Пример конфигурации беспроводного NAC вне диапазона (OOB)

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Условные обозначения
Общие сведения
Обзор решения Cisco для контроля допуска к сети (NAC)
Режим виртуального шлюза (режим моста)
Внеполосный режим
Единый вход в систему
Настройка беспроводного решения NAC OOB
Настройка коммутатора Catalyst
Пошаговая настройка NAC OOB в WLC и NAC Manager
Настройка единого входа в систему (SSO) с применением беспроводного решения OOB
Пошаговая настройка SSO в NAC Manager
Пошаговая настройка SSO на контроллере беспроводной локальной сети
Проверка
Команды для проверки в интерфейсе командной строки CISCO WLC
Проверка состояния клиента из графического интерфейса WLC
Проверка единого входа в систему на сервере NAC с WLC
Устранение неполадок
Команды для устранения неполадок
Дополнительные сведения

Введение

В этом документе даны рекомендации по проектированию сети для развертывания внеполосной (OOB) технологии Cisco для контроля допуска к сети (NAC) на устройствах, обеспечивающих безопасность оконечного оборудования в унифицированной беспроводной сети Cisco. В описании рекомендуемой практики предполагается, что унифицированная беспроводная сеть Cisco развернута в соответствии с рекомендациями, изложенными в Руководстве по проектированию корпоративных средств мобильности 3.0.

Рекомендуемое проектное решение — виртуальный шлюз (в режиме моста) и централизованное развертывание решения OOB с единым входом в систему на основе RADIUS. Контроллер беспроводной локальной сети (WLC) размещается на 2-м уровне в смежности с сервером NAC. Клиент связывается с WLC, и WLC выполняет аутентификацию

пользователя. После прохождения аутентификации пользовательский трафик проходит через карантинную сеть VLAN от WLC на сервер NAC. Выполняется процесс оценки состояния и корректировки нарушений. После того, как данные пользователя будут удостоверены, пользовательская сеть VLAN в WLC сменяется с карантинной на сеть VLAN для доступа. После того, как пользователь перейдет в сеть VLAN для доступа, трафик минует сервер NAC.

Предварительные условия

Требования

Описанная в этом документе конфигурация относится только к выпускам NAC 4.5 и WLC 5.1

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

- NAC Server 3350 4.5
- NAC Manager 3350 4.5
- WLC 2106 5.1

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

Обзор решения Cisco для контроля допуска к сети (NAC)

Cisco NAC использует сетевую инфраструктуру для обеспечения соответствия всех устройств, которые запрашивают доступ к вычислительным ресурсами, политикам безопасности. С помощью устройства Cisco NAC сетевые администраторы могут выполнять аутентификацию, авторизацию, оценку и устранение неполадок для проводных, беспроводных и удаленных пользователей, а также для их компьютеров, перед предоставлением доступа к сети. Устройство определяет, соответствуют ли сетевые устройства, например, переносные компьютеры, IP-телефоны и игровые консоли, политикам безопасности сети и устраняет уязвимости перед предоставлением доступа к этой сети.

Ниже поясняется терминология рекомендуемого проектного решения:

Режим виртуального шлюза (режим моста)

Устройство NAC, настроенное как виртуальный шлюз, играет роль моста между конечными пользователями и шлюзом по умолчанию (маршрутизатором) для управляемой клиентской подсети. Для конкретной клиентской сети VLAN, устройство NAC служит мостом для трафика от недоверенного интерфейса к доверенному интерфейсу. Когда оно применяется как мост между недоверенной и доверенной сторонами устройства, используются две сети VLAN. Например, между контроллером беспроводной локальной сети (WLC) и недоверенным интерфейсом устройства NAC определяется клиентская сеть VLAN 110. На коммутаторе распределения отсутствует маршрутизируемый интерфейс или виртуальный коммутируемый интерфейс (SVI), связанный с сетью VLAN 110. Сеть VLAN 10 настраивается между доверенным интерфейсом устройства NAC и интерфейсом маршрутизатора следующего перехода или интерфейсом SVI для клиентской подсети. В устройстве NAC задается правило привязки, которое пересылает пакеты, поступающие через сеть VLAN 110, на выход через сеть VLAN 10 в случае обмена информацией о метках VLAN, показанном на рис. 1-1. Для пакетов, возвращающихся клиенту, имеет место противоположный процесс. Следует отметить, что в этом режиме блоки BPDU из сетей VLAN недоверенной стороны в сети VLAN доверенной стороны не передаются. Параметр привязки VLAN обычно выбирается, когда устройство NAC логически внедрено между клиентами и защищаемыми сетями. Этот параметр мостового соединения должен использоваться в том случае, если устройство NAC развертывается в режиме виртуального шлюза в окружении унифицированной беспроводной сети. *Поскольку сервер NAC осведомлен о протоколах верхнего уровня, то по умолчанию он явным образом разрешает протоколы, которые требуют его подключения к сети в роли, подразумевающей прохождение аутентификации, например DNS и DHCP.*

Рис. 1-1 Виртуальный шлюз с привязкой сетей VLAN

Внеполосный режим

Внеполосная конфигурация требует прохождения пользовательского трафика через устройство NAC только в рамках аутентификации, оценки состояния и корректировки. После того, как пользователь пройдет аутентификацию и все проверки политики, трафик начинает коммутироваться обычным образом через сеть, минуя сервер NAC. Подробности можно найти в главе 4 Руководства по установке и администрированию Clean Access Manager для устройств Cisco NAC.

При настройке устройства NAC этим способом контроллер WLC представляет собой управляемое устройство с точки зрения NAC Manager аналогично тому, как коммутатор Cisco управляется диспетчером NAC Manager. После того, как пользователь пройдет аутентификацию и оценку состояния, диспетчер NAC Manager указывает контроллеру WLC маркировать пользовательский трафик из сети VLAN NAC для получения доступа к сети VLAN, предлагающей полномочия доступа.

Рис. 1-2. Устройство NAC во внеполосном режиме с режимом виртуального шлюза

Единый вход в систему

Концепция единого входа в систему или однократной регистрации (SSO) не требует вмешательства пользователя и относительно проста в реализации. Она использует функциональную возможность SSO для сетей VPN в решении NAC в совокупности с программным обеспечением Clean Access Agent, работающим на клиентском ПК. VPN SSO использует учетные записи RADIUS для уведомления устройства NAC о прошедших аутентификацию пользователях удаленного доступа, которые подключаются к сети.

Аналогичным образом эта функция может использоваться вместе с контроллером беспроводной локальной сети для автоматического уведомления сервера NAC о беспроводных клиентах, подключившихся к сети и прошедших аутентификацию.

Примеры беспроводного клиента, взаимодействующего с устройством NAC для аутентификации SSO, оценки состояния, корректировки и получения доступа к сети см. на рис. 1-3–1-6.

Эта последовательность операций показана на рис. 1-3:

1. Пользователь беспроводной сети проходит аутентификацию 802.1x/EAP на вышестоящем сервере AAA через контроллер беспроводной локальной сети.
2. Клиент получает IP-адрес от сервера AAA или сервера DHCP.
3. После получения IP-адреса клиентом контроллер WLC пересылает устройству NAC начальную запись учета RADIUS, включающую IP-адрес беспроводного клиента.**Примечание:** Использование контроллера WLC, которое одиночная учетная запись RADIUS (запускает) для аутентификации клиента 802.1x и присвоения IP-адреса, в то время как коммутаторы Cisco Catalyst передают две учетных записи: начальную запись после аутентификации клиента 802.1x и промежуточное обновление после назначения IP-адреса клиенту.
4. После обнаружения соединения с сетью ПО NAC Agent пытается подключиться к диспетчеру CAM (по протоколу SWISS). Трафик перехватывается сервером NAC, который, в свою очередь, опрашивает диспетчер NAC Manager, определяя присутствие пользователя в списке подключенных пользователей. В этом списке присутствуют только клиенты, прошедшие аутентификацию, что имеет место в рассмотренном выше примере в результате обновления RADIUS на шаге 3.
5. ПО NAC Agent выполняет локальную оценку состояния безопасности/риска клиентской машины и пересылает оценку серверу NAC для принятия решения о допуске к сети.**Рис. 1-3. Процесс аутентификации и оценка состояния клиента**

На рис. 1-4 представлена следующая последовательность:

1. Устройство NAC пересылает оценку диспетчеру устройств NAC (CAM).
2. В этом примере CAM заключает, что клиент не отвечает требованиям и указывает устройству NAC поместить пользователя в карантинную роль.
3. Затем устройство NAC передает клиентскому агенту сведения для корректировки.**Рис. 1-4. Движение информации об оценке состояния от сервера CAS к CAM**

Эта последовательность имеет место на рисунке 1-5:

1. Клиентский агент отображает время до завершения корректировки.
2. Агент пошагово ориентирует пользователя в процессе корректировки. Этот процесс может, например, заключаться в обновлении файла определений для антивируса.
3. После завершения корректировки агент оповещает сервер NAC.
4. CAM выдает пользователю текст принятых правил пользования (AUP).**Рис. 1-5. Процесс исправления клиента с применением CAS в качестве устройства реализации**

Эта последовательность имеет место на рисунке 1-6:

1. После согласия с принятыми правилами пользования устройство NAC переключает пользователя в подключенную (авторизованную) роль.
2. Функция SSO вносит IP-адрес клиента в список подключенных пользователей. После

корректировки запись хоста добавляется в подтвержденный список. Обе таблицы (вместе с таблицей обнаруженных клиентов) находятся в ведении CAM (диспетчера устройств NAC).
3. Диспетчер NAC передает контроллеру WLC уведомление о записи SNMP для изменения сети VLAN пользователя с карантинной на сеть доступа.
4. Пользовательский трафик начинает выходить из WLC с меткой сети VLAN доступа. Сервер NAC перестает быть транзитным для трафика данного конкретного пользователя.**Рис. 1-6 После переключения в сеть VLAN доступа подтвержденный клиент обходит сервер CAS**

Наиболее прозрачный способ упрощения аутентификации пользователей беспроводной сети состоит во включении аутентификации VPN-SSO на сервере NAC и настройке контроллеров WLC для передачи данных учета RADIUS на сервер NAC. В случае необходимости пересылки записей учета на вышестоящий сервер RADIUS, находящийся в сети, можно настроить сервер NAC для пересылки пакетов учета серверу RADIUS.

Примечание: Если аутентификация SSO VPN включена без Чистого агента Доступа, установленного на клиентском компьютере, пользователь все еще автоматически аутентифицируется. Однако он не подключается автоматически через устройство NAC, пока не будет открыт его web-браузер и не будет предпринята попытка подключения. В этом случае, когда пользователь открывает свой web-браузер, выполняется его мгновенная переадресация (без приглашения входа в систему) в рамках «безагентского» этапа. По завершении процесса SSO пользователь соединяется с первоначально запрошенным URL-адресом.

Настройка беспроводного решения NAC OOB

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.

В текущей реализации NAC WLC интегрируется с устройством Cisco NAC только во внутриполосном режиме, при котором устройство NAC должно оставаться на пути данных даже после подтверждения пользователя. После того, как устройство NAC завершит проверку состояния, сотрудник или гостевой пользователь получает доступ к сети в зависимости от его роли.

В выпусках NAC 4.5 и WLC 5.1 беспроводное решение NAC поддерживает интеграцию OOB с устройством NAC. Когда клиент связывается и выполняет аутентификацию 2-го уровня (L2Auth), проверяется, связан ли карантинный интерфейс с WLAN/SSID. Если да, то начальный трафик отправляется по карантинному интерфейсу. Клиентский трафик идет по карантинной сети VLAN, образующей групповой канал с устройством NAC. После подтверждения состояния диспетчер NAC отправляет сообщение установки SNMP, которое обновляет идентификатор сети VLAN доступа; контроллер обновляет свое состояние на основании идентификатора сети VLAN доступа, и начинается коммутация трафика данных непосредственно в сеть минуя сервер NAC.

Рис. 2-1. Пример автономного сервера CAS в режиме моста, подключенного к WLC через коммутатор

На рис. 2-1 контроллер WLC соединяется с портом магистрали, который обслуживает карантинную сеть VLAN и сеть VLAN доступа (176 и 175). На коммутаторе трафик карантинной сети VLAN передается по групповому каналу на устройство NAC, а трафик сети VLAN доступа непосредственно передается по групповому каналу на коммутатор 3-го уровня. Трафик, достигающий карантинной сети VLAN на устройстве NAC, привязывается для доступа к сети VLAN на основе статической конфигурации привязки. Когда связанный клиент выполняет аутентификацию 2-го уровня, он проверяет, связан ли карантинный интерфейс; если да, то данные передаются на карантинный интерфейс. Клиентский трафик идет по карантинной сети VLAN, образующей групповой канал с устройством NAC. После подтверждения состояния сервер NAC (CAS) передает сообщение установки SNMP, которое оповещает контроллер об идентификаторе сети VLAN доступа, после чего трафик начинает коммутироваться от контроллера WLC непосредственно в сеть, минуя сервер NAC.

Ограничения

- Не выполняется связывание профиля порта
- В NAC Manager не указывается идентификатор сети VLAN: он определяется на WLC
- Поддержка фильтра MAC-адресов не позволяет использовать идентификатор VLAN из настроек роли
- Внеполосный Действительный режим сервера NAC шлюза поддерживает только
- Контроллер WLC связывается с сервером NAC на 2-м уровне
- Для реализации OOB NAC нельзя использовать маршрутизатор ISR с функцией NAC и диспетчер сети с функцией WLC

Примечание: См. Сопоставление VLAN в разделе Режимов виртуального шлюза устройства Cisco NAC - Чистое Руководство Конфигурации сервера доступа, Выпуск 4.8 (1) для получения дополнительной информации о том, как безопасно настроить VLAN в режимах виртуального шлюза.

Настройка коммутатора Catalyst

```
interface GigabitEthernet2/21
 description NAC SERVER UNTRUSTED INTERFACE switchport switchport trunk native vlan 998
switchport trunk allowed vlan 176 switchport mode trunk no ip address ! interface
GigabitEthernet2/22 description NAC SERVER TRUSTED INTERFACE switchport switchport trunk native
vlan 999 switchport trunk allowed vlan 11,175 switchport mode trunk no ip address ! interface
GigabitEthernet2/23 description NAC MANAGER INTERFACE switchport switchport access vlan 10 no ip
address spanning-tree portfast ! interface GigabitEthernet2/1 description WLC switchport
switchport trunk allowed vlan 75,175,176 switchport trunk native vlan 75 switchport mode trunk
no ip address ! interface Vlan75 Description WLC Management VLAN ip address 10.10.75.1
255.255.255.0 ! interface Vlan175 Description Client Subnet Access VLAN ip address 10.10.175.1
255.255.255.0 end
```

Пошаговая настройка NAC OOB в WLC и NAC Manager

Для настройки NAC OOB в контроллере WLC и диспетчере NAC Manager выполните следующие шаги:

1. Включите на контроллере режим SNMP v2.
2. Создайте профиль для WLC на диспетчере CAM Manager. **Выберите OOB Management Profile > Device > New (Профиль управления OOB > Устройство > Создать).**
3. **После создания профиля на диспетчере CAM добавьте в профиль контроллер WLC; перейдите в раздел OOB Management > Devices > New (Управление OOB > Устройства**

> Создать) и введите IP-адрес интерфейса управления WLC.Теперь контроллер добавлен в диспетчер CAM Manager.

4. Добавьте CAM в качестве получателя сообщений прерывания SNMP-trap от WLC. В качестве получателя SNMP используйте точное имя получателя прерывания в CAM.
5. **Настройте получателя сообщения SNMP-trap в CAM под именем, совпадающим с заданным на контроллере; в разделе OOB Management > SNMP Receiver (Управление OOB > Получатель SNMP) выберите Profiles (Профили).**На этом этапе WLC и CAM могут взаимодействовать друг с другом для подтверждения состояния клиента и обновления состояния доступа/карантина.
6. В контроллере создайте динамический интерфейс с сетями VLAN для доступа и карантина.
7. Создайте сеть WLAN и свяжите ее с динамическим интерфейсом.
8. После этого включите NAC в сети WLAN.
9. **Добавьте клиентскую подсеть на сервере CAS в качестве управляемой подсети; щелкните CAS server > Select your CAS server > Manage >Advanced > Managed Subnets >Add Unused IP address from the client subnet (Сервер CAS > Выберите сервер CAS > Управление > Дополнительно > Управляемые подсети > Добавить неиспользуемый IP-адрес из клиентской подсети) и укажите карантинную (недоверенную) сеть VLAN для управляемой подсети.**
10. Создайте привязки VLAN на сервере CAS. Выберите **server> CAS Выбирают ваш server> CAS, Управляют> Усовершенствованный> Сопоставление VLAN**. Добавьте сеть VLAN доступа в качестве доверенной и карантинную сеть VLAN в качестве недоверенной.

Настройка единого входа в систему (SSO) с применением беспроводного решения OOB

Для поддержки SSO в беспроводной конфигурации существует ряд требований:

1. Включите аутентификацию VPN на сервере NAC. На устройстве NAC концентратор WLC определяется как «VPN concentrator» (концентратор VPN).
2. Включите на контролере WLC учет RADIUS. Контроллер, определенный на устройстве NAC, должен быть настроен для отправки записей учета RADIUS устройству NAC для каждой беспроводной локальной сети 802.1x/EAP, которая является управляемой подсетью на контроллере NAC.

Пошаговая настройка SSO в NAC Manager

Для настройки SSO в NAC Manager выполните следующие действия:

1. **В левой части экрана в разделе меню CAM Device Management (Управление устройствами) выберите CCA Server (Сервер Cisco Clean Access) и пройдите по ссылке NAC Server (Сервер NAC).**
2. **На странице Server Status (Состояние сервера) выберите вкладку Authentication (Аутентификация) и войдите во вложенное меню VPN Auth (Аутентификация VPN).** См. рис. 3-1.**Рис. 3-1. Включение сервера NAC для единого входа в систему**
3. **Для добавления новой записи WLC выберите VPN Concentrators Setting (Настройка концентраторов VPN, рис. 3-2).** Заполните поля IP-адреса управления WLC и общего

секретного ключа, используемого WLC и сервером NAC.**Рис. 3-2. Добавление WLC в качестве клиента RADIUS в разделе VPN-концентратора**

4. **Для привязки ролей добавьте новый сервер аутентификации с типом vpn sso в разделе User Management > Auth Servers (Управление пользователями > Серверы аутентификации).**
5. **Щелкните значок Mapping (Привязка) и добавьте правило привязки (Mapping Rule).** Привязка зависит от значения атрибута класса 25, отправляемого контроллером WLC в пакете учета. Это значение атрибута настраивается на сервере RADIUS и изменяется в зависимости от авторизации пользователя. **В этом примере атрибут имеет значение ALLOWALL и помещается в роль AllowAll.**

Пошаговая настройка SSO на контроллере беспроводной локальной сети

Для реализации единого входа в систему с сервером RADIUS необходимо настроить на WLC учет RADIUS.

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.**

Команды для проверки в интерфейсе командной строки CISCO WLC

```
(Cisco Controller) >show interface summary

Interface Name    Port Vlan Id    IP Address      Type    Ap Mgr Guest
------------------------------------------------ ---- -------- ------
ap-manager        1    untagged   10.10.75.3      Static  Yes    No
management        1    untagged   10.10.75.2      Static  No     No
nac-vlan          1    175        10.10.175.2     Dynamic No     No
service-port      N/A  N/A        192.168.1.1     Static  No     No
virtual           N/A  N/A        1.1.1.1         Static  No     No


(Cisco Controller) >show interface detailed management

Interface Name..................................... management
MAC Address........................................ 00:18:73:34:b2:60
IP Address......................................... 10.10.75.2
IP Netmask......................................... 255.255.255.0
IP Gateway......................................... 10.10.75.1
VLAN............................................... untagged
Quarantine-vlan.................................... 0
Active Physical Port............................... 1
Primary Physical Port.............................. 1
Backup Physical Port............................... Unconfigured
Primary DHCP Server................................ 10.10.75.1
Secondary DHCP Server.............................. Unconfigured
DHCP Option 82..................................... Disabled
ACL................................................ Unconfigured
AP Manager......................................... No
Guest Interface.................................... No
```

```
(Cisco Controller) >show interface detailed nac-vlan

Interface Name................................. nac-vlan
MAC Address.................................... 00:18:73:34:b2:63
IP Address..................................... 10.10.175.2
IP Netmask..................................... 255.255.255.0
IP Gateway..................................... 10.10.175.1
VLAN........................................... 175 Quarantine-
vlan.............................. 176 Active Physical Port.......................... 1
Primary Physical Port.......................... 1 Backup Physical
Port........................... Unconfigured Primary DHCP Server.............................
10.10.175.1 Secondary DHCP Server.......................... Unconfigured DHCP Option
82................................ Disabled ACL.........................................
Unconfigured AP Manager..................................... No Guest
Interface.............................. No
```

Проверка состояния клиента из графического интерфейса WLC

Первоначально клиент пребывает в состоянии карантина, пока устройство NAC не выполнит анализ состояния.

По завершении анализа состояния клиент должен получить состояние NAC Access (Доступ).

Проверка единого входа в систему на сервере NAC с WLC

В разделе VPN Auth (Аутентификация VPN) перейдите в подраздел Active Client (Активный клиент) для проверки поступления начального пакета учета от WLC. Эта запись присутствует при наличии на клиентской машине установленного агента CCA.

Для выполнения процесса единого входа в систему без агента необходимо открыть браузер. Когда пользователь открывает браузер, выполняется процесс SSO, и пользователь появляется в списке подключенных пользователей (OUL). Пользователь удаляется из списка активных клиентов посредством стоп-пакета RADIUS.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Команды для устранения неполадок

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

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

Дополнительные сведения

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