Защита беспроводных контроллеров LAN (WLAN)

Содержание

Введение

Предложения этого документа обзор нескольких важных аспектов должен был обработать взаимодействие безопасности между Контроллерами беспроводной локальной сети (WLC) и сеть, где они связаны. Этот документ фокусируется прежде всего на управлении трафиком и не обращается к политике безопасности WLAN, AAA или WPS.

Темы, влияющие на трафик с назначением “к контроллеру”, затронуты в этом документе и не отнесены к трафику, который отнесен “пользователю к сети”.

Примечание: Проверьте изменения прежде, чем применить их к вашей сети, поскольку некоторые примеры в этом документе могут заблокировать административный доступ к вашим контроллерам, если применено неправильно.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Знание того, как настроить WLC и Облегченную точку доступа (LAP) для главной операции
- Базовые знания о Модели OSI
- Понимание, как работает Список контроля доступа (ACL)

Используемые компоненты

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

- Cisco 2000 / 2100 / WLC серии 4400, который выполняет микропрограммное обеспечение 4.2.130.0, 5.2.157.0 или позже

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.

Обработка трафика в WLC

Один критически важный компонент на сетевой безопасности является управлением трафиком. На любых развертываниях это очень важно для прямоугольных типов трафика, поступающего в устройства для предотвращения проблем потенциальной угрозы безопасности (DoS, информационная потеря, расширение полномочий, и т.д.).

На WLC на управление трафиком влияет важный факт: существует два компонента, обрабатывающие трафик в устройстве:

- ЦП — Главный процессор, который заботится обо всем действии управления, RRM, управлении LWAPP, аутентификации, DHCP, и т.д.
- NPU — Сетевой процессор, который заботится о быстром перенаправлении трафика для аутентифицированных клиентов (соединенный проводом к радио и наоборот).

Эта архитектура позволяет быстрое перенаправление трафика и уменьшает загрузку на основном CPU, который может тогда выделить все его ресурсы для задач высокого уровня.

Эта архитектура найдена на этих 4400, WiSM и 3750 интегрированных контроллерах. Для 2106 и WLC NM и отнесенные контроллеры, передача сделана в программном обеспечении, также основным CPU. Поэтому это действительно берет более высокий налог на ЦП. Именно поэтому эти платформы предлагают более низкому пользователю и поддержке количества AP.

Управление трафиком

Каждый раз, когда вы хотите к трафику фильтрации относительно WLC, важно знать, является ли это пользователем к сетевому трафику, или это находится к основному CPU.

- Для любого трафика к ЦП, например, протоколы управления, такие как SNMP, HTTPS, SSH, Telnet или протоколы сетевых сервисов, такие как Радиус или DHCP, использует “ACL ЦП”.
- Для любого трафика к и от беспроводного клиента, включая трафик, проходящий туннель EoIP (гостевой доступ), Интерфейсный ACL, используется ACL WLAN, или на пользовательский ACL.

Трафик определен “к ЦП” как трафик, который вводит контроллер, с назначением к управлению IP-адресами, любому из динамических интерфейсов или адреса рабочего порта. AP - диспетчер не обрабатывает никакой другой трафик кроме LWAPP/CAPWAP.

Управление управляющим доступ

WLC имеют управление доступом “сеансового уровня” для протоколов управления. Важно понять, как они работают для предотвращения неправильной оценки того, что позволено или не позволено контроллером.

Команды для ограничения, какие протоколы управления позволены, (на глобальной области видимости):

- **config network ssh enable|disable** — Это включает или отключает сервис SSH на контроллере. Это значение используется по умолчанию. После того, как отключенный, порт (TCP 22) не будет достижим.
- **config network telnet enable|disable** — Это включает или отключает сервис Telnet на контроллере. Это отключено по умолчанию. После того, как отключенный, порт (TCP 23) не будет достижим.
- **http сети config enable|disable** — Это включает или отключает сервис http на контроллере. Порт (TCP 80) не более длинен достижимый. Это отключено по умолчанию.
- **https сети config enable|disable** — Это включает или отключает сервис https на контроллере. Это значение используется по умолчанию. После того, как отключенный, порт (TCP 443) не будет достижим.
- **config snmp version v1|v2|v3 enable|disable** — Это включает или отключает определенные версии сервиса SNMP на контроллере. Необходимо отключить все для предотвращения доступа SNMP к контроллеру, пока использование ACL.
- **config network mgmt-via-wireless enable|disable** — Это предотвращает это, клиенты, привязанные к этому контроллеру, могут протоколы управления доступом к нему (ssh, https, и т.д.). Это не предотвращает или закрывает соответствующие порты TCP с точки зрения беспроводного устройства. Это означает, что беспроводное устройство, когда это собирается отключить, может открыть SSH - подключение, если включен протокол. Пользователь мог бы видеть запрос имени пользователя, генерируемый демоном SSH, однако завершения сеанса, как только вы пытаетесь ввести имя пользователя.
- **сконфигурируйте сеть mgmt-via-dynamic-interface enable|disable** — Это предотвращает это устройства на той же VLAN, как контроллер может протоколы управления доступом

к нему (ssh, https, и т.д.) к соответствующему адресу динамического интерфейса на той VLAN. Это не предотвращает или закрывает соответствующие порты TCP с точки зрения устройства. Это означает, что устройство, когда это собирается отключить, может открыть SSH - подключение, если включен протокол. Пользователь мог бы видеть запрос имени пользователя, генерируемый демоном SSH, однако завершения сеанса, как только вы пытаетесь ввести имя пользователя. Кроме того, адрес управления будет всегда оставаться доступным от VLAN динамического интерфейса, пока ACL ЦП не будет на месте.

Например, это - конфигурация с помощью вышеупомянутой информации:

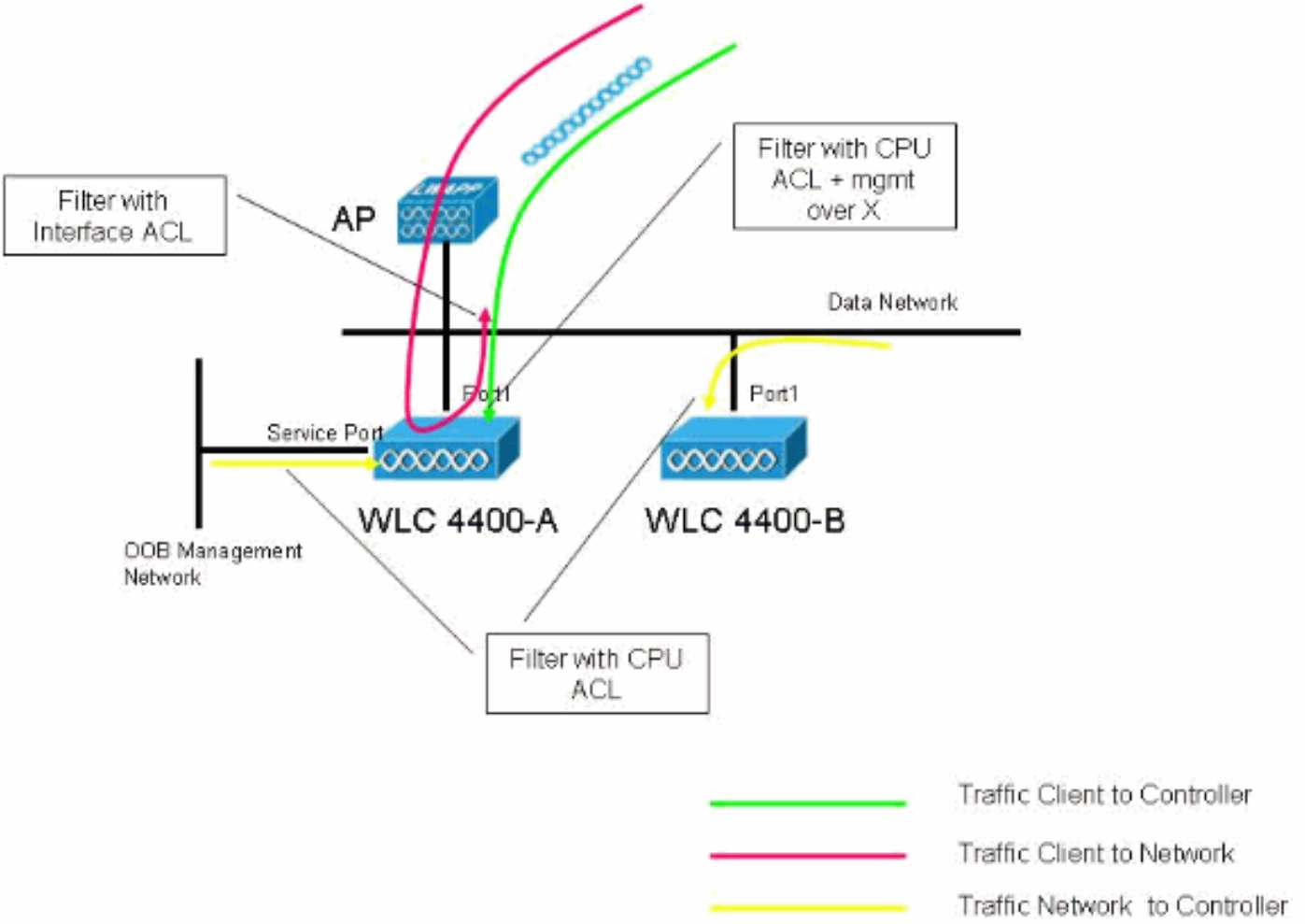
```
(Cisco Controller) >show network summary


RF-Network Name............................. 4400
Web Mode.................................... Disable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Web Mode Cipher-Option SSLv2......... Enable
Secure Shell (ssh).......................... Enable
Telnet...................................... Disable
Ethernet Multicast Mode..................... Enable   Mode: Ucast
Ethernet Broadcast Mode..................... Disable
AP Multicast Mode........................... Unicast
IGMP snooping............................... Disabled
IGMP timeout................................ 60 seconds
User Idle Timeout........................... 300 seconds
ARP Idle Timeout............................ 300 seconds
Cisco AP Default Master..................... Disable
AP Join Priority............................ Disable
Mgmt Via Wireless Interface................. Disable
Mgmt Via Dynamic Interface.................. Disable
Bridge MAC filter Config.................... Enable
Bridge Security Mode........................ EAP
Mesh Full Sector DFS........................ Enable
Over The Air Provisioning of AP's........... Enable
Apple Talk ................................. Disable
AP Fallback ................................ Enable
Web Auth Redirect Ports .................... 80
Fast SSID Change ........................... Disabled
802.3 Bridging ............................. Disable
IP/MAC Addr Binding Check .................. Enabled


(Cisco Controller) >show acl cpu

CPU Acl Name................................ NOT CONFIGURED
Wireless Traffic............................ Disabled
Wired Traffic............................... Disabled
```

Можно прийти к заключению что:

- Telnet и HTTP не будут доступны, таким образом, весь интерактивный трафик управления к контроллеру будет сделан через (зашифрованный) HTTPS/SSH.
- Пользователь беспроводной связи, привязанный к этому контроллеру, не будет в состоянии получить административный доступ.
- Если пользователь беспроводной связи, привязанный к этому контроллеру, сделает сканирование портов, то он будет show SSH и HTTP как открытые, даже при том, что не позволен никакой административный доступ.

- Если проводной пользователь (та же VLAN как динамический интерфейс) сделает сканирование портов, то она будет show SSH и HTTP как открытые, даже при том, что не позволен никакой административный доступ.

Следует отметить, что в средах с несколькими контроллерами на той же группе мобильности, отношение того, что является беспроводным клиентом, только к в настоящее время связанному контроллеру. Поэтому, если один клиент привязан к контроллеру A, то для контроллера B на той же группе мобильности, этот клиент является устройством, прибывающим из VLAN/динамического интерфейса. Это важно для принятия во внимание на менеджменте по беспроводной установке. См. эту схему для примера того, куда поместить ограничение трафика, и какие команды могут влиять на каждую точку входа:



ACL ЦП

Каждый раз, когда вы хотите управлять, какие устройства могут говорить с основным CPU, ACL ЦП используется. Важно упомянуть несколько характеристик для них:

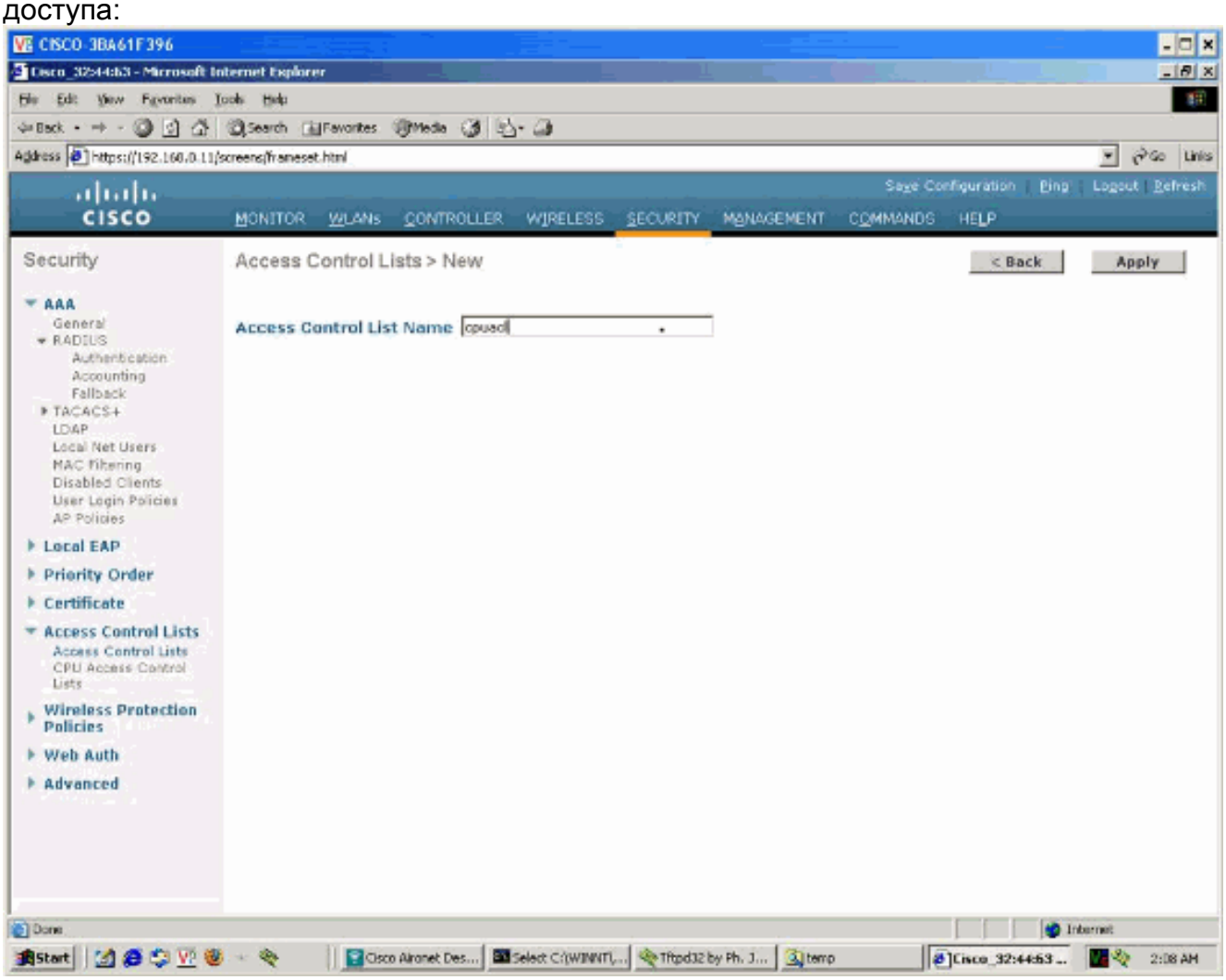
- ACL ЦП только трафик фильтрации к ЦП, и не любой выход трафика или генерируемый ЦП.**Примечание:** Для серии 5500 WLC в версиях 6.0 и позже, ACL ЦП применим для трафика, инициируемого из WLC также. Для других платформ WLC это поведение внедрено в версиях 7.0 и позже. Кроме того, когда создающие поля направления ACL ЦП не оказывают влияния.
- Полная поддержка для ACL ЦП для всего IP - управления контроллера и динамических адресов только присутствует на 4.2.130.0 и позже.
- ACL ЦП, блокирующие трафик сервисного порта, только присутствуют в 5.0 и позже.

- Когда ACL ЦП разработан, важно позволить контрольный трафик между контроллерами. **Команда sh rules** может открыть быстрый вид трафика, разрешенного к ACL ЦП на обычных условиях.
- Контроллер имеет ряд правил фильтрации для внутренних процессов, которые могут быть проверены с **командой sh rules**. ACL не влияют на эти правила, и при этом эти правила не могут модифицироваться на лету. ACL ЦП имеет приоритет по ним.
- На LWAPP или трафик данных CAPWAP не влияют правила ACL ЦП о 4400 базирующихся контроллерах, на контрольный трафик влияют (при выполнении строгого ACL, необходимо явно разрешить его).**Примечание:** На контрольный трафик CAPWAP не влияют ACL ЦП.

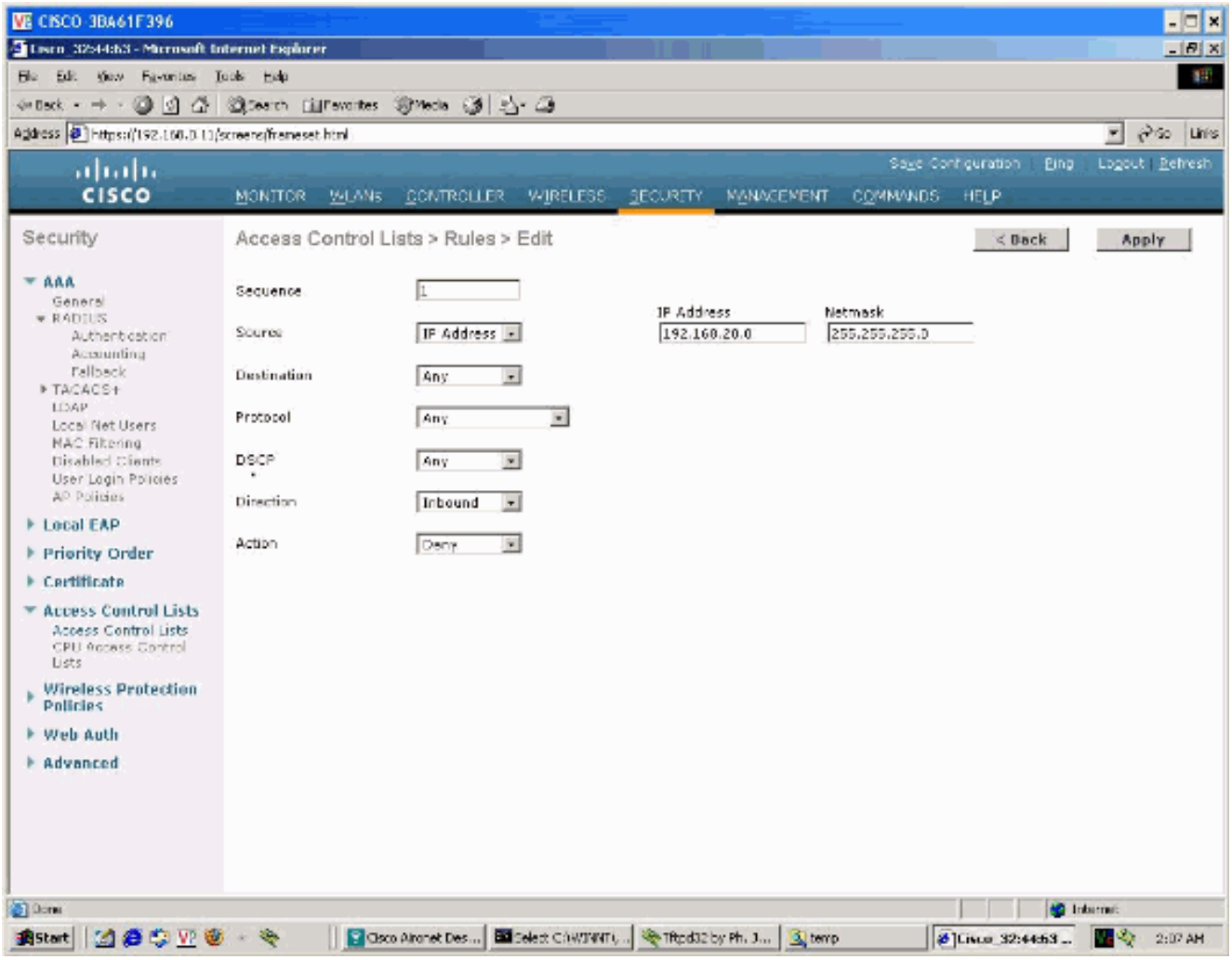
Пример

Например, вы могли бы хотеть заблокировать весь трафик, прибывающий из динамического интерфейса / VLAN (192.168.20.0/24), где пользователи привязаны к ЦП, но позволен любой другой трафик. Это не должно предотвращать беспроводных клиентов для получения согласованного адреса DHCP.

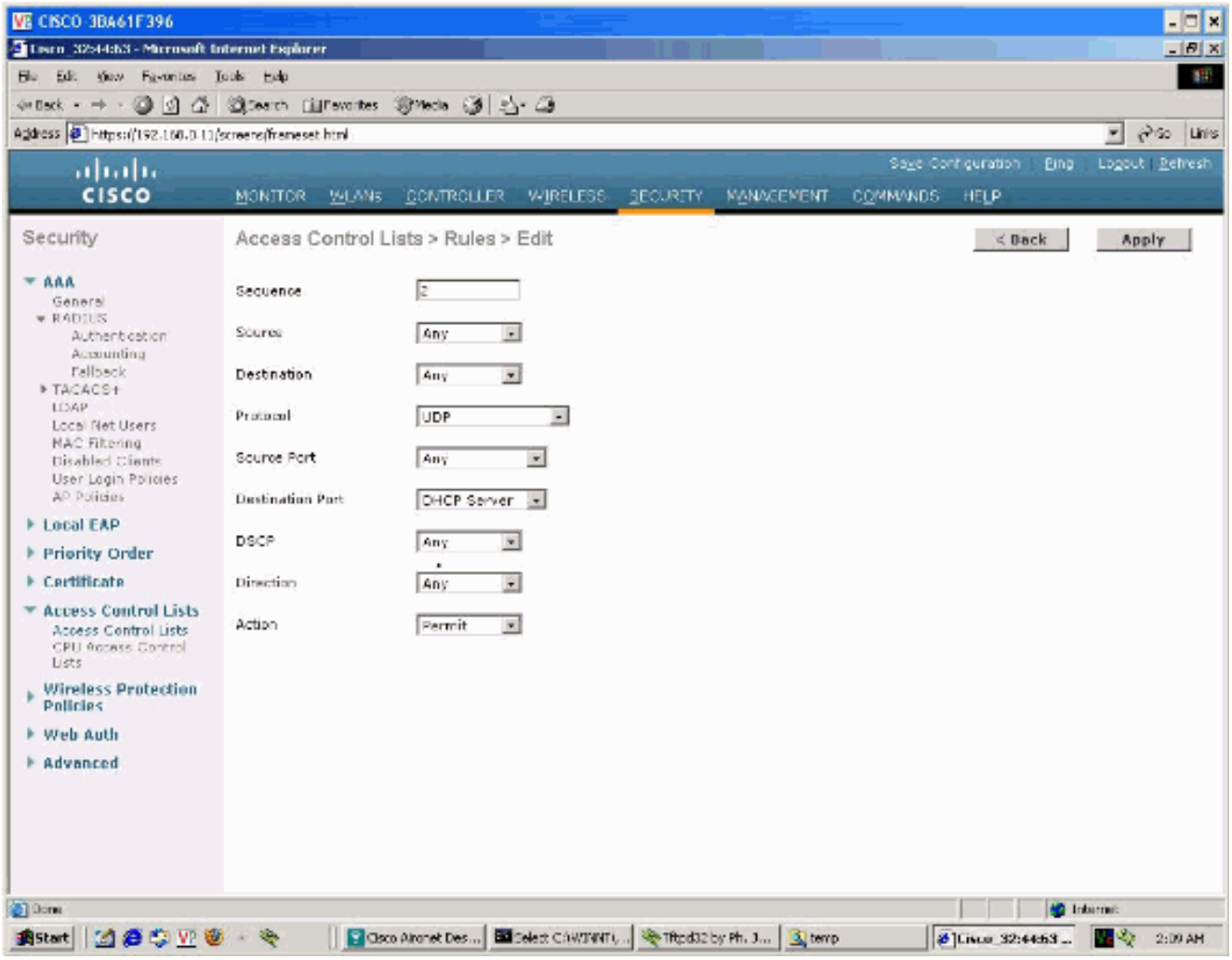
1. Как первый шаг, создан список доступа:



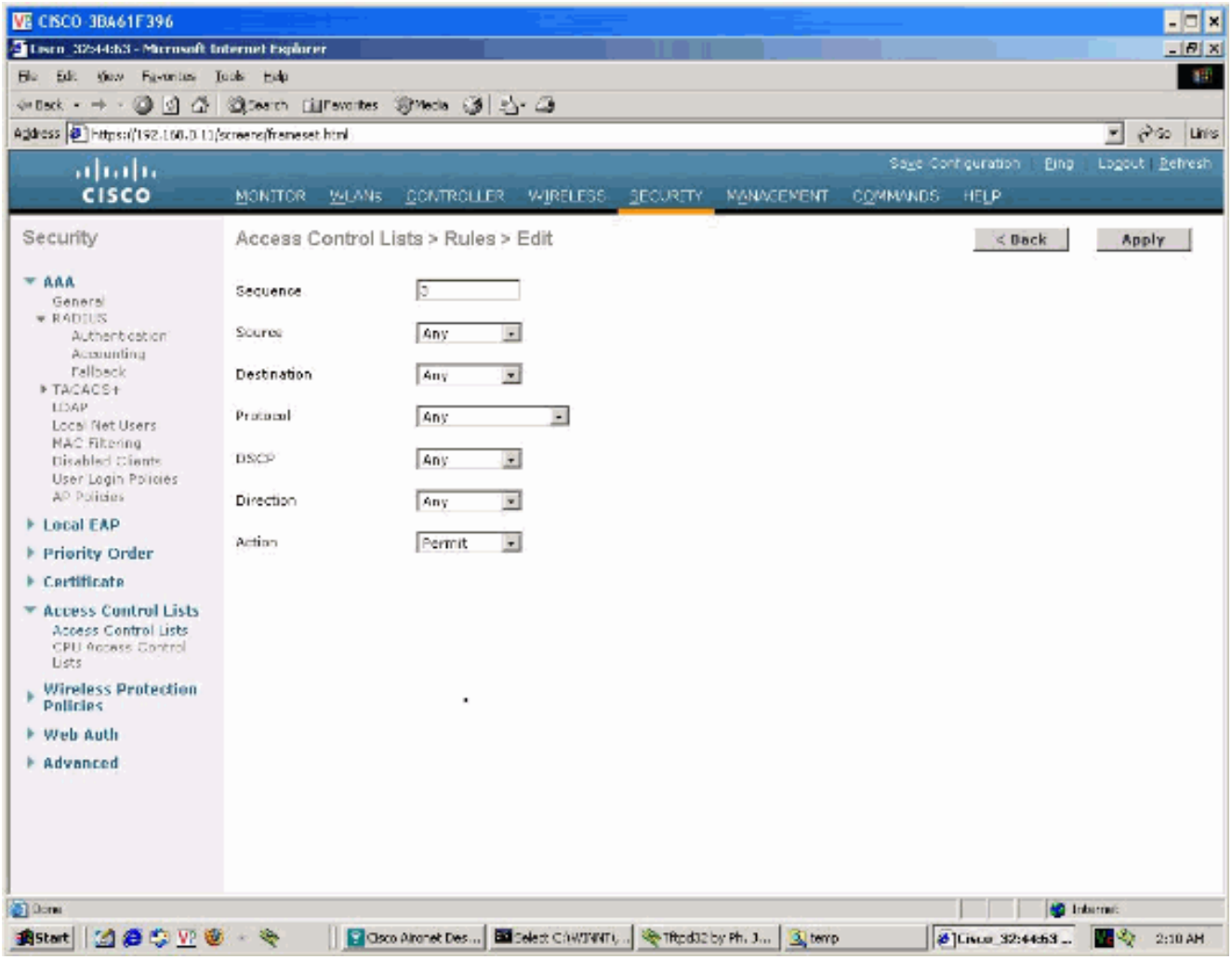
2. **Нажмите add new rule** и заставьте его блокировать весь исходный трафик, прибывающий от 192.168.20.0/24 до любого назначения.



3. Добавьте второе правило, для трафика DHCP, с портом сервера назначения, но с действием
разрешения:

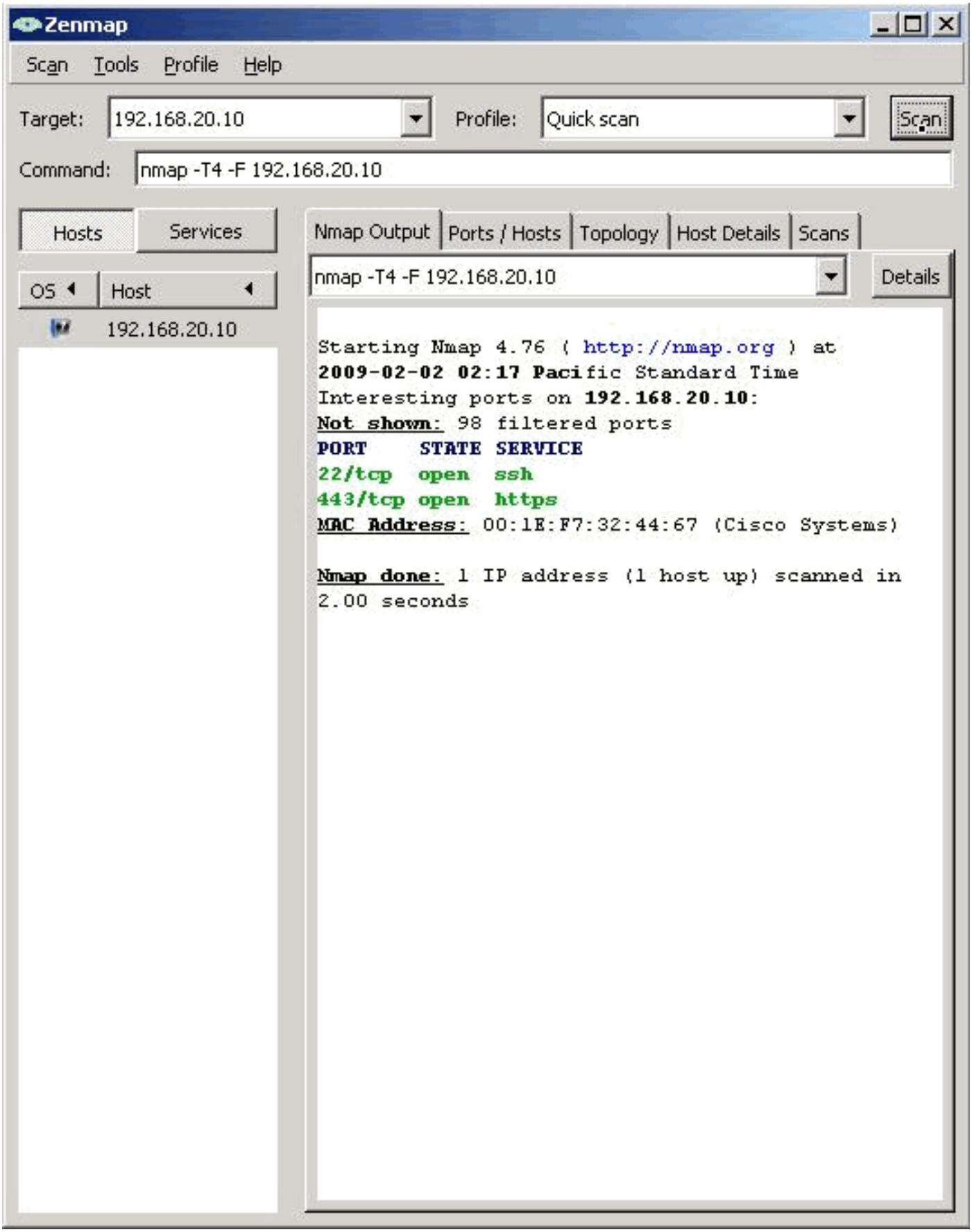


Затем на политику безопасности компании позволен весь другой трафик:



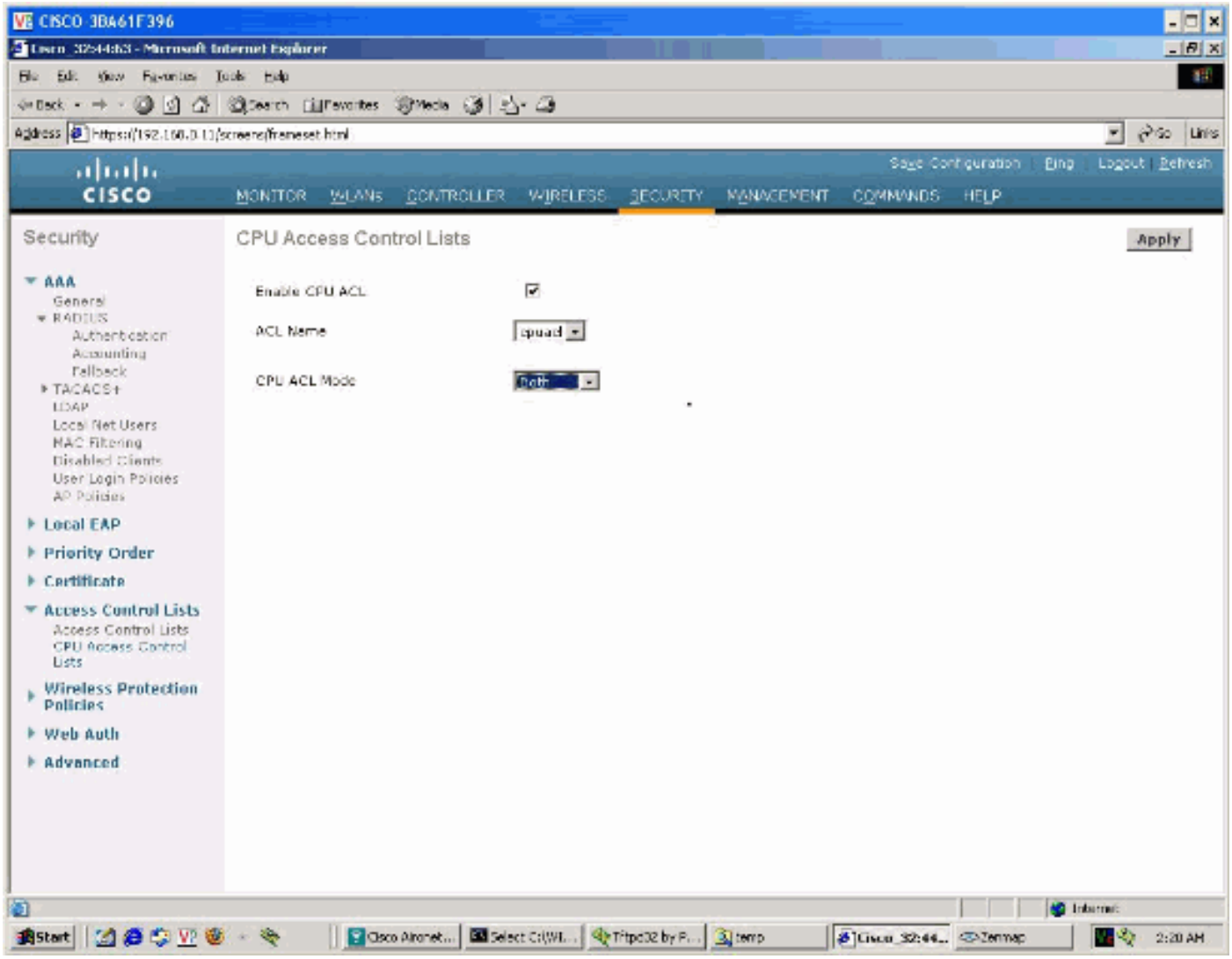
Тестирование перед ACL ЦП

Для проверки эффекта ACL ЦП можно выполнить быстрый просмотр от связанного беспроводного клиента на ВЫПОЛНЕННОМ Статусе для наблюдения текущих открытых портов, на основе конфигурации, прежде, чем применить ACL ЦП:



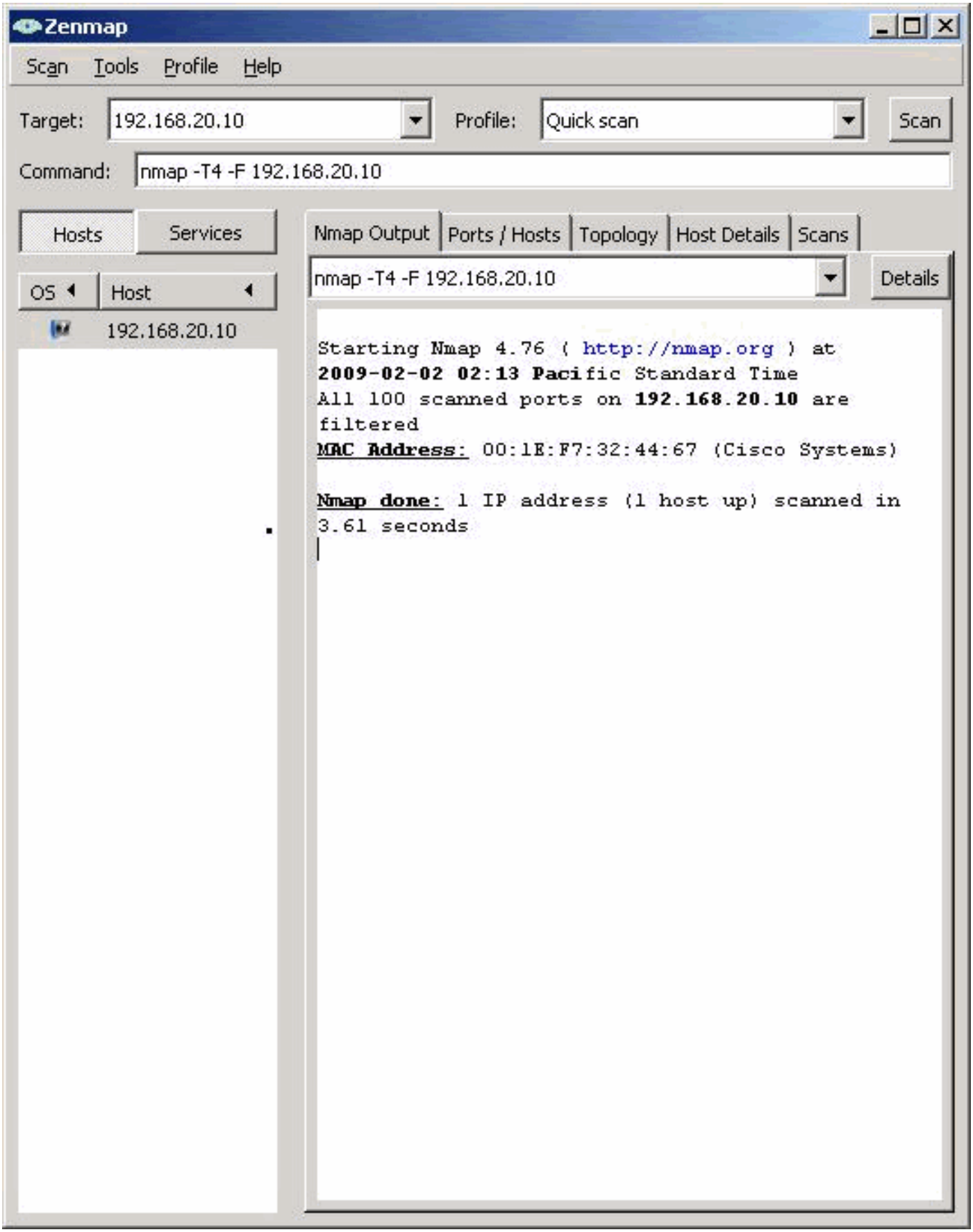
Тестирование после ACL ЦП

Перейдите к **Безопасности> менеджмент> Список контроля доступа ЦП**. Нажмите **Enable CPU ACL** и выберите ACL, который был создан на предыдущем этапе. Затем выберите **И** как направление, чтобы обеспечить, чтобы это было применено к трафику от беспроводных клиентов, и от других устройств на VLAN Динамического интерфейса:



Примечание: Нет никакого направления для трафика acl ЦПУ от 7.0 и далее для всех платформ WLC и только для WLC5500 в 6.0.

Теперь, если тот же просмотр, используемый прежде, повторен, все порты контроллера показывают, как закрыто:



Строгие ACL ЦП

Если политика безопасности требует, “запрещают любого” как последнюю линию для политики, важно понять, что существует несколько типов трафика, передаваемых между контроллером на той же группе мобильности для RRM, мобильности и другими задачами, и что вам мог бы проксировать трафик контроллер к себе для некоторых операций, в

особенности DHCP, где контроллер на режиме proxy DHCP (по умолчанию) может генерировать трафик к себе с целевым UDP 1067 для обработки.

Для полного списка портов, позволенных внутренними передающими правилами по умолчанию, проверьте выходные данные **команды sh rules**. Анализ полного списка выходит за рамки этого документа.

Можно проверить, какие правила списка прав доступа (ACL) поражаются трафиком с **командой config acl counter start**. Счетчики могут быть отображены с **командой sh acl detail ACLNAME**.

Control Plane Policing

Один аспект защиты сетевого устройства, должен удостовериться, что это не переполнено большим количеством трафика управления, который это может обработать. На всех контроллерах, после 4.1 кодов, существует ограничение уровня управления, включенное по умолчанию, который умрет, если трафик для ЦП превысит 2 Мбит/с.

На загруженных сетях возможно наблюдать ограничение в действительности (например, отброшенные эхо-запросы монитора к ЦП). Функция может управляться с **командой config advanced rate**. Можно только включить или отключить его, но скорости "not set" или против которого трафика это будет действовать сначала.

На нормальных работах рекомендуется, чтобы это оставили включенным.

Строгое шифрование для Трафика HTTPS

По умолчанию контроллер предлагает оба высоких и низких шифра силы для обеспечения совместимости с более старыми браузерами во время настройки HTTPS. Контроллер имеет в наличии от RC4 на 40 битов, DES на 56 битов, до AES 256 битов. Выбор самого сильного шифра сделан браузером.

Чтобы удостовериться, что только сильные шифры используются, можно включить им с **командой config network secureweb cipher-option high enable**, таким образом, только 168 3DES или 128 AES и более высокие длины шифра предлагаются контроллером на управляющем доступ HTTPS.

Управление сеансами

Параметры настройки telnet/SSH

По умолчанию контроллер позволяет максимум 5 сопользователей с таймаутом 5 минут. Важно, что эти значения настроены соответственно в вашей среде, поскольку установка их к неограниченному (нуль) может открыть дверь в потенциальный отказ в обслуживании против контроллеров, если пользователи должны были попробовать лобовую атаку перебором паролей против них. Это - пример настроек по умолчанию:

```
(Cisco Controller) >show sessions

CLI Login Timeout (minutes)..... 5
```

```
Maximum Number of CLI Sessions......... 5
```
Помните, что дизайном, даже если управление по радио или динамическому интерфейсу отключено, устройство может все еще сделать SSH - подключение к контроллеру. Это - ЦП налоговая задача, и WLC ограничивает количество одновременных сеансов, и как долго использование этих параметров.

Значения могут быть отрегулированы с **командой config sessions**.

Порт консоли

Последовательный порт имеет разделенное значение таймаута, которое установлено в 5 минут по умолчанию, но он обычно изменяется на 0 (неограниченный) во время сеансов устранения проблем.

```
Cisco Controller) >show serial

Serial Port Login Timeout (minutes)......... 5
Baud Rate.................................... 9600
Character Size............................... 8
Flow Control:................................ Disable
Stop Bits.................................... 1
Parity Type:................................. none
```
Желательно использовать по умолчанию 5 минут. Это предотвращает любого имеющего физический доступ к контроллеру для получения административного доступа, в случае, если зарегистрированный пользователь на консольном порте оставляет сеанс открытым. Значения могут быть отрегулированы с **командой config serial**.

Соединение всех

После проверки другого аспекта обеспечения WLC это может быть суммировано:

- Важно предотвратить устройства кроме станций управления с отступом для доступа к WLC, не только отключая неиспользуемые протоколы, но также и путем ограничения доступа на уровне 4/уровнях 3 с ACL ЦП.
- Ограничение скорости должно быть включено (это по умолчанию).
- Управление доступом посредством **команд management over X** недостаточно для безопасных установок, поскольку пользователи могут все еще протоколы управления доступом, говорящие непосредственно с управлением IP-адресами, с помощью ЦП и ресурсов памяти.

Методы безопасности

Вот некоторые методы безопасности:

- Создайте доступ отбрасывания ACL ЦП от всех VLAN динамического интерфейса или подсетей. Однако позвольте трафик DHCP порту сервера (67), таким образом, клиенты могут получить согласованный адрес DHCP, если прокси DHCP включен (это по умолчанию). Если динамический интерфейс имеет открытый IP - адрес, рекомендуется иметь правило списка прав доступа (ACL), запрещающее весь трафик от неизвестных источников к адресу динамического интерфейса.

- Установите все правила списка прав доступа (ACL), столь же входящие или с направлением **любой**, и отметьте их, как применено и как (соединенный проводом и как опция wireless).Как проверить:`(Cisco Controller) >show acl cpu`

```
CPU Acl Name.............................. acl1
Wireless Traffic.......................... Enabled
Wired Traffic............................. Enabled
```

- Включите ограничение уровня управления (оно включено по умолчанию).Как проверить:`(Cisco Controller) >show advanced rate`

```
Control Path Rate Limiting.....................  Enabled
```

- Всегда используйте зашифрованные протоколы управления (HTTPS, SSH). Это - конфигурация по умолчанию для интерактивного управления. Для SNMP вы, возможно, должны были бы позволить V3 позволить, шифровал/аутентифицировал трафик SNMP. Не забудьте повторно загружать контроллер при внесении изменений в конфигурацию SNMP.Это - то, как проверить:`(Cisco Controller) >show network summary`

```
RF-Network Name........................... 4400
Web Mode.................................. Disable
Secure Web Mode........................... Enable
Secure Web Mode Cipher-Option High........ Enable
Secure Web Mode Cipher-Option SSLv2....... Enable
Secure Shell (ssh)........................ Enable
Telnet.................................... Disable
...
```

- Включите высокое шифрование для HTTPS (это отключено по умолчанию).
- Это - хорошая идея установить проверенный серверный сертификат для доступа HTTPS к вашему контроллеру (подписанный вашим доверяемым CA), заменяя сам подписанный сертификат, установленный по умолчанию.
- Сеанс набора и консольный таймаут к 5 минутам.`(Cisco Controller) >show serial`

```
Serial Port Login Timeout (minutes)......... 5
Baud Rate................................... 9600
Character Size.............................. 8
Flow Control:............................... Disable
Stop Bits................................... 1
Parity Type:................................ none
```

```
(Cisco Controller) >show sessions

CLI Login Timeout (minutes)............ 5
Maximum Number of CLI Sessions......... 5
```

Дополнительные сведения

- Вопросы и ответы по облегченным точкам доступа
- Wireless LAN Controller (WLC) Troubleshoot FAQ
- Вопросы и ответы по контроллеру Wireless LAN (WLC)A
- Управление радиоресурсами при использовании Unified Wireless Network
- Cisco Systems – техническая поддержка и документация