Настройка интегрированная Регистрация URL и создание отчетов гостевого трафика в сети Cisco

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Условные обозначения
Общие сведения
Настройка
Схема сети
Интегрированная Регистрация URL от ASA до НАНОГРАММОВ
Конфигурации
Конфигурация ASA
Настройка WLC
Конфигурация НАНОГРАММОВ
Проверка
Приложения
Опция Appendix A - Wired-Guest
Приложение B – подробные конфигурации для WLC
WLC внешний контроллер
Приложение C – конфигурация ASA
Дополнительные сведения

Введение

Этот документ описывает, как интегрировать Гостевой сервер NAC (NGS) с Контроллерами беспроводной локальной сети (WLC) и Устройство адаптивной защиты (ASA) для обеспечения регистрации URL и создания отчетов гостевого трафика. Много компаний имеют требование для мониторинга гостевого трафика, и эта бумага предоставляет сведения о том, как настроить компоненты Cisco для соответствия тому требованию.

Обратите внимание на то, что существуют множественные решения Cisco для настройки Гостевого доступа в Сети Cisco. Эта статья фокусируется на методе, который использует WLC в качестве технологии включения. WLC имеет уникальную способность к туннельному трафику от границы сети до Интернета с EoIP. Эта функция избавляет от необходимости развертывать VPN или ACL в инфраструктуре сети для ограничения гостевого трафика от утечки во внутреннюю сеть компании.

Объем этой статьи покрытия “Интегрированная Регистрация URL и Сообщающий” в сети “беспроводного гостя”, но этой функции может быть настроен в сети “проводного гостя”, также. Приложение A предоставляет подробную информацию для сети “проводного гостя”.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- ASA, который выполняет версию 8.0.4.24 или позже
- Два контроллера Серии WLC-4400, которые выполняют версию 4.2.130 или позже
- Гостевой сервер NAC, который выполняет версию 2.0 или позже

Используемые компоненты

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

- ASA, который выполняется 8.0.4.26
- Два контроллера WLC-44xx, которые выполняют 4.2.130 кода
- Гостевой сервер NAC, который выполняет 2.0.0 кода
- Catalyst 6500

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

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Общие сведения

Беспроводной гостевой доступ предоставляет значительные деловые преимущества клиентам. Эти преимущества включают уменьшенные эксплуатационные расходы, улучшенную производительность, и упрощенное управление и инициализацию гостевого доступа. Кроме того, Гостевой сервер NAC позволяет клиентам отобразить свою политику допустимого использования и потребовать принятия этой политики до предоставления доступа к Интернету. Теперь, с добавлением интегрированной регистрации URL и создания отчетов, клиенты могут регистрировать гостевое использование и отследить соответствие против их политики допустимого использования.

Настройка

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

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схема сети

В настоящем документе используется следующая схема сети:

Лабораторная топология беспроводного гостя

Catalyst 6500 используется для моделирования корпоративной сети. Гостевой SSID, показанный в красном, сопоставляет с собственным VLAN в ASA, также показанном в красном. Гостевые трафики от ПК в точку доступа, через LWAPP туннелируют к WLC Внешний Контроллер, и затем через туннель EoIP к Якорному контроллеру WLC. Якорный контроллер предоставляет DHCP и сервисы проверки подлинности для гостевой сети. Сервис DHCP предоставляет гостю IP-адрес, шлюз по умолчанию и сервер DNS. Шлюз по умолчанию является ASA, и сервер DNS является общим сервером, расположенным в Интернете. Сервис проверки подлинности в Якорном контроллере связывается с НАНОГРАММАМИ через RADIUS для аутентификации пользователей против базы данных гостя в НАНОГРАММАХ. Гостевой вход в систему инициируется, когда гость открывает web-браузер, и Якорный контроллер перенаправляет трафик к странице аутентификации. В весь трафик в и из гостевой подсети проникают ASA для правила управления политиками и контроля.

Интегрированная Регистрация URL от ASA до НАНОГРАММОВ

Интегрированная Регистрация URL активирована при включении их:

- RADIUS, считающий от Якорного контроллера WLC до НАНОГРАММОВ
- Регистрация http Получает Запросы в ASA
- Передача сообщений системного журнала от ASA до НАНОГРАММОВ

Учет RADIUS предоставляет НАНОГРАММАМ сопоставление между гостевым IP-адресом и ID гостя для определенного периода времени. Регистрация http Добирается, Запросы предоставляет НАНОГРАММАМ журнал того, какой URL посетил гостевой IP-адрес в какое время. НАНОГРАММЫ могут тогда коррелировать эту информацию для представления отчета, который показывает URL, которые посещает определенный гость в течение периода определенного времени.

Обратите внимание на то, что точное время требуется для этой корреляции работать должным образом. Поэтому конфигурация серверов NTP настоятельно рекомендована на ASA, WLC и НАНОГРАММАХ.

Конфигурации

Эти конфигурации используются в данном документе:

- Конфигурация ASA
- Настройка WLC
- Конфигурация НАНОГРАММОВ

Конфигурация ASA

Ключевые задачи конфигурации на ASA включают их:

- NTP
- Проверка HTTP
- Системный журнал

NTP требуется, чтобы обеспечивать надлежащую корреляцию сообщений НАНОГРАММАМИ. Проверка HTTP включает регистрацию URL. Системный журнал является методом, используемым для передачи журналов URL к НАНОГРАММАМ.

В данном примере эта команда используется для включения NTP на ASA:

```
ntp server 192.168.215.62
```

Проверка HTTP позволяет ASA регистрировать URL. В частности **команда inspect http** включает или отключает регистрацию запроса GET с сообщением системного журнала 304001.

Команда inspect http размещена под class-map в policy-map. Когда включено с **командой service-policy**, журналы проверки HTTP Получают запросы с сообщением системного журнала 304001. Код 8.0.4.24 ASA или позже требуется для сообщения системного журнала 304001 показать имя хоста как часть URL.

В данном примере это подходящие команды:

```
policy-map global_policy
 class inspection_default
  inspect http
!
service-policy global_policy global
```

Системный журнал является методом, используемым для передачи регистрации URL к НАНОГРАММАМ. В этой конфигурации только сообщение системного журнала 304001 передается НАНОГРАММАМ с этой конфигурацией:

```
logging enable
logging timestamp
logging list WebLogging message 304001
logging trap WebLogging
logging facility 21
logging host inside 192.168.215.16
```

Настройка WLC

Ключевые действия настройки для Контроллеров беспроводной локальной сети включают их:

- Основной гостевой доступ
- NTP
- Учёт RADIUS

Основная конфигурация гостевого доступа включает конфигурацию WLC Внешний Контроллер и Якорный контроллер WLC так, чтобы гостевой трафик был туннелирован через корпоративную сеть к интернет-DMZ. Конфигурация основного гостевого доступа охвачена в отдельной документации. Рисунки, которые показывают конфигурацию для настройки, охвачены в Приложении.

Серверы NTP добавлены в экране Controller/NTP.

Конфигурация NTP на WLC

Учетный сервер RADIUS требуется так, чтобы сервер НАНОГРАММОВ мог сопоставить IP - адрес источника, полученный в сообщениях системного журнала ASA гостю, который использует тот адрес в то определенное время.

Эти два экрана показывают конфигурацию Проверки подлинности RADIUS и RADIUS, считающего на Якорном контроллере WLC. Конфигурация RADIUS не требуется на Внешнем Контроллере.

Аутентификация RADIUS Учёт RADIUS

Конфигурация НАНОГРАММОВ

- NTP
- Клиенты RADIUS
- Системный журнал

Сервер НАНОГРАММОВ настроен от https://(ip_address) / веб-страница admin. Имя пользователя по умолчанию / пароль является admin/admin.

Серверы NTP добавлены на экране Server/Date-Time-Settings. Рекомендуется, чтобы Системный Часовой пояс был установлен в часовой пояс, где физически расположен сервер. Когда NTP синхронизируется, вы видите сообщение у основания этого экрана, который говорит, “Статус: Активные серверы NTP” наряду с IP-адресом, который показывает “источник текущего времени”.

Конфигурация NTP НАНОГРАММОВ

Сервер НАНОГРАММОВ должен быть настроен с IP-адресом Якорного контроллера как Клиент RADIUS. Этот экран расположен в странице Devices/RADIUS-Clients. Удостоверьтесь, что общий секретный ключ совпадает с, был введен в Якорный контроллер. Нажмите кнопку **Restart** после внесения изменений для перезапуска Сервиса RADIUS на сервере НАНОГРАММОВ.

Клиенты RADIUS

По умолчанию сервер НАНОГРАММОВ принимает сообщения системного журнала от любого IP-адреса. В результате нет никаких дополнительных шагов, требуемых получить сообщения системного журнала от ASA.

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

Выполните эти действия, чтобы проверить, что регистрация URL работает должным образом.

1. От клиентского компьютера соединитесь с беспроводной гостевой сетью. ПК получает

IP-адрес, шлюз по умолчанию и сервер DNS от сервера DHCP в Якорном контроллере.
2. Откройте веб-браузер. Вы перенаправлены к экрану входа в систему. Введите гостевое имя пользователя и пароль. После успешной аутентификации вы перенаправлены к странице по умолчанию в Интернете.
3. Перейдите к различным веб-страницам в Интернете.
4. Подключите ПК управления с НАНОГРАММАМИ в https://(ip_address) и вход в систему как спонсор.
5. Нажмите **Account Management**. Вы видите список гостевых учетных записей. (Если ваша гостевая учетная запись не обнаруживается, нажимает кнопку **Advanced Search** и очищает фильтр, который указывает, что этот спонсор может только видеть учетные записи, которые они создали.)
6. Найдите учетную запись гостя от списка. Перейдите вправо, пока вы не будете видеть подробный значок. Нажмите **подробный** значок.
7. Нажмите вкладку **Activity Log**. Вы видите список URL, которые посетил гость.**Отчёт о Регистрации URL для пользователя**

Отчёт показывает, что гость посетил http://www. cisco . com 1 апреля 2009 в 14:51. Аппаратным адресом 192.168.59.49 является IP-адрес ASA, который передал сообщение системного журнала, содержащее журнал URL. IP - адрес источника для гостей 192.168.0.10. Адрес назначения (DA) 192.168.219.25 для http://www. cisco . com.

Приложения

Опция Appendix A - Wired-Guest

До этой точки эта статья касалась “Интегрированной Регистрации URL и Создания отчетов Гостевого Трафика” для использования в сети “беспроводного гостя”. Этот раздел предоставляет подробную информацию для настройки “проводного гостя”, также. Проводным гостям и беспроводным гостям можно включить на том же WLC Внешний Контроллер.

Это - схема сети для Лабораторной работы Проводной Гостевой сети.

Лабораторная топология проводного гостя

Лабораторная топология проводного гостя подобна лабораторной топологии беспроводного гостя, показанной ранее, за исключением добавления проводного гостевого VLAN. Проводной гостевой VLAN, показанный в красном, является соединением Уровня 2 между ПК проводного гостя и WLC Внешний Контроллер. Трафик от проводного гостя получен WLC Внешний Контроллер и передан EoIP Якорному контроллеру WLC. Якорный контроллер WLC предоставляет DHCP и сервисы проверки подлинности для проводного гостя таким же образом, это предоставило эти сервисы для беспроводного гостя. Шлюз по умолчанию является ASA, и сервер DNS является общим сервером в Интернете. Логически, весь трафик в и из подсети защищен ASA.

Рекомендуется не настроить интерфейс Уровня 3 на Проводном Гостевом VLAN, так как это может позволить точке старта для трафика просочиться из проводного гостевого VLAN в корпоративную сеть.

Приложение B – подробные конфигурации для WLC

Якорный контроллер WLC

Интерфейсы якорного контроллера

Конфигурацию интерфейсов на Якорном контроллере показывают:

Менеджер AP и интерфейсы управления находятся на собственном VLAN физического порта 1 из WLC. Порт 1 подключение к Коммутатору Catalyst и получает трафик от сети заказчика. Гостевой трафик получен через туннель EoIP от Внешнего Контроллера и завершается через этот порт.

Гостевой интерфейс находится на собственном VLAN порта 2, и проводной интерфейс находится на VLAN 9 порта 2. Порт 2 подключения к ASA и используется для отсылки трафика в Интернет.

Группы мобильности якорного контроллера

Для данного примера одна Группа мобильности настроена для Внешнего (Проводного) Контроллера и отдельная Группа мобильности для Якорного контроллера (Привязка). Конфигурацию на Якорном контроллере показывают.

WLAN якорного контроллера

Якорный контроллер - привязка к набору для гостевого WLAN

Для настройки или show mobility anchor для WLAN, переместите мышь в стрелку выпадающего списка справа и выберите **Mobility Anchors**, как показано.

Якорный контроллер - привязка к Набору к себе Якорный контроллер - WLAN для беспроводных Гостей Якорный контроллер - WLAN для (дополнительных) проводных гостей Якорный контроллер - области DHCP Якорный контроллер - область DHCP для беспроводных Гостей: Якорный контроллер - DHCP для (дополнительных) Проводных Гостей:

WLC внешний контроллер

Интерфейсы

Конфигурацию интерфейсов на Внешнем Контроллере показывают.

Менеджер AP и интерфейсы управления находятся на собственном VLAN физического порта 1 из WLC.

Если вы хотите предоставить гостевой доступ к проводной сети, проводной интерфейс является *дополнительным* и только требуется. Проводной интерфейс находится на VLAN 8 физического порта 1. Этот интерфейс получает трафик от Гостевого VLAN Коммутатора Catalyst и передает ему туннель EoIP, через собственный VLAN, к Якорному контроллеру.

Внешний контроллер - группы мобильности

Конфигурацию на Внешнем Контроллере показывают.

Внешний контроллер - WLAN

Для настройки или show mobility anchor для WLAN, переместите мышь через стрелку

выпадающего списка справа и выберите **Mobility Anchors**, как показано.

Набор Привязки к мобильности к Якорному контроллеру Внешний Контроллер - Гостевой WLAN для беспроводных Гостей

s

Внешний контроллер - WLAN для Проводных Гостей (Необязательно) – продолженный

Приложение C – конфигурация ASA

```
ASA-5520# show run
:
ASA Version 8.0(4)26
!
hostname ASA-5520
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address dhcp setroute
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.59.49 255.255.255.240
!
interface GigabitEthernet0/2
   <- Guest traffic enters this interface
 nameif wireless_guest
 security-level 50
 ip address 192.168.0.254 255.255.255.0
!
interface Management0/0
 nameif management
 security-level 100
 ip address 192.168.99.1 255.255.255.0
 management-only
!
boot system disk0:/asa804-26-k8.bin
clock timezone CST -6
clock summer-time CDT recurring
logging enable
logging timestamp
   <- provide a timestamp in each syslog message
logging list WebLogging message 304001
   <- list includes URL Log message (304001)
logging console errors
logging buffered notifications
logging trap WebLogging
   <- Send this list of Log messages to syslog servers
logging asdm informational
logging facility 21
logging host inside 192.168.215.16
   <- NGS is the syslog server
asdm image disk0:/asdm-61551.bin
route inside 10.10.10.0 255.255.255.0 192.168.59.62 1
route inside 192.168.215.0 255.255.255.0 192.168.59.62 1
route inside 198.168.1.15 255.255.255.255 192.168.59.62 1
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.99.0 255.255.255.0 management
!
```

```
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 198.168.1.15 <- Configure ntp server
!
class-map inspection_default
 match default-inspection-traffic
!
policy-map type inspect dns migrated_dns_map_1
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect http
   <- Enable http inspection on the global policy
!
service-policy global_policy global
   <- Apply the policy
prompt hostname context
Cryptochecksum:b43ff809eacf50f0c9ef0ae2a9abbc1d
: end
```

Дополнительные сведения

- Служба удаленной аутентификации пользователей коммутируемого доступа (RADIUS)
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация