой подсети передают ответы поддельному источнику. Когда атакующий передает непрерывный поток таких запросов, атакующий может создать намного более крупный поток ответов, которые могут полностью наводнить хост, адрес которого сфальсифицирован.

См. Последнее в Атаках "отказ в обслуживании": Описание "Смурфинга" и информация для Уменьшения Эффектов для стратегии заблокировать smurf-атаки на некоторых межсетевых экранах - маршрутизаторах (который зависит от организации сети). Документ также предоставляет общую информацию относительно smurf-атаки.

Целостность пути

Много атак зависят от способности влиять на пути, которые дейтаграммы берут через сеть. Если взломщики управляют маршрутизацией, существует шанс, что они могут имитировать адрес машины другого пользователя и передавать ответный трафик им. В некоторых случаях взломщики могут перехватить и чтения данных, которые предназначены для кого-то еще. Маршрутизация может также быть разрушена просто в целях DoS.

IP-маршрутизация от источника

Протокол "IP" поддерживает параметры исходной маршрутизации, которые позволяют отправителю дейтаграммы IP управлять маршрутом, которым дейтаграмма следует к конечному пункту назначения, и общим образом, маршрут, которым следует любой ответ. Эти параметры редко используются для легальных целей в реальных сетях. Некоторые более старые реализации IP не обрабатывают пакеты с маршрутизацией от источника должным образом. Кто-то может передать дейтаграммы с параметрами исходной маршрутизации и, возможно, машины катастрофического отказа, которые выполняют эти реализации.

CSS настроен по умолчанию с **командой no ip source-route set**. CSS никогда не передает пакет IP, который несет параметр исходной маршрутизации. Оставьте команду по умолчанию настроенной, пока вы не знаете, что вашей сети нужна маршрутизация источника.

Переадресация ICMP

Сообщение переадресации ICMP дает конечному узлу команду использовать определенный маршрутизатор в качестве пути к индивидуальному пункту назначения. В IP - сети, который функционирует должным образом, маршрутизатор передает перенаправления только к хостам на локальных подсетях маршрутизатора. Конечный узел никогда не передает перенаправление, и перенаправления никогда не пересекают несколько сетевых переходов. Однако атакующий может нарушить эти правила, и некоторые атаки основываются на этих правилах. Входящие ICMP-сообщения о перенаправлении необходимо отфильтровывать на входных интерфейсах всех маршрутизаторов, которые находятся на границе двух административных доменов. Кроме того, у вас может быть любой ACL, который применен на входную сторону Интерфейса маршрутизатора Cisco, отфильтровывают все переадресации ICMP. Эта фильтрация не вызывает воздействия на эксплуатационные характеристики в сети, которая настроена правильно.

Этот тип фильтрации предотвращает только наступление перенаправления, в которое идут удаленные атакующие. Кроме того, атакующие могут использовать перенаправления для доставления значительных неприятностей, если хост атакующего напрямую подключается к тому же сегменту как хост, который является под атакой.

По умолчанию CSS настроен для принятия перенаправлений на каждом IP - адресе канала, который настроен. Выполните **команду no redirect** под IP - адресом канала для выключения этой функции.

Фильтрация и аутентификация для протокола маршрутизации

При использовании протокол динамической маршрутизации, который поддерживает

аутентификацию, включите ту аутентификацию. Аутентификация предотвращает некоторые злонамеренные атаки на инфраструктуре маршрутизации и может также помочь предотвращать ущерб, который могут нанести неконтролируемые устройства неверна настроенного в сети.

По тем же причинам поставщики услуг и другие операторы больших сетей могут рассмотреть использование фильтрации маршрута. С фильтрацией маршрута сетевые маршрутизаторы не принимают ясно неверную информацию о маршрутизации. Для фильтрации маршрута используйте параметр **distribute-list** в команде. Чрезмерное использование фильтрации маршрута может уничтожить преимущества динамической маршрутизации. Но выборочное использование часто помогает предотвращать плохие результаты. Например, при использовании протокола динамической маршрутизации для передачи с тупиковой сетью заказчика, не принимайте маршруты от того клиента кроме маршрутов к адресному пространству, которое вы фактически делегировали клиенту.

CSS не может фильтровать маршруты. Вместо этого настройте одноранговые узлы маршрутизации CSS с этой функцией.

Этот документ не предоставляет подробную инструкцию на конфигурации проверки подлинности при маршрутизации и фильтрации маршрута. Такая документация доступна на Cisco.com и в другом месте. Можно сослаться на документ Основные элементы Cisco ISP - Существенные Функции IOS, которые Должен Рассмотреть Каждый интернет-провайдер. Из-за сложности обратитесь за опытным советом, если вы - новичок перед настройкой этих функций на важных сетях.

Управление лавинной маршрутизацией

Много атак DoS полагаются на лавинные рассылки бесполезных пакетов. Данные flood-атаки перегружают сетевые каналы, замедляют работу узлов и могут вызвать перегрузку маршрутизаторов. Тщательная настройка маршрутизатора может уменьшить воздействие таких лавинных потоков.

Важный компонент управления лавинной маршрутизацией является осведомленностью о том, где могут произойти узкие места производительности. Если лавинная рассылка перегружает линию T1, отфильтруйте лавинную рассылку на маршрутизаторе во входном конце линии. Если вы фильтруете в стороне получателя в этом случае, существует минимальный эффект. Если сам маршрутизатор является большей частью перегруженного компонента сети, можно усугубить положение при фильтрации мер защиты, которые размещают высокие требования в маршрутизатор. Помните это, когда вы рассмотрите реализацию предложений в этом разделе.

Транзитная лавинная пересылка

Можно использовать Характеристики QoS Cisco на восходящих маршрутизаторах Cisco IOS® для защиты CSS, хостов и ссылок против некоторых видов лавинных рассылок. К сожалению, этот документ не предоставляет общую обработку этого вида управления лавинной маршрутизацией. Кроме того, защита зависит в большой степени от атаки. Единственное простое, обычно применяемый совет должен использовать обслуживание очередей на основе равнодоступности (WFQ) везде, где ресурсы ЦПУ могут поддержать WFQ. WFQ является по умолчанию для низкоскоростных последовательный линий в более поздних версиях программного обеспечения Cisco IOS. Другие функции возможного

интереса включают:

- Committed Access Rate (CAR)
- Generic traffic shaping (GTS)
- Настраиваемая организация очереди

Иногда, можно настроить эти функции когда под активной атакой.

CSS может уменьшить влияние синхроннных атак на VIP и реальных серверах. По умолчанию CSS ограничивает количество SYN и неполных трехэтапных установлений связи и регистрирует их, поскольку нападает DoS.

См. Ссылочную информацию безопасности для получения дополнительной информации.

Возможно, излишние службы

Как правило отключите любой ненужный сервис в любом маршрутизаторе, который достижим от потенциально опасной сети. Сервисы, что этот раздел списки иногда полезен. Но отключите эти сервисы, если они не находятся в активном использовании.

SNTP

SNTP не особенно опасен, но любой ненужный сервис может представить путь преодоления защиты. Если вы фактически используете SNTP, несомненно, явно настроят доверяемый источник времени. SNTP не использует аутентификацию. Повреждение временной базы является хорошим способом ниспровергать определенные протоколы безопасности. Лучший метод должен использовать источник, который является внутренним и менее вероятным имитироваться.

Протокол Cisco Discovery Protocol

Протокол CDP, который был представлен в WEBNS 5.10, используется для некоторых управлений сертификатами. CDP опасен, потому что любая система на непосредственно связанном сегменте может выполнить эти действия:

- Узнайте, что маршрутизатор является устройством Cisco
- Определите номер модели и версию программного обеспечения, которая выполняется

Атакующий может использовать эту информацию для разработки атак на CSS. Информация от CDP доступна только напрямую подключенным системам. CSS только объявляет информацию CDP. CSS не слушает. Вы не можете выполнить команду глобальной кофигурации **cdp run** для отключения протокола CDP. Вы не можете отключить CDP на CSS на поинтерфейсной основе.

Установка обновлений

Как все программное обеспечение, Программное обеспечение webns Cisco имеет дефекты. Некоторые из этих дефектов затрагивают безопасность. Кроме того, новые атаки продолжают быть изобретенными. И поведение, которое считали корректным, когда компонент программного обеспечения был записан, может иметь отрицательные воздействия, когда сознательно использовано поведение.

При обнаружении серьезной уязвимости безопасности в продукте Cisco компания Cisco распространяет информационное сообщение об этой уязвимости. См. Информационную политику Уязвимости безопасности о процессе, посредством которого выполнены эти предупреждения. См. Рекомендации по вопросам безопасности для предупреждений.

Почти любое неожиданное поведение любого компонента программного обеспечения может создать угрозу безопасности где-нибудь. Информационные сообщения только упоминают дефекты, которые имеют прямые последствия для безопасности системы. Если вы совершенствуете свое программное обеспечение, даже в отсутствие какой-либо рекомендации по вопросам безопасности, можно улучшить безопасность.

Некоторые проблемы безопасности не являются результатом ошибок в программном обеспечении, и администраторы сети должны остаться знающий о тенденциях в атаках. Существует много веб-сайтов, интернет-списков рассылки и Конференций Usenet, которые касаются этих тенденций.

Дополнительные сведения

- RFC 2267
- Сообщения по безопасности
- Политика уязвимости безопасности
- Сведения о безопасности
- Сетевые протоколы CSS Настройки
- Методы удаленного доступа CSS Настройки
- Профили пользователей Настройки и параметры CSS
- Комментарии к релизу
- Описание и отслеживание лавинной передачи пакетов с помощью маршрутизаторов Cisco
- Cisco ISP Essentials основные функции IOS, о которых должен знать любой поставщик интернет-услуг
- Последнее в атаках "отказ в обслуживании": описание "Смурфинга" и информация для уменьшения эффектов
- Cisco Systems – техническая поддержка и документация