Пример конфигурации фильтра ACL точки доступа

Содержание

Введение

В этом документе поясняется настройка списков управления доступом (ACL) на основе фильтров на точках доступа Cisco Aironet (AP) с помощью интерфейса командной строки (CLI).

Предварительные условия

Требования

Cisco рекомендует иметь базовые знания об этих темах:

- Конфигурация беспроводного соединения с использованием AP Aironet и Клиентского адаптера a/b/g 802.11 Aironet
- ACL

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- AP aironet серии 1200, который выполняет релиз 12.3 программного обеспечения Cisco IOS (7) JA1
- Aironet 802.11a/b/g Клиентский адаптер
- Выпуск ПО служебной программы рабочего стола Aironet (ADU) 2.5

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.

Условные обозначения

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

Общие сведения

Можно использовать фильтры на AP для выполнения этих задач:

- Ограничьте доступ к сети (WLAN) беспроводной локальной сети
- Предоставьте дополнительный уровень безопасности беспроводной связи

Можно использовать различные типы фильтров к трафику фильтрации на основе:

- Определенные протоколы
- MAC-адрес устройства клиента
- IP-адрес устройства клиента

Можно также позволить фильтрам ограничить трафик от пользователей на проводной LAN. IP-адрес и Фильтры MAC - адреса позволяют или запрещают передачу индивидуальной рассылки и пакетов групповой адресации, которые передаются или от определенного IP или MAC-адресов.

Основанные на протоколе фильтры предоставляют более гранулированный способ ограничить доступ к определенным протоколам через Ethernet и радиоинтерфейсы AP. Можно использовать любой из этих методов для настройки фильтров на AP:

- Веб-GUI
- CLI

Этот документ объясняет, как использовать ACL для настройки, проникает в CLI. Для получения информации о том, как настроить, проникает в GUI, обратитесь к Фильтрам Настройки.

Можно использовать CLI для настройки этих типов основанных на ACL фильтров на AP:

- Фильтры тот стандарт использования ACL
- Фильтры то использование расширенные списки ACL
- Фильтры тот MAC-адрес использования ACL

Примечание: Количество позволенных записей на ACL ограничено ЦП AP. Если существует большое число записей для добавления к ACL, например при фильтрации списка MAC-адресов для клиентов используйте коммутатор в сети, которая может выполнить задачу.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Все конфигурации в этом документе предполагают, что уже установлено беспроводное соединение. Этот документ фокусируется только о том, как использовать CLI для настройки фильтров. Если у вас нет соединения базового беспроводного подключения, обратитесь к Примеру конфигурации Подключения LAN Базового беспроводного подключения.

Фильтры Использование стандартных списков доступа

Можно использовать стандартные ACL, чтобы позволить или запретить запись устройств клиента в сеть WLAN на основе IP-адреса клиента. Стандартные ACL сравнивают адрес источника пакетов IP к адресам, которые настроены в ACL чтобы к контрольному трафику. Этот тип ACL может упоминаться как source IP на основе адреса ACL.

Формат синтаксиса команды стандартного ACL является *access-list-number* **access-list {разрешение | запрещает}** {*IP-адрес* **хоста |** *source-wildcard source-ip* **| любой}**.

В релизе 12.3 программного обеспечения Cisco IOS (7) JA, номер ACL может быть любым номером от 1 до 99. Стандартные ACL могут также использовать расширенный диапазон 1300 - 1999. Этими дополнительными номерами являются расширенные ACL IP.

Когда стандартный ACL настроен, чтобы запретить доступ клиенту, клиент все еще связывается к AP. Однако нет никакой передачи данных между AP и клиентом.

Данный пример показывает стандартный ACL, который настроен для фильтрации IP-адреса клиента 10.0.0.2 от беспроводного интерфейса (radio0 интерфейс). IP-адрес AP 10.0.0.1.

После того, как это сделано, клиент с IP-адресом 10.0.0.2 не может передать или получить данные через сеть WLAN даже при том, что клиент привязан к AP.

Выполните эти шаги для создания стандартного ACL через CLI:

1. Войдите к AP через CLI.Используйте консольный порт или используйте Telnet для доступа к ACL через Интерфейс Ethernet или беспроводной интерфейс.
2. Введите режим глобальной конфигурации в AP:`AP#configure terminal`
3. Выполните эти команды для создания стандартного ACL:`AP<config>#access-list 25 deny host 10.0.0.2 !--- Create a standard ACL 25 to deny access to the !--- client with IP address 10.0.0.2. AP<config>#access-list 25 permit any !--- Allow all other hosts to access the network.`
4. Выполните эти команды для применения этого ACL к радиоинтерфейсу:`AP<config>#interface Dot11Radio 0 AP<config-if>#ip access-group 25 in !--- Apply the standard ACL to the radio interface 0.`

Можно также создать стандартный именованный список управления доступом (ACL) (NACL). NACL использует название вместо номера для определения ACL.

```
 AP#configure terminal AP<config>#ip access-list standard name AP<config>#permit | deny {host
ip-address | source-ip [source-wildcard] | any} log
```

Выполните эти команды для использования стандартного NACLs для запрета доступа хоста 10.0.0.2 к сети WLAN:

```
AP#configure terminal AP<config>#ip access-list standard TEST !--- Create a standard NACL TEST.
AP<config-std-nacl>#deny host 10.0.0.2 !--- Disallow the client with IP address 10.0.0.2 !---
access to the network. AP<config-std-nacl>#permit any !--- Allow all other hosts to access the
network. AP<config-std-nacl>#exit !--- Exit to global configuration mode. AP<config>#interface
Dot11Radio 0 !--- Enter dot11 radio0 interface mode. AP<config-if>#ip access-group TEST in !---
Apply the standard NACL to the radio interface.
```

Фильтры Использование расширенных списков доступа

Расширенные списки ACL сравнивают адреса источника и назначения пакетов IP к адресам, которые настроены в ACL чтобы к контрольному трафику. Расширенные списки ACL также предоставляют средство для трафика фильтрации на основе определенных протоколов. Это предоставляет более тонкую настройку для реализации фильтров на сети WLAN.

В то время как клиент не может обратиться к другим ресурсам, расширенные списки ACL позволяют клиенту обращаться к некоторым ресурсам в сети. Например, можно внедрить фильтр, который позволяет трафик DHCP и трафик Telnet клиенту, в то время как это ограничивает весь другой трафик.

Это - синтаксис команды расширенных списков ACL:

Примечание: Эта команда обернута к четырем линиям из-за пространственных факторов.

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit} protocol
source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [log |
log-input] [time-range time-range-name]
```

В программном обеспечении Cisco IOS версии 12.3 (7) JA, расширенные списки ACL могут использовать номера в диапазоне 100 - 199. Расширенные списки ACL могут также использовать номера в диапазоне 2000 - 2699. Это - растянутый диапазон для расширенных списков ACL.

Примечание: Регистрационное ключевое слово в конце отдельных записей ACL показывает:

- Номер ACL и название
- Был ли пакет разрешен или запрещен
- Определяемая портом информация

Расширенные списки ACL могут также использовать названия вместо номеров. Это - синтаксис для создания расширенного NACLs:

```
ip access-list extended name {deny | permit} protocol source source-wildcard destination
destination-wildcard [precedence precedence] [tos tos] [log | log-input] [time-range time-range-
name]
```

Этот пример конфигурации использование расширил NACLs. Требование - то, что расширенный NACL должен предоставить доступ Telnet клиентам. Необходимо ограничить все другие протоколы на сети WLAN. Кроме того, клиенты используют DHCP для получения IP-адреса. Необходимо создать расширенный список ACL что:

- Позволяет трафик DHCP и трафик Telnet
- Запрещает все другие типы трафика

Как только этот расширенный список ACL применен к радиоинтерфейсу, клиенты

связываются с AP и получают IP-адрес от сервера DHCP. Клиенты также в состоянии использовать Telnet. Все другие типы трафика запрещены.

Выполните эти шаги для создания расширенного списка ACL на AP:

1. Войдите к AP через CLI.Используйте консольный порт или Telnet для доступа к ACL через Интерфейс Ethernet или беспроводной интерфейс.
2. Введите режим глобальной конфигурации в AP:`AP#configure terminal`
3. Выполните эти команды для создания расширенного списка ACL:`AP<config>#ip access-list extended Allow_DHCP_Telnet !--- Create an extended ACL Allow_DHCP_Telnet. AP<config-extd-nacl>#permit tcp any any eq telnet !--- Allow Telnet traffic. AP<config-extd-nacl>#permit udp any any eq bootpc !--- Allow DHCP traffic. AP<config-extd-nacl>#permit udp any any eq bootps !--- Allow DHCP traffic. AP<config-extd-nacl>#deny ip any any !--- Deny all other traffic types. AP<config-extd-nacl>#exit !--- Return to global configuration mode.`
4. Выполните эти команды для применения ACL к радиоинтерфейсу:`AP<config>#interface Dot11Radio 0 AP<config-if>#ip access-group Allow_DHCP_Telnet in !--- Apply the extended ACL Allow_DHCP_Telnet !--- to the radio0 interface.`

Фильтры Использование на основе MAC ACL

Можно использовать MAC, на основе адреса фильтрует для фильтрации устройств клиента на основе твердого закодированного MAC-адреса. Когда клиенту запрещают доступ через на основе MAC фильтр, клиент не может связаться с AP. Фильтры MAC - адреса позволяют или запрещают передачу индивидуальной рассылки и пакетов групповой адресации, или передаваемых от или адресованный определенным MAC-адресам.

Это - синтаксис команды для создания MAC на основе адреса ACL на AP:

Примечание: Эта команда была обернута к двум линиям из-за пространственных факторов.

access-list *access-list-number* **{permit | deny}** *48-bit-hardware-address 48-bit-hardware-address-mask*

В программном обеспечении Cisco IOS версии 12.3 (7) JA, ACL MAC-адреса могут использовать номера в диапазоне 700 - 799 как номер ACL. Они могут также использовать номера в растянутом диапазоне 1100 - 1199.

Данный пример иллюстрирует, как настроить, на основе MAC проникают в CLI, для фильтрации клиента с MAC-адресом **0040.96a5.b5d4**:

1. Войдите к AP через CLI.Используйте консольный порт или Telnet для доступа к ACL через Интерфейс Ethernet или беспроводной интерфейс.
2. Введите режим глобальной конфигурации в CLI AP:`AP#configure terminal`
3. Создайте MAC-адрес ACL 700.Этот ACL не позволяет клиентскому 0040.96a5.b5d4 связываться с AP.
   `access-list 700 deny 0040.96a5.b5d4 0000.0000.0000 !--- This ACL denies all traffic to and from !--- the client with MAC address 0040.96a5.b5d4.`
4. Выполните эту команду для применения этого на основе MAC ACL к радиоинтерфейсу:
   `dot11 association mac-list 700 !--- Apply the MAC-based ACL.`

После настройки этого фильтра на AP клиент с этим MAC-адресом, который был ранее привязан к AP, разъединен. Консоль AP передает это сообщение:

```
AccessPoint# *Mar 1 01:42:36.743: %DOT11-6-DISASSOC: Interface
```

```
Dot11Radio0, Deauthenticating Station 0040.96a5.b5d4
```

Фильтры Использование списков управления доступом (ACL) с временным критерием

Списками управления доступом (ACL) с временным критерием являются ACL, которые могут быть включены или отключены для определенного периода времени. Эта возможность предоставляет устойчивость и гибкость для определения политики контроля доступа, что любой permit or deny определенные виды трафика.

Данный пример иллюстрирует, как настроить списки управления доступом (ACL) с временным критерием через CLI, где Telnet - подключение разрешен от внутренней части до внешней сети в рабочие дни во время рабочих часов:

Примечание: Списки управления доступом (ACL) с временным критерием могут быть определены или на Порте Fast Ethernet или на Радиопорте AP Aironet, на основе ваших требований. Это никогда не применяется на Виртуальный интерфейс группы мостовой передачи (BVI).

1. Войдите к AP через CLI.Используйте консольный порт или Telnet для доступа к ACL через Интерфейс Ethernet или беспроводной интерфейс.
2. Введите режим глобальной конфигурации в CLI AP:`AP#configure terminal`
3. Создайте Временной диапазон. Чтобы сделать это, выполните эту команду в режиме глобальной конфигурации:`AP<config>#time-range Test !--- Create a time-range with name Test. AP(config-time-range)# periodic weekdays 7:00 to 19:00 !--- Allows access to users during weekdays from 7:00 to 19:00 hrs.`
4. Создайте ACL 101:`AP<config># ip access-list extended 101 AP<config-ext-nacl>#permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet time-range Test !--- This ACL permits Telnet traffic to and from !--- the network for the specified time-range Test.` Этот ACL разрешает сеанс Telnet к AP в рабочие дни.
5. Выполните эту команду для применения этих списков управления доступом (ACL) с временным критерием к Интерфейсу Ethernet:
   `interface Ethernet0/0 ip address 10.1.1.1 255.255.255.0 ip access-group 101 in !--- Apply the time-based ACL.`

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

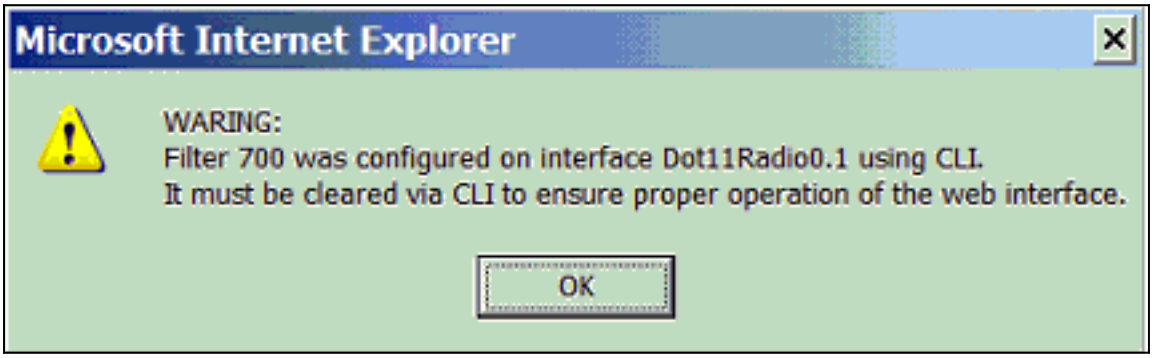
Используйте этот раздел для устранения неполадок своей конфигурации.

Выполните эти шаги для удаления ACL из интерфейса:

1. Войдите в режим конфигурации интерфейса.
2. Войдите **не** перед **командой ip access-group**, как показано в примере:
   `interface interface no ip access-group {access-list-name | access-list-number} {in | out}`

Можно также использовать *название* **show access-list |** команда *номера* для устранения проблем конфигурации. **Команда show ip access-list** предоставляет количество пакетов, которое показывает, какая запись ACL поражается.

Избегите использования и CLI и интерфейсов вебов - обозревателей для настройки беспроводного устройства. При настройке беспроводного устройства с CLI интерфейс веб - обозреватель может отобразить неточную интерпретацию конфигурации. Однако погрешность не обязательно означает, что неправильно сконфигурировано беспроводное устройство. Например, при настройке ACL с CLI интерфейс веб - обозреватель может отобразить это сообщение:



Если вы видите это сообщение, используйте CLI, чтобы удалить ACL и использовать интерфейс веб - обозреватель для реконфигурирования их.

Дополнительные сведения

- Настройке фильтров
- Страница поддержки беспроводных технологий
- Cisco Systems – техническая поддержка и документация