# Уровень 3 NAC Cisco OOB с ACL

## Содержание

# Введение

Система контроля доступа к сети Cisco NAC (NAC) принуждает политику сетевой безопасности организации на всех устройствах, ища доступ к сети. NAC Cisco позволяет только совместимые и доверяемые оконечные устройства, такие как PC, серверы и PDA, на сеть. Доступ ограничен для не соответствующих стандарту устройств, который ограничивает потенциальный ущерб от появляющихся угроз безопасности и рисков. NAC Cisco дает организациям мощный, основанный на ролях метод предотвращению неавторизованный доступа, и улучшите способность сети к восстановлению.

Решение для NAC Cisco предоставляет следующие деловые преимущества:

- **Соответствие политики безопасности**: Гарантирует, что оконечные точки соответствуют политике безопасности; защищает инфраструктуру и эффективность работы сотрудника; защищает управляемые и неуправляемые активы; поддерживает внутренние среды и гостевой доступ; политика адаптации к вашему уровню риска.
- **Защищает существующие вложения**: совместимо с приложениями для управления стороннего разработчика; гибкие варианты развертывания минимизируют потребность в модернизациях инфраструктуры.
- **Снижает риски от вирусов, червей и неавторизованный доступа**: Управляет и уменьшает крупномасштабные разрушения инфраструктуры; уменьшает эксплуатационные расходы путем создания шагов, добавляет и изменяется динамичный и автоматизированный, который включает более высокую эффективность IT; интегрируется с другими компонентами Cisco SDN для отправки защиты универсальной безопасности.

# Обзор решения

Этот раздел кратко представляет Уровень 3 внеполосные (OOB) методы списка контроля доступа (ACL) использования для реализации системы контроля доступа к сети Cisco NAC (NAC) архитектура.

## Описание решения

NAC Cisco используется в инфраструктуре сети для обеспечивания соблюдения политики безопасности на всех устройствах, которые запрашивают доступ к сетевым ресурсам. NAC Cisco позволяет администраторам сети аутентифицировать и авторизовать пользователей и оценивать и повторно добиваться своих связанных машин, прежде чем им предоставят доступ к сети. Существует несколько методов задания конфигурации, которые можно использовать для выполнения этой задачи, но внеполосный (OOB) Уровень 3 быстро стал одной из самых популярных методологий развертываний для NAC. Это переключается на нижний регистр, популярность основывается на нескольких движущих силах, включая лучшее использование аппаратных ресурсов.

Путем развертывания NAC Cisco в Уровне 3 методология OOB одиночное устройство Cisco NAC (диспетчер Cisco NAC Manager или сервер Cisco NAC) может масштабироваться для размещения большего количества пользователей. Это также позволяет NAC-устройствам быть расположенными в центре, а не распределенным через кампус или организацию. Таким образом Уровень 3 развертывания OOB намного более экономически эффективен и

от капитала и от точки зрения эксплуатационных расходов.

Это руководство описывает основанную на ACL реализацию NAC Cisco в Уровне 3 развертывания OOB.

# Архитектура решения

Архитектура решения (см. рисунок 1) определяет ключевые компоненты данного решения и точки интеграции.

**Рисунок 1: Размещение устройства Cisco NAC в типичной среде комплекса зданий**

Следующие разделы описывают уровень доступа, уровень распределения, магистральный уровень и точки интеграции услуг ЦОД, которые составляют типичную архитектуру кампуса.

## Уровень доступа

Уровень 3 Cisco решение для NAC OOB применим к маршрутизировавшему проекту уровня кампуса доступа. В маршрутизировавшем режиме доступа коммутируемые виртуальные интерфейсы Уровня 3 (SVI) настроены на коммутаторе доступа, и существует ссылка Уровня 3 между доступом и коммутаторами распределения.

**Примечание:** Термин “коммутатор доступа” и “коммутатор Edge” использован взаимозаменяемо в этом документе.

Как замечено на рисунке 2, VLAN доступа Уровня 3 (например, VLAN 14) настроена на коммутаторе Edge, маршрутизация Уровня 3 поддерживается от коммутатора до восходящего коммутатора распределения или маршрутизатора, и диспетчер Cisco NAC Manager управляет портами на коммутаторе доступа.

**Рис. 2: Коммутаторы доступа с уровнем 3 к краю**

## Уровень распределения

Уровень распределения ответственен за маршрутизацию Уровня 3. В отличие от решения для Уровня 2, сервер Cisco NAC не должен быть расположен в уровне распределения. Вместо этого это размещено централизованно в блок сервиса ЦОД.

## Центральный уровень

Магистральный уровень использует Маршрутизаторы на основе IOS Cisco. Магистральный уровень зарезервирован для высокоскоростной маршрутизации без любых сервисов. Сервисы могут быть размещены в сервисный коммутатор в ЦОД.

## Уровень сервисов ЦОД

Уровень сервисов ЦОД использует Маршрутизаторы на основе IOS Cisco и коммутаторы. Диспетчер Cisco NAC Manager и сервер Cisco NAC расположены в центре в блоке сервиса ЦОД.

# Компоненты решения

В этом разделе описываются компоненты решения для устройства Cisco NAC.

### Диспетчер Cisco NAC Manager

Диспетчер Cisco NAC Manager является административным сервером и базой данных, которая централизует конфигурацию и мониторинг всех серверов Cisco NAC, пользователей и политики в развертываниях устройства Cisco NAC. Для развертываний NAC OOB Менеджер предоставляет управление OOB, чтобы добавить и управляющие переключатели в домене Менеджера и настроить порты коммутатора.

### Сервер Cisco NAC

Сервер Cisco NAC является точкой осуществления между недоверяемой (управляемой) сетью и доверяемой (внутренней) сетью. Сервер принуждает полицейских, определенных в диспетчере Cisco NAC Manager, и оконечные точки связываются с Сервером во время аутентификации. В этом дизайне Сервер не размещен логически или “физически встроенный” для разделения недоверяемого и надежной сети. Это понятие обращено более подробно позже во “Внеполосном (OOB) Режиме” раздел.

### Агент Cisco NAC

Агент Cisco NAC является дополнительным компонентом решения для NAC Cisco. Когда Агенту включают для ваших развертываний NAC Cisco, Агент гарантирует, что компьютеры, которые обращаются к вашей сети, удовлетворяют системные требования положения, которые вы задаете. Агент Cisco NAC является простой в использовании, программой маленького места только для чтения, которая находится на пользовательских машинах. Когда пользователь пытается обратиться к сети, Агент проверяет систему клиента для программного обеспечения, которого вы требуете, и помогает пользователям получать любые недостающие обновления или программное обеспечение.

## Внеполосный (OOB) режим

В устройстве Cisco NAC развертывания OOB сервер Cisco NAC связывается с конечным хостом только во время процесса проверки подлинности, оценки положения и исправления. После того, как это будет сертифицироваться, конечный хост не связывается с Сервером. В режиме OOB диспетчер Cisco NAC Manager использует протокол SNMP для управляющих переключателей и присвоений set VLAN для портов. Когда Cisco NAC Manager и сервер NAC установлен для OOB, Менеджер может управлять портами коммутатора поддерживаемых коммутаторов. Для списка поддерживаемых коммутаторов перейдите:

http://www. cisco . com/en/US/docs/security/nac/appliance/support_guide/switch_spt.html#wp40017.

Следующие несколько схем показывают, как диспетчер Cisco NAC Manager использует OOB, чтобы управлять, как пользователь получает доступ к сети. Последовательность следующие:

1. ПК физически связан с коммутатором в сети (см. рисунок 3).
2. Коммутатор передает MAC-адрес с помощью SNMP для диспетчера Cisco NAC Manager (см. рисунок 3).

3. Диспетчер Cisco NAC Manager проверяет, “сертифицируется” ли ПК.Если ПК не сертифицируется, диспетчер Cisco NAC Manager дает коммутатору команду назначать порт коммутатора ПК на опознавательную VLAN (см. рисунок 4). Продолжите шаг 4 посредством шага 6.Если ПК сертифицируется, перейти к шагу 5.
4. ПК связывается с сервером Cisco NAC и проходит аутентификацию, оценку положения и исправление (см. рисунок 4).
5. Сервер Cisco NAC сообщает диспетчеру Cisco NAC Manager, что ПК “сертифицируется” (см. рисунок 5).
6. ПК связан с сетью как надежное устройство.

**Рис. 3: Связь SNMP OOB (1 из 3) Рис. 4: Связь SNMP OOB (2 из 3) Рис. 5: Связь SNMP OOB (3 из 3)**

# Принципы проектирования

Когда вы считаете Уровень 3 развертываниями NAC OOB, необходимо рассмотреть несколько вопросов проектирования. Эти факторы перечислены обсужденные в следующих подразделах, и краткое обсуждение их важности включено.

## Классификация оконечных точек

Несколько факторов способствуют классификации оконечных точек, включая типы устройства и роли пользователя. И тип устройства и роль пользователя влияют на роль оконечной точки.

Возможные типы устройства

- Корпоративные устройства
- Некорпоративные устройства
- Устройства NONPC

Возможные роли пользователя

- Сотрудник
- Подрядчик
- Гости

Первоначально, все оконечные точки назначены на не прошедшую поверку подлинности VLAN. Доступ к другим ролям разрешен после идентичности и процесса положения завершено.

## Роли оконечной точки

Роль каждого типа оконечной точки должна быть первоначально определена. Типичные развертывания кампуса включают несколько ролей, таких как сотрудники, гости, и подрядчики и другие оконечные точки, такие как принтеры, точки беспроводного доступа и IP-камеры. Роли сопоставлены с VLAN коммутатора Edge.

**Примечание:** Неаутентифицированная роль первоначально сопоставляет всех пользователей с не прошедшей поверку подлинности VLAN для новой аутентификации.

## Изоляция роли

Жизненно важно изолировать роли оконечной точки при реализации решения для NAC Cisco. Выберите соответствующий механизм осуществления для обеспечения трафика и изоляции пути для всего трафика, происходящего из машин неавторизованный хоста и не прошедшего поверку подлинности. В Уровне 3 среда OOB, коммутатор Edge Уровня 3 (использующий ACL) действует как точка осуществления, которая гарантирует сегрегацию между “чистыми” и “не прошедшими поверку подлинности” сетями.

## Трафик

Когда оконечная точка соединяется с управляемым коммутатором NAC, процесс NAC начинается. Трафик, классифицированный как “не прошедший поверку подлинности”, ограничен ACL, примененными на не прошедшую поверку подлинности VLAN. Оконечной точке позволяют связаться с “Недоверяемым” интерфейсом сервера Cisco NAC для продолжения через оценку положения и процесс исправления (существует несколько методов для выполнения оценки положения и исправления, которые обсуждены позже в “Политике обновления от Cisco.com на диспетчере Cisco NAC Manager”. раздел). После аутентификации оконечная точка перемещена в доверяемую VLAN.

## Режим сервера Cisco NAC

Сервер Cisco NAC может быть развернут или в действительном шлюзе (мост), режим или РЕАЛЬНЫЙ IP-ШЛЮЗ (маршрутизировали) режим.

### Действительный шлюз (мост) режим

Действительный шлюз (мост), режим, как правило, используется, когда сервером Cisco NAC является Уровень 2, смежный с оконечными точками. В этом режиме Сервер действует как мост и не вовлечен в решение о маршрутизации сетевого трафика.

**Примечание:** Действительный шлюз (мост) режим не применим для Уровня 3 дизайн ACL OOB.

### РЕАЛЬНЫЙ IP-ШЛЮЗ (Направленный) режим

Когда сервер Cisco NAC является множественными переходами далеко от оконечной точки, (маршрутизировавший) режим РЕАЛЬНОГО IP-ШЛЮЗА применим. Когда вы будете использовать Сервер в качестве РЕАЛЬНОГО IP-ШЛЮЗА, задайте IP-адреса его двух интерфейсов: один IP-адрес для доверяемой стороны (для обеспечения управления от диспетчера Cisco NAC Manager) и один IP-адрес для недоверяемой стороны. Два адреса должны быть на других подсетях. IP-адрес ненадежного интерфейса используется для связи с оконечной точкой на недоверяемой подсети. Уровень 3 развертывания OOB с помощью ACL требует, чтобы оконечная точка связалась с ненадежным интерфейсом в целях проверки подлинности и авторизация. Поскольку режим реального IP использует действительный IP - адрес для ненадежного интерфейса, сервер Cisco NAC должен быть настроен для функционирования в режиме РЕАЛЬНОГО IP-ШЛЮЗА.

## Масштабируемость

Стандартный сервер Cisco NAC может управлять до 5000 параллельных конечных пользователей. Уровень 3 дизайн ACL OOB подходит для узла, служащего не больше, чем 5000 пользователей. Если у вас есть множественные узлы, у вас могут быть дополнительные Серверы на узел. Если у вас есть одиночный узел, который должен служить больше чем 5000 пользователей, можно использовать внешние способы распределения нагрузки (например, Балансировщик Загрузки ядра управления приложениями (ACE)) для масштабирования больше чем 5000 пользователей для одиночного узла.

**Примечание:** Первоклассное балансирующее обсуждение загрузки выходит за рамки этого документа.

### Хост обнаружения

Хост Обнаружения является полным доменным именем (FQDN) или IP-адресом ненадежного интерфейса, используемым агентом Cisco NAC, чтобы обнаружить, что сервер Cisco NAC определил местоположение множественных переходов далеко в сети. Агент инициирует процесс обнаружения путем передачи пакетов UDP к известному Адресу узла Обнаружения. Пакеты обнаружения должны достигнуть ненадежного интерфейса Сервера NAC для получения ответа. В случае Уровня 3 развертывания OOB Сервер не находится в пути трафика данных на опознавательной VLAN. Поэтому Параметр хоста Обнаружения должен быть настроен, чтобы быть IP-адресом ненадежного интерфейса сервера Cisco NAC так, чтобы агент мог передать пакеты обнаружения непосредственно к Серверу.

### Пользовательский опыт (с агентом Cisco NAC)

Как правило, администраторы корпоративной сети устанавливают агента Cisco NAC на клиентских компьютерах прежде, чем выполнить те машины пользователям. Адрес IP - адреса хоста Обнаружения или разрешимое название в агенте Cisco NAC инициируют пакеты обнаружения, которые будут передаваться Ненадежному интерфейсу Сервера NAC, который автоматически ведет клиентский компьютер посредством процесса NAC.

### Пользовательский опыт (без агента Cisco NAC)

Оконечные точки без агента Cisco NAC (наиболее вероятные гости, подрядчики и некорпоративное имущество) могут не автоматически продолжиться посредством процесса NAC. Ручные и управляемые методы существуют для помощи оконечным точкам, которые не имеют Агента. Для большего количества подробности см. “Оконечную точку к разделу” Связи сервера Cisco NAC.

**Примечание:** Для лучшей возможной производительности конечного пользователя используйте сертификаты, которым доверяет браузер конечного пользователя. Использование самогенерируемых сертификатов на сервере Cisco NAC не рекомендуется для производственной среды.

## Потоки процессов NAC Cisco

Этот раздел объясняет поток основного процесса для NAC решение OOB. Сценарии описаны и с и без агента Cisco NAC, установленного на клиентском компьютере. Этот раздел показывает, как диспетчер Cisco NAC Manager управляет портами коммутатора с

помощью SNMP в качестве среды контроля. Эти потоки процессов макроаналитичны по своей природе и содержат только функциональные шаги решения. Потоки процессов не включают каждую опцию или шаг, который происходит, и не включайте решения об авторизации, которые основываются на критериях оценки оконечной точки.

См. схему потока процессов, показанную на рисунке 7 для окруженных шагов, показанных на рисунке 6.

**Рис. 6: Поток процессов NAC для уровня 3 внеполосное решение для NAC Рисунок 7: Схема потока процессов**

# Реализация решения NAC Cisco

В Уровне 3 дизайн NAC OOB, который использует ACL, сервер Cisco NAC, ведет функции аутентификации, но Сервер не является точкой принудительной политики в сети. Коммутатор Edge действует как точка осуществления во время аутентификации, карантина и этапов доступа. На основе этого сдвига некоторые дополнительные изменения требуются на коммутаторе Edge.

## Изоляция роли

Для успешных развертываний NAC изоляция оконечных точек важна. После того, как дизайн классификации оконечных точек определен, разрешения между классами должны быть определены. Рекомендованный подход придерживается, на основе рисунка 8.

**Рис. 8: Подход изоляции роли в NAC Cisco решение OOB**

**Примечание:** Интерфейс диспетчера Cisco NAC Manager и доверяемый интерфейс сервера Cisco NAC проиллюстрированы выше на других VLAN. Если Сервер развернут в режиме РЕАЛЬНОГО IP-ШЛЮЗА, Однако эти два интерфейса могут быть на той же VLAN.

Не прошедшая поверку подлинности VLAN требует доступа к этим ресурсам:

- Инфраструктурные услуги, такие как DHCP и DNS
- Серверы проверки подлинности, как правило, контроллер домена для Домена Windows входит до проверки NAC
- Ненадежный интерфейс Сервера NAC
- (Дополнительные) серверы исправления

VLAN сотрудника, как правило, имеет неограниченный доступ ко всем ресурсам, VLAN подрядчика, как правило, имеет ограниченный доступ к подмножеству ресурсов, и гостевой VLAN, как правило, только имеет доступ к Интернету.

## Способ списка доступа

Список доступа (ACL) используется для определения сетевого трафика. После определения трафика с ACL можно сделать множество вещей с трафиком. Например, можно позволить его, запретить его, ограничить его или использовать его для ограничения обновлений маршрута.

В способе ACL ряд ACL применен к каждому новому интерфейсу виртуальной локальной сети (VLAN), который вы создаете на основе своих требований. Команды CLI, данные в следующих подразделах, показывают команды, требуемые настраивать доверяемый и

изоляция пути сети без доверия с помощью ACL VLAN. Выполните процедуру ниже для реализации ACL.

**Примечание:** Добавление VLAN для изоляции роли и ACL настройки на тех VLAN должно быть выполнено на каждом коммутаторе Edge. Эта работа должна быть частью готовности развертываний NAC.

1. Прежде, чем внедрить NAC, исследуйте конфигурацию существующей VLAN.Команды CLI, показанные в следующем тексте, показывают, как VLAN сотрудников, как правило, настраивается, прежде чем NAC внедрен.!
```
int vlan
200description EMPLOYEES_Vlan
ip address 10.100.1.1 255.255.255.0
!
```
2. Настройте дополнительные VLAN.Планирование NAC перед развертываниями требует настройки дополнительных VLAN, и соответствующие ACL применились к интерфейсам виртуальной локальной сети (VLAN). Как пример, следующий текст CLI показывает, как добавить новую VLAN Уровня 3 для каждого из не прошедших поверку подлинности, сотрудников, подрядчиков и ролей guest.!
```
int vlan
100description UNAUTHENTICATED_Vlan
ip address 172.16.1.1 255.255.255.0
!
int vlan
200description EMPLOYEES_Vlan
ip address 10.100.1.1 255.255.255.0
!
int VLAN
210description CONTRACTORS_Vlan
ip address 10.120.1.1 255.255.255.0
!
int vlan
300description GUESTS_Vlan
ip address 192.168.1.1 255.255.255.0
!
```
3. Ограничения внедрения на неаутентифицированную роль.Не прошедшие поверку подлинности устройства в неаутентифицированной роли, как правило, требуют доступа к ресурсам в чистой сети, таким как DNS, DHCP, Active Directory и серверы исправления. Они также требуют доступа к ненадежному интерфейсу сервера Cisco NAC В примере конфигурации ниже, неаутентифицированная роль имеет доступ к ресурсам на 10.10.10.0 / 24 сети и ненадежный интерфейс сервера Cisco NAC.!
```
! this access-list permits traffic destined to devices on 10.10.10.x
! this should be a consistent ACL that can be applied across all L3
switches
!
ip host NAC_SERVER_UNTRUSTED_INTERFACE <IP_Address>
access-list 100 permit ip any host NAC_SERVER_UNTRUSTED_INTERFACE
access-list 100 permit ip any 10.10.10.0 255.255.255.0
!
!
! then apply this access-list to the UNAUTHENTICATED_Vlan
!
int vlan100
description UNAUTHENTICATED_Vlan
ip address 172.16.1.1 255.255.255.0
ip access-group 100 in
!
int vlan200
```

```
description EMPLOYEES_Vlan
ip address 10.100.1.1 255.255.255.0
!
int vlan300
description GUESTS_Vlan
ip address 192.168.1.1 255.255.255.0
!
```

4. Ограничения внедрения на гостевую VLAN.Как правило, роль guest имеет доступ к Интернету только. Весь доступ к ненужным ресурсам, таким как все внутренние сети, должен быть явно запрещен. Единственным исключением может быть внутренний сервер DNS.!

```
! ACL 100 permits traffic destined to devices on 10.10.10.0 / 24
! this should be a consistent ACL that can be applied across all L3
switches
!
access-list 100 permit ip any 10.10.10.0 255.255.255.0
!
!
! ACL 101 for Guests should deny access to all internal networks
! while DNS is permitted
!
access-list 101 permit udp any host GUEST_DNS_SERVER eq 53
access-list 101 deny ip any 10.0.0.0 255.0.0.0
access-list 101 deny ip any 192.168.0.0 255.255.0.0
access-list 101 deny ip any 172.16.0.0 255.240.0.0
access-list 101 permit ip any any
!
int VLAN100
description UNAUTHENTICATED_VLAN
ip address 172.16.1.1 255.255.255.0
ip access-group 100 in
!
int VLAN200
description EMPLOYEES_VLAN
ip address 10.100.1.1 255.255.255.0
!
!
int VLAN300
description GUESTS_VLAN
ip address 192.168.1.1 255.255.255.0
ip access-group 101 in
!
```

## Оконечная точка к связи сервера Cisco NAC

Сервер Cisco NAC добирается, MAC - информация или от агента Cisco NAC или от веб-страницы для входа включил для ActiveX или приложения Java, чтобы определить MAC - адрес устройства и сообщить его к диспетчеру Cisco NAC Manager.

### Агент Cisco NAC

Агент Cisco NAC должен связаться с ненадежным интерфейсом Сервера NAC для инициирования процесса регистрации в системе. Агент пытается обнаружить Сервер на основе известного значения Хоста Обнаружения. Как показано на рисунке 9, значение Хоста Обнаружения в агенте Cisco (nacs.nac.local) указывает к ненадежному интерфейсу (172.23.117.57) на Сервере NAC. Рисунок 9 показывает комбинацию трех экранов.

Посмотрите, что входит “Агент”. раздел для получения дополнительной информации по

регистрации через агента Cisco NAC.

**Рис. 9: Хост обнаружения, указывающий на ненадежный интерфейс сервера NAC**

**Примечание:** Если Агент не в состоянии получить какой-либо ответ назад от сервера Cisco NAC, агент Cisco NAC не появляется.

### Веб-вход в систему

Веб-вход в систему, как правило, требуется для гостевых сеансов регистрации. Когда метод изоляции ACL используется, ненадежный интерфейс Сервера NAC не находится непосредственно в пути трафика данных. Когда браузер сначала открыт, Поэтому пользователь автоматически не перенаправлен к странице входа. Две опции могут позволить конечному хосту получить страницу входа.

Вариант 1

- Создайте гостевой URL входа в систему, известный пользователям (например, гость. cisco . com).
- Гость должен тогда открыть браузер и ввести тот URL, который вызывает перенаправление к странице входа.

Вариант 2

- Создайте фиктивный сервер DNS для не прошедшей поверку подлинности пользовательской подсети.
- Этот фиктивный сервер DNS решает каждый URL к ненадежному интерфейсу сервера Cisco NAC.
- Когда гость открывает браузер, независимо от которого URL он пытается достигнуть, он перенаправлен к странице входа.
- Когда пользователь тогда перемещен в соответствующую VLAN для его роли, он получает новое присвоение Адреса DNS, когда выполнение IP освобождает или возобновляет на успешной регистрации в системе.

В Уровне 3 дизайн OOB пользователи, которые входят в использование веб-страницы, загружают и выполняют любого элемент управления ActiveX (для браузеров Internet Explorer) или приложение Java (для браузеров неIE). Элемент управления ActiveX (или Java) должен работать для выполнения придерживающегося:

- Соберите MAC-адрес хоста, который, как сообщают, серверу Cisco NAC и диспетчеру Cisco NAC Manager предоставляет сопоставление MAC-адреса и IP-адрес.
- Выполните выпуск IP и возобновите клиента оконечной точки.

**Примечание:** Решение позволить гостям использовать внутренний или внешний DNS является решением о применении политики, которое должна сделать каждая организация. Использование общего сервиса DNS представляет наименее потенциальную угрозу в этом подходе.

Посмотрите веб-вход в систему, для получения дополнительной информации при регистрации через веб-страницу.

## Уровень 3 NAC пример конфигурации списков управления доступом (ACL) OOB

Для успешного развертывания NAC решение OOB компоненты NAC должны быть настроены для соответствия с желаемой архитектурой. Рисунок 10 показывает NAC Уровня 3 логическую схему сети OOB, которая используется в этом разделе для иллюстрирования соответствующей конфигурации диспетчера Cisco NAC Manager, сервера Cisco NAC и коммутатора Edge для Уровня 3 NAC развертывания OOB с помощью ACL.

**Рис. 10: Уровень 3 NAC схема логической топологии OOB**

Для настройки реального IP Уровня 3 развертывания NAC OOB выполните эти действия:

1. Настройте коммутатор Edge для осуществления.Во-первых, создайте три дополнительных VLAN (НЕ ПРОШЕДШИЙ ПОВЕРКУ ПОДЛИННОСТИ, CONTRACTORS и ГОСТИ) на коммутаторе Edge. Существующая производственная VLAN будет использоваться для сотрудников.Настройте и примените ACL на каждую VLAN для ограничения доступа к сетевому на назначенной роли.Неаутентифицированная роль: VLAN 17 и название ACL: UNAUTH_ACL`! Create SVI for Un-auth VLAN`

   ```
   Edge Switch(config)#interface vlan 17
   Edge Switch (config)#ip address 192.168.7.1 255.255.255.0
   Edge Switch (config)#ip helper-address 192.168.3.10
   ! 192.168.3.10 is the dhcp server (see Figure 10)

   ! Configure ACL for Un-auth Role
   Edge Switch(conf)#ip access-list extended UNAUTH_ACL
      remark Allow Discovery packets from Agent to NAC Server
      permit udp any host 192.168.8.10 eq 8906
      remark Allow Discovery packets from Agent to NAC Server for ADSSO
      permit udp any host 192.168.8.10 eq 8910
      remark Allow Web traffic from PC to NAC Server
      permit tcp any host 192.168.8.10 eq www
      remark Allow SSL traffic from PC to NAC Server
      permit tcp any host 192.168.8.10 eq 443
      remark Allow DHCP permit udp any any eq bootpc
      permit udp any any eq bootps
      remark Allow DNS
      permit udp any any eq domain
      remark Allow Web traffic to the Remediation Server
      permit tcp any host 192.168.3.10 eq www

   ! Apply ACL for Un-auth VLAN Interface

   Edge Switch(config)#interface vlan 17
   Edge Switch(config)# ip access-group UNAUTH_ACL in
   ```

   Роль подрядчика: VLAN 77 и название ACL: CONTRACTOR_ACL`! Create SVI for Contractor VLAN`

   ```
   Edge Switch(config)#interface vlan 77
   Edge Switch (config)#ip address 192.168.77.1 255.255.255.0
   Edge Switch (config)#ip helper-address 192.168.3.10

   ! Configure ACL for Contractor Role

   Edge Switch(conf)#ip access-list extended CONTRACTOR_ACL
      remark Allow DHCP permit udp any any eq bootpc
      permit udp any any eq bootps
      remark Allow DNS
      permit udp any any eq domain
      remark Allow traffic to DMZ Subnet
      permit ip any 192.168.3.0 0.0.0.255
      remark deny rest of the internal resources
      deny ip any 10.0.0.0 255.0.0.0
   ```

```
   deny ip any 192.168.0.0 255.255.0.0
   deny ip any 172.16.0.0 255.240.0.0
   remark permit internet
   permit ip any any

! Apply ACL for Contractor VLAN Interface

Edge Switch(config)#interface vlan 77
Edge Switch(config)# ip access-group CONTRACTOR_ACL in
```
Роль guest: VLAN 78 и название ACL: GUEST_ACL
```
! Create SVI for GUEST VLAN

Edge Switch(config)#interface vlan 78
Edge Switch (config)#ip address 192.168.78.1 255.255.255.0
Edge Switch (config)#ip helper-address 192.168.3.10

! Configure ACL for Guest Role

Edge Switch(conf)#ip access-list extended GUEST_ACL
   remark Allow DHCP
   permit udp any any eq bootpc
   permit udp any any eq bootps
   remark Allow DNS
   permit udp any any eq domain
   remark deny access to the internal resources
   deny ip any 10.0.0.0 255.0.0.0
   deny ip any 192.168.0.0 255.255.0.0
   deny ip any 172.16.0.0 255.240.0.0
   remark permit internet
   permit ip any any

! Apply ACL for GUEST VLAN Interface

Edge Switch(config)#interface vlan 78
Edge Switch(config)# ip access-group GUEST_ACL in
```
Роль сотрудника: VLAN 14 и ACL: Production_ACLСуществующая производственная VLAN может использоваться для перемещения сотрудника от не прошедшей поверку подлинности VLAN до VLAN сотрудника. После того, как конечный клиент перемещен в эту VLAN, агент Cisco NAC все еще пытается обнаружить сервер Cisco NAC. Агент разработан для поведения этого пути. Если Агент в состоянии достигнуть Сервера, Агент появляется и пытается выполнить процесс регистрации в системе снова, даже при том, что машина уже предоставила доступ. Очевидно, это - нежелательное поведение, и администраторы должны гарантировать, что отброшен UDP 8906 пакетов обнаружения, происходящих от Агента. Employee_ACL настроен для отбрасывания этих пакетов обнаружения.
```
! Use Existing Production Layer 3 VLAN for Employees

Edge Switch(config)#interface vlan 14
Edge Switch (config)#ip helper-address 192.168.3.10

! Configure ACL to prevent discovery packets from reaching the
untrusted interface on the NAC Server

Edge Switch(conf)#ip access-list extended Employee_ACL
   remark Deny Discovery packets from Agent to NAC Server
   deny udp any host 192.168.8.10 eq 8906
   permit ip any any

! Apply ACL for Employee VLAN Interface

Edge Switch(config)#interface vlan 14
Edge Switch(config)# ip access-group Employee_ACL in
```

2. Выполните начальную настройку Cisco NAC Manager и сервера NAC.Установка Cisco NAC Manager и сервера NAC выполнена через консольный доступ. Утилита установки ведет вас через начальную конфигурацию и для Менеджера и для Сервера. Для выполнения начальной настройки перейдите:http://www. cisco . com/en/US/docs/security/nac/appliance/installation_guide/hardware/47/hi_instal.html
3. Примените лицензию на диспетчера Cisco NAC Manager.После того, как вы выполняете начальную настройку через консоль, обращаетесь к GUI диспетчера Cisco NAC Manager, чтобы продолжить настраивать Cisco NAC Manager и сервер NAC. Сначала загрузите Менеджера и Серверные лицензии, которые шли с устройствами. Для большего количества подробности о загрузке лицензий перейдите:http://www. cisco . com/en/US/docs/security/nac/appliance/installation_guide/hardware/47/hi_instal.html#wp1113597**Примечание:** Все лицензии Cisco NAC Manager и сервера NAC основываются на MAC-адресе eth0 Менеджера. В настройке аварийного переключения лицензии основываются на MAC-адресе eth0 и основных и вторичных диспетчеров Cisco NAC Manager.
4. Политика обновления от Cisco.com на диспетчере Cisco NAC Manager.Диспетчер Cisco NAC Manager должен быть настроен для получения периодических обновлений из центрального сервера обновления, расположенного в Cisco. Устройство Cisco NAC Поддерживаемый Список продуктов AV/AS является имеющим версию XML-файлом, распределенным от централизованного сервера обновления, который предоставляет актуальнейшую матрицу поддерживаемого антивируса и поставщиков антишпиона и версий продукта, использовало настраивать антивирус или правила антишпиона и антивирус или требования обновления определения антишпиона для оценки положения и исправления. Этот список регулярно обновляется для антивируса и продуктов антишпиона, и версии, поддерживаемые в каждом агенте Cisco NAC, освобождают, и включает новые продукты для новых Версий агента. Обратите внимание на то, что список предоставляет сведения о версии только. Когда диспетчер Cisco NAC Manager загружает поддерживаемый антивирус и список продуктов антишпиона, это загружает информацию о том, что последние версии для продуктов антишпиона и антивируса; это не загружает фактические файлы исправления или файлы определения вируса. На основе этой информации Агент может тогда инициировать собственный антивирус или приложение антишпиона для выполнения обновлений. Для получения дополнительной информации о том, как обновления получены, перейдите:http://www. cisco . com/en/US/docs/security/nac/appliance/configuration_guide/47/cam/m_agntd.html#wp1351880
5. Установите сертификаты от стороннего центра сертификации (CA).Во время установки, сценария служебной программы конфигурации и для диспетчера Cisco NAC Manager и для сервера Cisco NAC требует, чтобы вы генерировали временный сертификат SSL. Для лабораторной среды можно продолжить использовать подписанные сертификаты; однако, им не рекомендуют для рабочей сети.Для получения дополнительной информации об установке сертификатов на диспетчере Cisco NAC Manager от независимого поставщика CA, перейдите:http://www. cisco . com/en/US/docs/security/nac/appliance/configuration_guide/47/cam/m_admin.html#wp1078189Для получения дополнительной информации об установке сертификатов на сервере Cisco NAC от независимого поставщика CA, перейдите:http://www. cisco . com/en/US/docs/security/nac/appliance/configuration_guide/47/cas/s_admin.html#wp104011

1**Примечание:** При использовании самоподписывать сертификаты в лабораторной среде, диспетчере Cisco NAC Manager и сервере Cisco NAC каждая потребность доверять сертификату другого, который требует, чтобы вы загрузили сертификаты для обоих как Доверенный центр сертификации под SSL> Доверенные центры сертификации.

6. Добавьте сервер Cisco NAC к диспетчеру Cisco NAC Manager.Чтобы добавить Сервер NAC к Менеджеру NAC, выполните эти действия:Нажмите **CCA Servers** под областью Device Management (см. рисунок 11).Нажмите **Новую вкладку Server**.Используйте коробку *IP-адреса сервера* для добавления IP-адреса Доверяемого интерфейса Сервера NAC.В коробке *Расположения сервера* введите **Сервер NAC OOB** как расположение сервера.Выберите **Out-of-Band Real-IP Gateway** из выпадающего списка *Server Type*.**Нажмите Add чистый сервер доступа**.**Рис. 1-1: Добавление сервера Cisco NAC к диспетчеру Cisco NAC Manager** После добавления сервера Cisco NAC это появляется в списке под вкладкой List of Servers (см. рисунок 12).**Примечание:** Диспетчер Cisco NAC Manager и сервер Cisco NAC должны доверять центру сертификации (CA) друг друга для Менеджера для успешного добавления Сервера.
7. Настройте сервер Cisco NAC.Как показано на рисунке 12, нажмите вкладку **List of Servers**.Нажмите значок **Manage** (кружился) для сервера Cisco NAC для продолжения конфигурации.**Рисунок 12: Сервер Cisco NAC, управляемый диспетчером Cisco NAC Manager** После нажатия значка Manage экран, показанный на рисунке 13, появляется.
8. Включите поддержку Уровня 3.Нажмите вкладку **Network** (рисунок 13).Проверьте флажок **Enable L3 Support**.Проверьте **Разрешать L3 строгий режим для блокирования устройств NAT с Чистым флажком Agent Доступа**.**Нажмите кнопку Update (Обновить).**Перезагрузите сервер Cisco NAC, как проинструктировано.**Рисунок 13: Подробные данные сети сервера Cisco NAC Примечание:** Всегда генерируйте сертификат для сервера Cisco NAC с IP-адресом его Ненадежного интерфейса. Для сертификата name-based название должно решить к IP-адресу ненадежного интерфейса. Когда оконечная точка свяжется с ненадежным интерфейсом Сервера для начала процесса NAC, Сервер перенаправит пользователя к имени хоста сертификата или IP. Если точки сертификата к доверяемому интерфейсу, процесс регистрации в системе не будет функционировать правильно.На рисунке 13 выше, вы видите, что присутствуют эти два шлюза по умолчанию. Только шлюз по умолчанию, настроенный на доверяемом интерфейсе, применим. Значение на ненадежном интерфейсе не используется для передачи трафика. Трафик, который передан от ненадежного интерфейса, зависит от статического маршрута, покрытого следующим шагом.
9. Настройте статические маршруты.После перезагрузок сервера Cisco NAC возвратитесь к Серверу и продолжите конфигурацию.Сервер должен использовать ненадежный интерфейс для передачи с оконечными точками на не прошедшей поверку подлинности VLAN.Перейдите **Усовершенствованный> Статические маршруты** (см. рисунок 14) добавить маршруты к не прошедшей поверку подлинности VLAN.Заполните соответствующие подсети для не прошедших поверку подлинности VLAN.**Нажмите Add маршрут**.Выберите **Ненадежный интерфейс [eth1]** для этих маршрутов.**Рисунок 14: Добавление статического маршрута для достижения не прошедшей поверку подлинности пользовательской подсети**
10. Установите профили для коммутаторов в диспетчере Cisco NAC Manager.Выберите **OOB Management> Profiles> Device> Edit** (см. рисунок 15).Заполните информацию о

Профиле устройства, с помощью примера в качестве руководства.Каждый коммутатор будет привязан к профилю. Добавьте профиль для каждого типа коммутатора Edge, которым будет управлять диспетчер Cisco NAC Manager. Менеджер поддерживает SNMPv1, SNMPv2c и SNMPv3. Данный пример покрывает SNMPv1 только. Можно хотеть настроить SNMPv2 или SNMPv3c для более безопасной связи SNMP между Менеджером и коммутатором.**Рисунок 15: Профиль SNMP, используемый для управления коммутатором**Установите конфигурацию коммутатора для SNMP.Коммутатор Edge должен быть настроен для тех же строк имени и пароля чтения-записи SNMP как настроенные на диспетчере Cisco NAC Manager. Посмотрите команды CLI ниже.`3560-remote(config)#snmp-server community cisco123 RO`

`3560-remote(config)#snmp-server community cisco321 RW`Выберите **OOB Management> Profiles> Port> New** (см. рисунок 16).Для контроля за отдельным портом настройте профиль порта под **менеджментом OOB> Профили> порт**, который включает не прошедшую поверку подлинности VLAN по умолчанию и VLAN доступа по умолчанию. В разделе VLAN доступа укажите, что выпадает VLAN Роли пользователя с помощью **VLAN Доступа**. Диспетчер Cisco NAC Manager изменяет не прошедшую поверку подлинности VLAN на VLAN доступа на основе VLAN, определенной в роли, где принадлежит пользователь.Определите профиль порта для управления VLAN порта, основанной на ролях пользователя и внедренных VLAN.Подлинная VLAN является НЕ ПРОШЕДШЕЙ ПОВЕРКУ ПОДЛИННОСТИ VLAN (VLAN 17), на который первоначально назначены не прошедшие поверку подлинности устройства.VLAN Доступа По умолчанию является VLAN EMPLOYEES (VLAN 14). Если проверенному пользователю не определили основанную на роли VLAN, эта VLAN используется.VLAN Доступа может отвергнуть виртуальную локальную сеть (VLAN) по умолчанию к VLAN роли пользователя, которая определена под ролью пользователя (для получения дополнительной информации об устанавливании ролей пользователя, посмотрите, “Настраивают роли пользователя”. раздел). Сопоставления LDAP могут использоваться для сопоставления ролей пользователя в NAC группам LDAP. Для получения дополнительной информации перейдите:http://www. cisco . com/en/US/products/ps6128/products_tech_note09186a0080846d7a.shtml**Рисунок 16: Профиль порта для управления портом коммутатора Примечание:** Можно также определить названия VLAN вместо ID. При определении названий VLAN у вас могут быть другие ИДЕНТИФИКАТОРЫ VLAN на других коммутаторах через кампус, но то же название VLAN, подключенное к специальной роли.Дополнительные параметры доступны под профилем порта для IP, освобождают и возобновляют опции. Прокрутите вниз страницу, которая, как показывают на рисунке 16, видела эти опции.Если пользователь находится позади IP-телефона, снимите флажок с Сильным ударом порт после того, как VLAN является измененным флажком (см. рисунок 17), который, если проверено, мог бы перезагрузить IP-телефон, когда возвращен порт.**Рисунок 17: Различные варианты, доступные под портом профиль**

11. Настройте параметры настройки получателя SNMP.В дополнение к устанавливанию Строки имени и пароля SNMP для чтения или записи, необходимо также настроить диспетчера Cisco NAC Manager для получения trap-сообщений SNMP от коммутатора. Когда пользователь подключает и разъединяет от порта, эти trap-сообщения передаются. Когда сервер Cisco NAC передает адресную информацию MAC/IP конкретной оконечной точки Менеджеру, Менеджер создает таблицу соответствий

внутренне для MAC/IP и порта коммутатора.**Примечание:** Вы должны настроить все коммутаторы для передачи trap-сообщений или сообщаете диспетчеру Cisco NAC Manager с помощью строк имени и пароля, определенных на рисунке 18.Выберите **OOB Management> Profiles> SNMP Receiver** (см. рисунок 18).Настройте параметры настройки trap-сообщения SNMP с помощью экрана на рисунке 18 как руководство.**Рисунок 18: Менеджер NAC значение получателя SNMP для сбора trap-сообщений SNMP и сообщает**Для настройки параметров коммутатора для trap-сообщений SNMP увеличьте таймер сброса Clean Access Manager (CAM) стандартного коммутатора до 1 часа (3600 в коробке CLI ниже) на рекомендации по оптимальному использованию Cisco для NAC OOB. Выборка CLI показывает набор параметров mac-address-table aging-time 3600.Установка таймера к 1 часу уменьшает частоту уведомлений MAC, передаваемых из уже присоединенных устройств диспетчеру Cisco NAC Manager. Используйте команду source trap для определения адреса источника, который используется для отсылки trap-сообщений.`snmp-server enable traps mac-notification`
`snmp-server host 192.168.2.33 informs NacTraps`
`snmp-server trap-source Vlan 2`
`mac-address-table aging-time 3600`Дополнительно, настройте установление соединения и ловушки нисходящего канала для передачи к диспетчеру Cisco NAC Manager (не показанный в выборке CLI). Эти trap-сообщения используются только в сценарии развертывания, где конечные хосты НЕ связаны позади IP-телефона.**Примечание:** Infrom-сообщения SNMP рекомендуются, потому что они более надежны, чем trap-сообщения SNMP. Кроме того, рассмотрите QoS для SNMP в сетевой среде большого объема трафика.
12. Добавьте коммутаторы как устройства в диспетчере Cisco NAC Manager.Выберите **OOB Management> Devices> Devices> New** (см. рисунок 19).Профиль коммутатора, созданный в Шаге 10, будет использоваться для добавления коммутатора.Под Профилем устройства используйте профиль, который вы создали, но не изменяйте значение Профиля Порта по умолчанию, когда вы добавляете коммутатор.**Примечание:** Для Профиля Порта по умолчанию всегда выбирайте “неуправляемый”, потому что вы никогда не управляете всеми портами коммутатора доступа. Минимум одного порта каскадного соединения должен быть неуправляемым. Поэтому необходимо добавить, что коммутатор с неуправляемым портом представляет и затем выбирает порты, которым нужно управлять.**Рисунок 19: Добавление коммутатора Edge в диспетчере Cisco NAC Manager для управления Использованием SNMP**После того, как коммутатор добавлен к диспетчеру Cisco NAC Manager, выберите порты, которыми вы хотите управлять.
13. Настройте порты коммутатора для устройств, которые будут управляемы NAC.Выберите **OOB Management> Devices Switch [IP address]> Ports> List** для наблюдения доступных портов коммутатора, которыми можно управлять (см. рисунок 20).**Рис. 20: Выбор управления портами, доступный для управляемого коммутатора**Выберите **OOB Management> Devices Switch [IP address]> Ports> Manage** для управления несколькими портами сразу (см. рисунок 21).**Рис. 21: Управление множественными портами с опцией соединения**
14. Настройте роли пользователя.В данном примере созданы три дополнительных роли. VLAN уже создали в краю, который каждый соответствует роли.Выберите **User Management> User Roles> Edit Role** и создайте роль сотрудника с помощью рисунка 22 в качестве руководства.**Рисунок 22: Создание Роли Сотрудника и Сопоставление с**

производством VLAN 14Выберите **User Management> User Roles> Edit Role** и создайте роль подрядчика с помощью рисунка 23 в качестве руководства.**Рисунок 23: Создание Роли Подрядчика и Сопоставление его к ограниченному доступу VLAN 77**Выберите **User Management> User Roles> Edit Role** и создайте роль guest с помощью рисунка 24 в качестве руководства.**Рисунок 24: Создание Роли guest и Сопоставление его к Интернету Только VLAN** Всего, необходимо видеть шесть ролей, созданных в этом разделе (три роли по умолчанию и три новых роли), как показано на рисунке 25.**Рисунок 25: Добавление ролей в менеджере NAC**

15. Добавьте пользователей и назначьте на соответствующую роль пользователя.В среде комплекса зданий вы будете интегрироваться с внешним сервером проверки подлинности и сопоставлять пользователя со специальной ролью посредством атрибута LDAP. Данный пример использует локального пользователя и партнеров что локальный пользователь с ролью.
16. Настройте страницу регистрационной информации пользователя для входа для веб-входа в систему.Страница для входа по умолчанию уже создана в диспетчере Cisco NAC Manager. Можно дополнительно настроить страницу входа для изменения появления веб-портала. Для Уровня 3 NAC решение OOB, ActiveX или Компонент Java должны быть загружены до конца клиент для выполнения следующих задач:Выберите MAC-адрес клиентского компьютера.Выполните выпуск IP-адреса и возобновите.Выберите **Administration> User Pages** (см. рисунок 26).Отредактируйте страницу для создания, включают варианты, показавшие на рисунке 26.**Рисунок 26: Параметры настройки страницы пользователя для веб-входа в систему**
17. Настройте агента Cisco NAC для ролей пользователя.Выберите **Device Management> Clean Access> General Setup> Agent Login** (см. рисунок 27).Диспетчер Cisco NAC Manager может быть настроен для создания Агента обязательным для любой роли пользователя. В данном примере Агент является обязательным для роли сотрудника. Подрядчик и роли guest должны использовать веб-вход в систему.Проверьте **Потребовать использование флажка Agent**.**Рисунок 27: Вход в систему агента, требуемый для роли сотрудника**
18. Распределите хост обнаружения к агенту Cisco NAC.Распространение программного обеспечения агента Cisco NAC, установка и конфигурация охвачены в Приложении в “устройстве Cisco NAC Настройки для Входа в систему Агента и Клиентского раздела” Оценки Положения. Данный пример настраивает хост обнаружения на диспетчере Cisco NAC Manager.Выберите **Device Management> Clean Access> Clean Access Agent> Installation** (см. рисунок 28).**Схема 28: Хост обнаружения к агенту Cisco NAC** Если агент Cisco NAC загружен от сервера Cisco NAC, поле Host Обнаружения предварительно заполнено как показано на рисунке 28.
19. Веб-вход в систему.Подключите клиентский компьютер с помощью одного из портов Edge, управляемых диспетчером Cisco NAC Manager.Клиентский компьютер размещен в не прошедшую поверку подлинности VLAN. Машина должна получить IP-адрес от не прошедшей поверку подлинности подсети VLAN.Откройте браузер для выполнения входа в систему.Предположение - то, что этому клиентскому компьютеру не установили агента Cisco NAC уже. Если все Записи DNS перенаправляются к ненадежному интерфейсу сервера Cisco NAC, браузер должен быть перенаправлен к странице входа автоматически. В противном случае перейдите к определенному URL (например, guest.nac.local) для выполнения входа в систему (рисунок 29).**Рис. 29: Веб-страница для входа**
20. Вход в систему агента.Агент Cisco NAC может быть распределен точно так же, как

любое другое программное приложение конечным пользователям или он может быть вызван с помощью сервера Cisco NAC.**Примечание:** Более подробная информация о Распределении агента и установке доступна в *устройстве Cisco NAC - Чистят Руководство по конфигурации Access Manager*.Когда агент активирован, экран, показанный на рисунке 30, появляется.**Рисунок 30: Вход в систему агента** Выберите сервер из **выпадающего списка Server**.**Ввести имя пользователя.Ввести пароль.Щелкните "Регистрация в системе".**Экран на рисунке 31 кажется, придерживавшимся вскоре рисунком 32.**Рисунок 31: агент Cisco NAC, выполняющий IP, освобождает и возобновляет Рис. 32: Агент Cisco NAC, указывающий на полный доступ к сети после обновления IPНажмите кнопку OK.**

# Проверьте назначение VLAN

Управляемый порт для данного примера является 0/7. После успешного завершения процесса регистрации в системе VLAN изменена от не прошедшего поверку подлинности VLAN 14 до сотрудника VLAN 17. Можно подтвердить, какой порт выполняет конфигурацию с помощью следующей команды:

```
3560-remote#show run interface fast 0/7
Building configuration…

Current configuration : 153 bytes
!
interface FastEthernet0/7
 switchport access VLAN 14
 switchport mode access
 snmp trap mac-notification change added
 spanning-tree portfast
end
```

# Уровень 3 NAC решение для ACL OOB для беспроводных сетей

Существующий NAC беспроводное решение OOB в настоящее время ограничивается Уровнем 2 решение OOB с сервером Cisco NAC в режиме виртуального шлюза. Ограничение того решения - то, что контроллером беспроводной локальной сети (WLC) должен быть Уровень 2, смежный с сервером Cisco NAC. Для получения дополнительной информации об Уровне 2 развертывания радио OOB, перейдите:

http://www. cisco . com/en/US/products/ps6128/products_configuration_example09186a0080a138cc.shtml

**Примечание:** В настоящее время Cisco работает на Уровень 3 NAC решение для ACL OOB для беспроводных развертываний.

# Приложение

## Режим высокой доступности

Каждый из отдельных диспетчеров Cisco NAC Manager и серверов Cisco NAC в решении может быть настроен в режиме высокой доступности, означая, что существует два

устройства, которые действуют в активно-резервной конфигурации.

## Менеджер NAC

Диспетчер Cisco NAC Manager может быть настроен в режиме высокой доступности, где существует два Менеджера NAC, которые действуют в активно-резервной конфигурации. Полная конфигурация на Менеджере сохранена в базе данных. Резервный Менеджер синхронизирует его базу данных с базой данных по активному Менеджеру. Любые изменения конфигурации, сделанные активному Менеджеру, сразу выдвинуты резервному Менеджеру. Следующие ключевые точки предоставляют высокоуровневую сводку Менеджера высокой доступности операция:

- Режим высокой доступности диспетчера Cisco NAC Manager является активной или пассивной двумя конфигурациями сервера, в которых резервный Менеджер действует как резервная копия активному Менеджеру.
- Активный диспетчер Cisco NAC Manager выполняет все задачи для системы. Резервный Менеджер контролирует активного Менеджера и поддерживает, его база данных синхронизировалась с базой данных активного Менеджера.
- Оба диспетчера Cisco NAC Manager совместно используют действительного сервисного IP для интерфейса Eth0, которому доверяют. Сервисный IP должен использоваться для сертификата SSL.
- Основные и вторичные диспетчера Cisco NAC Manager обмениваются тактовыми контрольными пакетами UDP каждые 2 секунды. Если таймер пульса истекает, перехват управления при отказе с синхронизацией состояния происходит.
- Гарантировать активного диспетчера Cisco NAC Manager всегда доступно, его доверяемый интерфейс (Eth0) должен быть подключен. Ситуации нужно избежать, где Менеджер активен, но не доступен через ее доверяемый интерфейс. Это условие происходит, если резервный Менеджер получает тактовые контрольные пакеты от активного Менеджера, но сбоев интерфейса Eth0 активного Менеджера). Ссылка - обнаруживает механизм, позволяет резервному Менеджеру знать, когда интерфейс Eth0 активного Менеджера становится недоступным.
- Можно выбрать к, “автоматически настраивают” интерфейс Eth1 на странице Administration> CCA Manager> Failover. Однако необходимо вручную настроить другой (Eth2 или Eth3) интерфейсы высокой доступности с IP-адресом и маской подсети перед настройкой высокой доступности на диспетчере Cisco NAC Manager.
- Eth0, Eth1 и интерфейсы Eth2/Eth3 могут использоваться для тактовых контрольных пакетов и синхронизации базы данных. Кроме того, любой доступный сериал (COM) интерфейс может также использоваться для тактовых контрольных пакетов. При использовании нескольких из этих интерфейсов аварийное переключение происходит, только если все биение взаимодействует сбой.

**Примечание:** Пара высокой доступности диспетчера Cisco NAC Manager не может быть разделена ссылкой Уровня 3.

Для получения дополнительной информации обратитесь к документации диспетчера Cisco NAC Manager в:

http://www. cisco . com/en/US/docs/security/nac/appliance/installation_guide/hardware/47/hi_ha.html

## Сервер Cisco NAC

Для обеспечивания защиты против единственного уязвимого звена сервер Cisco NAC может быть настроен в режиме высокой доступности. Режим высокой доступности для сервера Cisco NAC подобен тому из диспетчера Cisco NAC Manager и также использует активно-резервную конфигурацию. Серверы Cisco NAC все еще совместно используют виртуальный IP - адрес (названный Сервисным IP), но они не совместно используют виртуальные MAC - адреса.

Следующие ключевые точки предоставляют общий обзор операции сервера Cisco NAC высокой доступности:

- Режим высокой доступности сервера Cisco NAC является активно-пассивной двумя конфигурациями сервера, в которых резервная машина сервера Cisco NAC действует как резервная копия к активному серверу Cisco NAC.
- Активный сервер Cisco NAC выполняет все задачи для системы. Поскольку большая часть Конфигурации сервера сохранена на диспетчере Cisco NAC Manager, когда аварийное переключение Сервера происходит, Менеджер выдвигает конфигурацию к недавно-активному-серверу.
- Резервный сервер Cisco NAC не передает пакетов между своими интерфейсами.
- Резервный сервер Cisco NAC контролирует состояние активного сервера через интерфейс биения (последовательный и один или несколько интерфейсов UDP). Тактовые контрольные пакеты могут быть переданы на последовательном интерфейсе, специализированном интерфейсе Eth2, специализированном интерфейсе Eth3 или интерфейсе Eth0/Eth1 (если интерфейс № Eth2 или Eth3 доступен).
- Основные и вторичные серверы Cisco NAC обмениваются тактовыми контрольными пакетами UDP каждые две секунды. Если таймер пульса истекает, перехват управления при отказе с синхронизацией состояния происходит.
- В дополнение к основанному на биении аварийному переключению сервер Cisco NAC также предоставляет основанное на ссылке аварийное переключение на основе отказа соединения Eth0 или Eth1. Сервер передает пакеты Функции проверки связности ICMP ping к внешнему IP - адресу через интерфейс Eth0 и/или Eth1. Аварийное переключение происходит, только если один сервер Cisco NAC может пропинговать внешние адреса.

Для получения дополнительной информации обратитесь к документации сервера Cisco NAC в:

http://www. cisco . com/en/US/docs/security/nac/appliance/installation_guide/hardware/47/hi_ha.html

## Active Directory SingleSignOn (SSO Active Directory)

SSO Active Directory Windows является способностью к устройству Cisco NAC для автоматической регистрации в пользователей, уже аутентифицируемых на Контроллере домена Kerberos бэкэнда (Сервер Active Directory). Эта способность избавляет от необходимости входить в сервер Cisco NAC после того, как вы будете уже зарегистрированы в домен. Для получения дополнительной информации о настройке SSO Active Directory на устройстве Cisco NAC, перейдите:

http://www. cisco . com/en/US/docs/security/nac/appliance/configuration_guide/47/cas/s_adsso.html

## Факторы среды домена Windows

При подготовке к развертываниям NAC могут требоваться изменения к политике сценария регистрации. Сценарии регистрации Windows могут быть классифицированы как запуск или завершение и сценарии входа в систему или выхода из системы. Windows выполняет запуск и сценарии завершения в “контексте машины”. Выполнение сценариев только функционирует, если устройство Cisco NAC открывает соответствующие сетевые ресурсы, требуемые сценарием для специальной роли, когда эти сценарии выполняются в ПК, загружаются или завершают работу, который, как правило, является неаутентифицированной ролью. Войдите в систему и выйдите из системы, сценарии выполняются в “пользовательском контексте”, что означает, что сценарий входа в систему выполняется после того, как пользователь вошел через Windows GINA. Сценарий входа в систему может быть не в состоянии выполняться, если оценка положения аутентификации или клиентского компьютера не завершает, и доступ к сети не предоставляют вовремя. Эти сценарии могут также быть прерваны обновлением IP-адреса, инициируемым агентом Cisco NAC после события входа в систему OOB. Для получения дополнительной информации относительно необходимых изменений к сценариям регистрации, перейдите:

http://www. cisco . com/en/US/products/ps6128/products_configuration_example09186a0080a70c18.shtml

## Устройство Cisco NAC Настройки для входа в систему агента и клиентской оценки положения

Агент Cisco NAC и веб-Агент NAC Cisco предоставляют локальную оценку положения и исправление для клиентских компьютеров. Пользователи загружают и устанавливают агента Cisco NAC или веб-Агента NAC Cisco (клиентское программное обеспечение только для чтения), который может проверить реестр хоста, процессы, приложения и сервисы. Для получения дополнительной информации об агенте и оценке положения и исправлении, перейдите:

http://www. cisco . com/en/US/docs/security/nac/appliance/configuration_guide/47/cam/m_agntd.html

# Дополнительные сведения

- Cisco Systems – техническая поддержка и документация