Уровень 3 NAC Cisco OOB Использование облегченного VRF для изоляции трафика

Содержание

Введение

Это руководство описывает реализацию системы контроля допуска к сети (NAC) при внеполосном (OOB) развертывании на уровне 3 на основе пересылки по виртуальным маршрутам (VRF)-Lite.

Обзор решения

В этом разделе приведены краткое введение Уровню 3 OOB использование Облегченных VRF методов для реализации архитектуры NAC.

Пояснительная записка

NAC Cisco принуждает политику сетевой безопасности организации по всем устройствам, которые ищут доступ к сети. NAC Cisco позволяет только совместимые и доверяемые оконечные устройства, такие как PC, серверы и PDA, на сеть. NAC Cisco ограничивает доступ несовместимых устройств, который ограничивает потенциальный ущерб от появляющихся угроз безопасности и рисков. NAC Cisco дает организациям мощный, основанный на ролях метод, чтобы предотвратить неавторизованный доступ и улучшить способность сети к восстановлению.

Решение для NAC Cisco предоставляет эти 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 доступ** — Управляет и уменьшает крупномасштабные разрушения инфраструктуры; уменьшает эксплуатационные расходы путем создания шагов, добавляет и изменяется динамичный и автоматизированный, таким образом включающая более высокая эффективность IT; интегрируется с другими компонентами Cisco SDN для отправки защиты универсальной безопасности

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. Можно использовать несколько методов задания конфигурации для выполнения этой задачи. Этот документ фокусирует в частности на основанной на VRF реализации NAC Cisco в Уровне 3 развертывания OOB, где сервер Cisco NAC (Сервер Cisco Clean Access) настроен в (маршрутизировавшем) режиме реального IP-шлюза.

Уровень 3 OOB является одной из самых популярных методологий развертываний для NAC. Это переключается на нижний регистр, популярность основывается на нескольких движущих силах, которые включают лучшее использование аппаратных ресурсов. Путем развертывания NAC Cisco в Уровне 3 методология OOB одиночное устройство Cisco NAC может масштабироваться для размещения большего количества пользователей. Это также позволяет устройствам Cisco NAC быть расположенными в центре, а не распределенным через кампус или организацию. Поэтому Уровень 3 развертывания OOB более экономически эффективен и от капитала и от точки зрения эксплуатационных расходов.

Это руководство описывает реализацию NAC Cisco в Уровне 3 развертывания OOB, которые основываются Облегченный VRF.

Простое определение VRF

Один способ посмотреть на виртуализацию устройства VRF состоит в том, чтобы прировнять его к появлению VLAN. Созданные виртуальные коммутаторы VLAN из одиночного физического коммутатора. VRF расширяют ту виртуализацию мимо границы Уровня 2 и позволяют создание виртуальных маршрутизаторов. Виртуальные маршрутизаторы обеспечивают полностью виртуализированные сети от от начала до конца.

Другой способ посмотреть на дизайн VRF состоит в том что каждый VRF действия точно так же, как VPN или туннель. Трафик, который размещен в VRF, не может связаться за пределами VRF (туннель), пока трафик не проходит через устройство, которое завершает туннель (целевой маршрутизатор с поддержкой VPN).

Примечание: Эти определения предназначаются, чтобы помочь представлять новую концепцию. Эти определения не являются точными представлениями или официальными определениями VRF.

Рисунок 1 показывает рисунок виртуализации устройства с VRF. Каждый цветной уровень в схеме представляет другой виртуальный маршрутизатор или VRF. Методология VRF предоставляет уровень управления и изоляцию пути плоскости данных, наряду со способностью иметь множественные отдельные плоскости данных. Другими словами, это предоставляет возможность для отдельного виртуального маршрутизатора или сеть для каждого типа трафика, который ожидается в среде, которая использует NAC Cisco. Типичные типы трафика:

- Не прошедший поверку подлинности трафик пользователя
- Трафик проверенного пользователя
- Трафик подрядчика
- Гостевой трафик

Рисунок 1 – ***виртуализация устройства***

Архитектура решения

Серверы Cisco NAC были первоначально разработаны, чтобы быть внутриполосными устройствами. Использование устройств Cisco NAC на инфраструктуре Сети Cisco позволяет вам брать устройство, которое было разработано, чтобы быть внутриполосным ко всему сетевому трафику и развернуть его с методологией OOB.

Архитектура решения (см. рисунок 2) определяет ключевые компоненты данного решения и точку интеграции сервера Cisco NAC.

Примечание: В этом документе термины “коммутатор Edge” и “коммутатор доступа” использованы взаимозаменяемо.

Рисунок 2 – ***архитектура решения***

Следующие разделы описывают доступ, распределение, ядро и уровни ЦОД, которые составляют типичную архитектуру кампуса.

Уровень доступа

Уровень 3 OOB решение для NAC Cisco применим к Направленному проекту уровня кампуса Доступа. В маршрутизировавшем режиме доступа коммутируемые виртуальные интерфейсы Уровня 3 (SVI) настроены на коммутаторе доступа. Поскольку рисунок 3 показывает, VLAN доступа Уровня 3 (например, VLAN 100) 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.

Рисунок 3 – ***коммутаторы доступа с уровнем 3 к краю***

Уровень распределения

Уровень распределения ответственен за маршрутизацию Уровня 3 и агрегацию уровней доступа коммутатора. В то время как можно разместить серверы Cisco NAC в этот уровень в

Уровне 2 дизайн OOB, вы не определяете местоположение их здесь в Уровне 3 дизайн OOB. Вместо этого разместите серверы Cisco NAC централизованно в Блоке Сервиса ЦОД, поскольку архитектура решения показывает (рисунок 2).

Центральный уровень

Магистральный уровень использует Маршрутизаторы на основе IOS Cisco. Магистральный уровень зарезервирован для высокоскоростной маршрутизации без любых сервисов. Разместите сервисы в сервисный коммутатор в ЦОД.

Уровень сервисов ЦОД

Уровень сервисов ЦОД использует Маршрутизаторы на основе IOS Cisco и переключается в сеть уровня кампуса. Диспетчер Cisco NAC Manager и сервер Cisco NAC расположены в центре в Блоке Сервиса ЦОД в этом Уровне 3 дизайн OOB.

Компоненты решения

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 Cisco OOB диспетчер Cisco NAC Manager предоставляет управление OOB, чтобы добавить и управляющие переключатели в домене диспетчера Cisco NAC Manager 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 логически разделяет недоверяемое и надежные сети, и это служит централизованной точкой осуществления для всех списков доступа (ACL) и ограничения полосы пропускания для устройств в сети без доверия. Посмотрите Выбор режима OOB для получения дополнительной информации.

Агент Cisco NAC

Агент Cisco NAC является дополнительным компонентом решения для NAC Cisco. Когда Агенту включают для ваших развертываний NAC Cisco, они гарантируют, что компьютеры, которые обращаются к вашей сети, удовлетворяют системные требования положения, которые вы задаете. Агент 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 вам получать любые недостающие обновления или программное обеспечение. Посмотрите Шаг 6: Политика Обновления от Cisco.com на диспетчере Cisco NAC Manager для получения дополнительной информации.

Принципы проектирования

Когда вы считаете Уровень 3 развертываниями NAC OOB, рассматриваете несколько вопросов проектирования. Эти факторы перечислены в этих подразделах, наряду с кратким обсуждением их важности.

Режим OOB

В устройстве Cisco NAC развертывания OOB Сервер NAC связывается с конечным хостом только во время процесса проверки подлинности, оценки положения и исправления. После того, как конечный хост сертифицируется, он не связывается с Сервером.

В режиме OOB диспетчер Cisco NAC Manager использует протокол SNMP чтобы 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. Контроль портов коммутатора известен как уровень управления SNMP. Для списка моделей поддерживаемого коммутатора обратитесь к разделу *Поддерживаемых коммутаторов OOB* Поддержки коммутаторов для устройства Cisco NAC.

Режим OOB прежде всего используется для проводных развертываний. Когда метод VRF Уровня 3, OOB используется, весь трафик от недоверяемых (грязных) VLAN, включая трафик агента, достигает централизованного сервера Cisco NAC, где все осуществление имеет место. Осуществление трафика в Сервере является основным дифференцирующим звеном между методом VRF и методом ACL Уровня 3 OOB.

Примечание: Сервер Cisco NAC был первоначально спроектирован, чтобы быть внутренним устройством. Другими словами, Сервер был разработан для имения всего трафика через него, который позволит Серверу быть контрольной точкой. При использовании Метода VRF Уровня 3 OOB все не прошедшие поверку подлинности потоки трафика пользователя через Сервер точно, как будто это были внутриполосные развертывания. Этот трафик обеспечивает последовательную, предсказуемую среду.

Классификация оконечных точек

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

Это возможные типы устройства:

- Корпоративные устройства
- Некорпоративные устройства
- Устройства NONPC

Это 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, подрядчики и другие оконечные точки, такие как принтеры, точки беспроводного доступа и IP-камеры. Роли сопоставлены с VLAN коммутатора Edge.

Примечание: Дополнительная роль требуется для Аутентификации, которой первоначально принадлежат все оконечные точки. Эта роль сопоставляет с не прошедшей поверку подлинности “грязной” VLAN.

Изоляция роли

Для этого типа дизайна NAC трафик, классифицированный как “грязный”, должен течь в “недоверяемую” сторону сервера Cisco NAC. Помните этот принцип при разработке реализации NAC Cisco. Кроме того, не позволяйте “чистым” и “грязным” сетям связываться непосредственно друг с другом.

Рисунок 4 показывает, что, когда Уровень 3 дизайн OOB использует VRF, VRF гарантирует, что не прошедший поверку подлинности трафик остается отдельным в своей собственной виртуальной сети. Сервер Cisco NAC действует как точка осуществления или контроллер, который гарантирует сегрегацию и безопасную связь между “чистыми” и “грязными” сетями.

Рисунок 4 – ***подключения сервера Cisco NAC к грязным и чистым сторонам***

Трафик

Когда оконечная точка связана с управляемым NAC портом коммутатора, процесс NAC начинается. Трафик, классифицированный как “грязный” или “не прошедший поверку подлинности”, изолирован от остатка сети (сетей), как это находится в “грязном” VRF. Этот трафик изолирован и передан ненадежному интерфейсу на сервере Cisco NAC. См. рис. 4.

Примечание: Устройство Cisco NAC не обращает внимания на то, как трафик представлен ему. Другими словами, само Устройство не имеет никакого предпочтения, поступает ли трафик через туннель универсальной инкапсуляции маршрутизации (GRE) или перенаправлен через конфигурацию маршрутизации на основе политик, маршрутизировавшую VRF, или другие методы перенаправления.

Режим сервера Cisco NAC

Можно развернуть сервер Cisco NAC в одном из этих двух режимов:

- Действительный шлюз (мост) режим
- Реальный IP-шлюз (направленный) 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: Этот режим не применим для этого определенного дизайна ACL.

РЕАЛЬНЫЙ IP-ШЛЮЗ (направленный) режим

(Маршрутизировавший) режим РЕАЛЬНОГО IP-ШЛЮЗА более применим в дизайне, где сервер Cisco NAC является многоуровневым 3 перехода далеко от оконечной точки, таким как Уровень 3 OOB. Когда вы будете использовать Сервер в качестве РЕАЛЬНОГО IP-ШЛЮЗА, задайте IP-адреса его двух интерфейсов: один для доверяемой стороны (управление сервером) и один для недоверяемой (грязной) стороны. Два адреса должны быть на других подсетях. IP ненадежного интерфейса используется для связи с оконечной точкой на недоверяемой подсети. Режимом, который использует это руководство, является РЕАЛЬНЫЙ IP-ШЛЮЗ.

Пользовательский опыт (с агентом Cisco NAC)

Как правило, корпоративным объектам развернули агента Cisco NAC заранее до конца клиенты. Параметр хоста Обнаружения в Агенте инициирует пакеты обнаружения, которые будут передаваться ненадежному интерфейсу сервера Cisco NAC, который автоматически продолжает оконечную точку посредством процесса NAC.

В Уровне 3 OOB с моделью VRF Хост Обнаружения, как правило, собирается быть именем DNS или IP-адресом диспетчера Cisco NAC Manager. Менеджер существует в чистой сети. Поскольку весь трафик от “грязных” сетей маршрутизируется по умолчанию через сервер Cisco NAC, Пакеты обнаружения автоматически текут через Сервер. Трафик, описанный здесь, является одним из преимуществ к Методу VRF. Этот трафик обеспечивает последовательный, предсказуемый опыт. Посмотрите Потоки процессов NAC Cisco для получения дополнительной информации.

Пользовательский опыт (без агента Cisco NAC)

Способность работать без агента Cisco NAC является другим преимуществом модели VRF. Весь трафик от “грязных” сетей маршрутизируется естественно через сервер Cisco NAC. Это означает, что пользователь на машине без агента Cisco NAC только должен открыть web-браузер и перейти к любому допустимому веб-сайту. Трафик браузера пытается пройти через Сервер, который в свою очередь перехватывает сеанс через обозреватель и перенаправляет его к присоединенному порталу. Посмотрите Потоки процессов NAC Cisco для получения дополнительной информации.

Примечание: Для лучшей возможной производительности конечного пользователя используйте сертификаты, которым доверяет браузер конечного пользователя. Самогенерируемые сертификаты на сервере Cisco NAC и диспетчере Cisco NAC Manager не рекомендуются для производственной среды.

Примечание: Всегда генерируйте сертификат для сервера Cisco NAC с IP-адресом его ненадежного интерфейса.

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 на рисунке 6 для окруженных шагов, которые находятся на рисунке 5.

Рисунок 5 – ***поток процессов NAC для уровня 3 OOB решение для NAC Cisco*** **Рисунок 6 –** ***блок-схема потока процессов NAC Cisco***

Реализация решения NAC Cisco

В этом разделе описывается внедрить решение для NAC Cisco.

Топология

Рисунок 7 показывает топологию, используемую для создания этого руководства. Внутренняя сеть, которая состоит из VLAN 200 и 210, маршрутизируется при помощи таблицы глобальной маршрутизации. Внутренняя сеть не имеет никакого VRF, привязанного к нему.

Грязный VRF содержит только VLAN DIRTY и связанные транзитные сети, которые необходимы для создания одиночной виртуальной сети для всего Грязного трафика для течения Грязной стороне централизованного сервера Cisco NAC.

Гостевой VRF содержит ГОСТЕВУЮ VLAN и привязанные транзитные сети, которые необходимы для завершения всего источника данных от ГОСТЕВОЙ VLAN на отдельном подчиненном интерфейсе на межсетевом экране. Каждую из этих трех виртуальных сетей (DIRTY, ГОСТИ и ГЛОБАЛЬНЫЙ) несут на той же физической инфраструктуре и предоставляет завершенный трафик и изоляцию пути.

Рисунок 7 – ***Топология, Используемая в этом Руководстве***

Заказ операций

Заказ операций для развертываний решения для NAC Cisco подключен легко дебатам. Вы настраиваете часть NAC решения, прежде чем будет подготовлена сеть? Или, вы готовите сеть перед настройкой устройств NAC Cisco?

В целях организации это руководство фокусируется на конфигурации сети сначала. Это гарантирует, что сеть готова к NAC, тогда конфигурация продуктов NAC Cisco.

Конфигурация сети

Это руководство фокусируется на сквозном, Облегченном VRF для изоляции пути. Следует отметить, что можно использовать VRF с Туннелем GRE для разрешения изоляции пути посредством существующего распределения и магистрального уровня, не требуя никакой конфигурации в тех устройствах. Для получения дополнительной информации о том, когда,

и почему использовать Туннели GRE по сравнению со сквозным дизайном VRF, посмотрите Расширение VRF Между Двумя разделами Устройств. Можно также обратиться к Уровню 3 NAC Внеполосное Руководство по дизайну Который Использование, Облегченное VRF для Изоляции Трафика.

Этот документ является полным руководством по дизайну, фокусируемым на Облегченном VRF с методом GRE.

Кроме того, полная коммутация на основе тэгов может использоваться вместо Облегченного VRF когда это применимо. Коммутацию на основе тэгов считают из области в целях этого документа.

Важные факторы для облегченного VRF

Примечание: Облегченный VRF функция, которая позволяет вам поддержать две или больше виртуальных сети. Облегченный VRF также обеспечивает перекрывающиеся IP-адреса среди виртуальных сетей. Однако наложение IP-адреса не рекомендуется для реализации NAC, потому что, в то время как сама инфраструктура поддерживает совмещенные адреса, это может создать сложности устранения проблем и неправильное создание отчетов.

Подробные данные, данные в шагах, предоставленных в этом разделе, выделяют шаги, необходимые для настройки сети для изоляции пути, использующей Облегченный VRF. Конфигурация, требуемая для вставки устройства Cisco NAC в вашу сеть как Уровень 3 РЕАЛЬНЫЙ IP-ШЛЮЗ OOB, также предоставлена.

Облегченные VRF входные интерфейсы использования для различения маршрутов для других виртуальных сетей и форм разделяют таблицы виртуальной маршрутизации путем соединения одного или более Интерфейсов уровня 3 к каждому VRF. Интерфейсы в VRF могут быть или физическими, такими как Порты Ethernet, или они могут быть или логические, такие как подчиненные интерфейсы, Туннельные интерфейсы или виртуальные интерфейсы коммутатора VLAN (SVI).

Примечание: Интерфейс уровня 3 не может принадлежать нескольким VRF за один раз.

Обратите внимание на эти Облегченные VRF факторы:

- Облегченный VRF является локально значительным только к коммутатору, где он определен, и членство VRF определено входным интерфейсом. Никакое манипулирование заголовком пакета или информационным наполнением выполнено.
- Коммутатор с Облегченным VRF разделен множественными виртуальными сетями (домены защиты), и все домены защиты имеют свои собственные уникальные таблицы маршрутизации.
- Все домены защиты должны иметь свои собственные VLAN.
- Облегченный VRF не поддерживает всю Многопротокольную коммутацию по меткам (MPLS) - функциональность VRF, такая как обмен метки, смежность Протокола распределения меток (LDP) или помеченные пакеты, которые являются также, знает как коммутация на основе тэгов).
- Ресурс Ternary Content Addressable Memory (TCAM) Уровня 3 разделен между всеми VRF. Чтобы гарантировать, что любой VRF имеет достаточное пространство ассоциативной памяти (CAM), используйте **команду maximum routes**.

- Коммутатор Catalyst, который использует Облегченный VRF, может поддержать одну глобальную сеть и до 64 VRF. Общее число поддерживаемых маршрутов ограничено размером TCAM.
- Можно использовать большинство протоколов маршрутизации, таких как Протокол BGP, Протокол OSPF, Протокол EIGRP, Протокол RIP и статичная маршрутизация между устройствами, которые работают Облегченный VRF.
- В большинстве случаев нет никакой потребности выполнить BGP с Облегченным VRF.
- Облегченный VRF не влияет на скорость коммутации пакетов.
- Вы не можете настроить Групповую адресацию и Облегченный VRF на том же Интерфейсе уровня 3 в то же время.
- Используйте **подкоманду capability vrf-lite** под маршрутизатором ospf при настройке OSPF как протокола маршрутизации между сетевыми устройствами.

Определите VRF

В этом Примере проектирования изоляция пути должна быть предоставлена для не прошедших поверку подлинности или грязных пользователей и гостей. Всему другому трафику разрешают использовать внутреннюю сеть. Необходимо определить два VRF, поскольку эта конфигурация показывает:

Пример конфигурации VRF

```
!--- This command creates a VRF for the DIRTY virtual
network: ! ip vrf DIRTY ! !--- This command names the
VRF and places you into VRF configuration mode: !
description DIRTY_VRF_FOR_NAC ! !--- Gives the VRF a
user friendly description field for documentation ! rd
100:3 ! !--- Creates a VRF table by specifying a route
distinguisher. !--- Enter either an AS number and an
arbitrary number (xxx:y) or an IP !--- address and
arbitrary number (A.B.C.D:y). ! !--- This document uses
the Autonomous System number and a unique router-id in
that AS. !--- This example signifies AS 100:Router-ID 3
!
```

Примечание: Признак маршрута не является требуемой конфигурацией для Облегченного VRF. Однако это считают оптимальным методом для настройки признака маршрута для будущего, так, чтобы это работало эффективно с коммутацией на основе тэгов.

```
! -- Here we create a VRF for the GUEST Virtual Network: ! ip vrf GUESTSdescription
GUESTS_VRF_FOR_VISITORSrd 600:3 !
```

Привяжите VLAN или интерфейс с VRF

После того, как VRF определен на Коммутаторе 3 уровня или маршрутизаторе, необходимо привязать интерфейсы, которые переходят, участвуют в Облегченной VRF конфигурации с VRF, где они принадлежат. Можно связаться или физический или виртуальные интерфейсы с VRF. Этот раздел предоставляет примеры физического интерфейса, интерфейса sub, коммутируемого виртуального интерфейса и туннельного интерфейса, которые все привязаны к VRF.

Примечание: Примеры являются выборками только и не использовались в топологии этого документа.

Пример конфигурации физического интерфейса
interface FastEthernet0/1 ip vrf forwarding GUESTS *!--- Associates the interface with the appropriate VRF defined in Step 1.* ip address 192.168.39.1 255.255.255.252

Пример конфигурации подчиненного интерфейса
interface FastEthernet3/1.10 encapsulation dot1Q 10 ip vrf forwarding DIRTY ip address 192.168.10.1 255.255.255.252

Пример конфигурации коммутируемого виртуального интерфейса
interface Vlan100 ip vrf forwarding DIRTY ip address 192.168.100.1 255.255.255.0

Пример конфигурации туннельного интерфейса
interface Tunnel0 ip vrf forwarding GUESTS ip address 192.168.38.2 255.255.255.252 tunnel source Loopback0 tunnel destination 192.168.254.1

Расширьте устройство VRF между двумя устройствами

Существует несколько приемлемых методологий, которые можно использовать для расширения VRF между двумя частями инфраструктуры. Удостоверьтесь, что метод, который вы выбираете, основывается на этих критериях:

- Рассмотрите возможности платформы. Вся текущая Cisco способная к уровню 3 Коммутация Предприятия и Облегченная VRF поддержка Платформ маршрутизации. Эти платформы включают, но не ограничены, Catalyst 6500, 4500, 3750, и 3560 платформ.
- Платформа маршрутизации должна выполнить соответствующий IOS. Платформы включают, но не ограничены, 7600, 3900, 3800, 2900, 2800, 1900, 1800, и маршрутизаторы ISR серии 800 (ISR).
- Рассмотрите количество переходов Уровня 3 между соответствующими частями инфраструктуры. Для определения количества переходов Уровня 3 поддержите развертывания максимально простыми. Например, если пять переходов Уровня 3 существуют между инфраструктурой, которая размещает устройства Сигнализации по выделенному каналу (CAS) и клиентов, она может создать административную служебную информацию.

С неправильным решением:

- Транкинг уровня 2 создает очень субоптимальную топологию Уровня 2.
- Подчиненные интерфейсы уровня 3 создают много дополнительных интерфейсов для настройки. Больше интерфейсов для настройки может создать дополнительную служебную информацию управления и потенциальные проблемы IP-адресации. Учитывая, что нет никакого резервирования в инфраструктуре, каждый уровень сети имеет и входной и выходной физический интерфейс. Вычисление для количества подинтерфейсов тогда (2 * количество уровней в сети * количество VRF). Наш пример

имеет два VRF, таким образом, формула (2 *5 * 2) или 20 подчиненных интерфейсов. После того, как резервирование добавлено, этот номер более чем удваивается. Сравните это с расширением GRE, где только четыре интерфейса требуются с тем же конечным результатом. Это сравнение иллюстрирует, как GRE уменьшает влияние конфигурации.

Транкинг уровня 2

Транкинг уровня 2 предпочтен в сценариях, где устройства уровня доступа не поддерживают подчиненные интерфейсы. Catalyst 3560, 3750, и 4500 платформ не поддерживает подчиненные интерфейсы.

В модель доступа Уровня 3, которая соединяется с платформой, которая не поддерживает подчиненные интерфейсы к платформе, которая делает, только используйте транкинг Уровня 2 на одной стороне и используйте подчиненные интерфейсы с другой стороны. Эта конфигурация поддерживает все преимущества архитектуры помещения Уровня 3 и все еще преодолевает ограничение никакой поддержки подчиненного интерфейса на некоторых платформах.

Одно из основных преимуществ настройки транкинга Уровня 2 только на одной стороне ссылки - то, что Связующее дерево не введено назад в среду Уровня 3. Посмотрите 3750 Примеров Соответствующей конфигурации где 3750 Коммутаторов доступа. то, которое не поддерживает GRE или подчиненные интерфейсы, связано с 6500 Коммутаторами распределения. 6500 Коммутаторов распределения действительно поддерживают GRE и подчиненные интерфейсы.

3750 соответствующих конфигураций

В этой конфигурации настройка по умолчанию для СОБСТВЕННОГО VLAN является VLAN 1 на FastEthernet 1/0/1. Эта конфигурация не была изменена. Однако VLAN 1 не позволяют быть соединенным магистралью через ссылку. Позволенный VLANs ограничен только VLAN, которые помечены.

Нет никакой потребности в согласовании магистрали между коммутаторами или трафике Транкингового протокола VLAN (VTP) в этой топологии Уровня 3. Поэтому нет также никакой потребности ни в каком немаркированном трафике, который будет передан на этой ссылке. Эта конфигурация увеличивает положение безопасности архитектуры, потому что это не открывает ненужные дыры безопасности уровня 2.

3750 примеров соответствующей конфигурации

```
!--- 3750 Switch configuration, related to connecting it
to a !--- sub-interface capable switch (Catalyst 6500):
! ip vrf DIRTY rd 100:1 ! ip vrf GUEST rd 600:1 !
interface GigabitEthernet1/0/48 description Uplink to
Cat6k switchport trunk encapsulation dot1q switchport
trunk allowed vlan 901-903,906 switchport mode trunk
spanning-tree portfast trunk ! !--- Since the 3750 does
not support sub-interfaces, !--- you must configure one
SVI per transit network: ! interface Vlan901 description
DIRTY_TRANSIT ip vrf forwarding DIRTY ip address
172.26.120.2 255.255.255.252 ! interface Vlan902
description GLOBAL_TRANSIT ip address 172.26.120.6
255.255.255.252 ! interface Vlan906 description
GUEST_TRANSIT ip vrf forwarding GUEST ip address
```

```
172.26.120.14 255.255.255.252 ! !--- This configuration
uses EIGRP as the routing protocol !--- of choice in
this document. !--- Each VRF is defined as a separate !-
-- Autonomous System under the Global AS. ! router eigrp
26 ! address-family ipv4 vrf DIRTY network 172.26.120.0
0.0.0.255 autonomous-system 100 no auto-summary exit-
address-family ! address-family ipv4 vrf GUEST
redistribute static network 172.26.120.0 0.0.0.255
autonomous-system 600 no auto-summary exit-address-
family network 172.26.0.0
```

6500 соответствующих конфигураций

В этой конфигурации инкапсуляция dot1q используется для маркировки кадров с VLAN 901, 902, и 906. При выборе тегов VLAN для использования на подчиненном интерфейсе, вы не можете использовать номер виртуальной локальной сети (VLAN), который уже определен локально в Базе данных VLAN на коммутаторе.

6500 примеров соответствующей конфигурации

```
!--- 6500 Switch configuration, related to connecting it
!--- to a non-sub-interface capable switch (Catalyst
3750): ! ip vrf DIRTY rd 100:26 ! ip vrf GUEST rd 600:26
! interface FastEthernet1/34 description NAC LAB - 3750
no ip address ! interface FastEthernet1/34.901
encapsulation dot1Q 901 ip vrf forwarding DIRTY ip
address 172.26.120.1 255.255.255.252 ! interface
FastEthernet1/34.902 encapsulation dot1Q 902 ip address
172.26.120.5 255.255.255.252 ! interface
FastEthernet1/34.906 encapsulation dot1Q 906 ip vrf
forwarding GUEST ip address 172.26.120.13
255.255.255.252 ! !--- EIGRP is the routing protocol of
choice in this document. !--- Each VRF is defined as a
!--- separate Autonomous System under the Global AS. !--
- See Configure Routing for the VRF for more
information. ! router eigrp 26 network 172.26.0.0
0.0.255.255 no auto-summary passive-interface Vlan1
redistribute static ! address-family ipv4 vrf DIRTY
autonomous-system 100 network 172.26.120.0 0.0.0.3
network 172.26.160.0 0.0.0.255 no auto-summary no
default-information out redistribute static route-map
gw-route exit-address-family ! address-family ipv4 vrf
GUEST redistribute static network 172.26.120.0 0.0.0.255
autonomous-system 600 no auto-summary exit-address-
family !
```

Настройте маршрутизацию для VRF

Как обсуждено ранее в Важных Факторах для Использования Облегченного VRF раздела, Облегченного VRF BGP поддержек, OSPF и EIGRP. В этом примере конфигурации выбран EIGRP, потому что это - протокол маршрутизации, который Cisco рекомендует для реализации на Сетях уровня кампуса, где требуется быстрая конвергенция.

Примечание: OSPF работает одинаково хорошо с Облегченным VRF, как делает BGP.

Примечание: BGP требуется, если дизайн требует, чтобы трафик был “пропущен” между VRF.

Маршрутизация для VRF с Примерами конфигураций EIGRP
! *!--- This base routing protocol configuration handles the routing !--- for the Global Routing Table.* ! router eigrp 26 network 172.26.50.0 0.0.0.255 network 172.26.51.0 0.0.0.255 network 172.26.52.0 0.0.0.255 network 172.26.55.0 0.0.0.255 network 172.26.60.0 0.0.0.255 network 172.26.61.0 0.0.0.255 network 172.26.62.0 0.0.0.255 network 172.26.120.4 0.0.0.3 network 172.26.176.0 0.0.0.255 network 172.26.254.1 0.0.0.0 no auto-summary passive-interface Vlan1 redistribute static ! *!--- You must define an address family for each VRF !--- that is to be routing using the routing protocol. !--- Routing protocol options such as auto-summarization, !--- AS number, and router id are all configured under the !--- address family. EIGRP does not form a neighbor !--- relationship without the AS specified under the address family. !--- Also, this AS number needs to be unique for !--- each VRF and cannot be the same as the global AS number.* ! address-family ipv4 vrf DIRTY autonomous-system 100 network 172.26.120.0 0.0.0.3 network 172.26.160.0 0.0.0.255 no auto-summary no default-information out redistribute static route-map gw-route exit-address-family ! address-family ipv4 vrf GUEST redistribute static network 172.26.120.0 0.0.0.255 autonomous-system 600 no auto-summary exit-address-family !

Трафик маршрута между таблицей глобальной маршрутизации и грязным VRF

В зависимости от требований развертываний NAC может быть необходимо передать трафик с недоверяемой или грязной стороны сети доверяемой или чистой стороне сети. Например, сервисы исправления могут потенциально жить на Доверяемой стороне устройства Cisco NAC. В случае развертываний единой точки входа Active Directory необходимо передать подмножество трафика к Active Directory для разрешения интерактивного обмена билета Kerberos входов в систему и так далее.

При любых обстоятельствах очень важно, чтобы таблица глобальной маршрутизации знала, как достигнуть грязного VRF, и что грязный VRF знает, как достигнуть таблицы глобальной маршрутизации, если какие-либо данные должны пройти между двумя. Это, как правило, обрабатывается методологией на рисунке 8.

Грязные настройки по умолчанию VRF к недоверяемому или грязному интерфейсу устройства Cisco NAC. Глобальный имеет статические маршруты только к подсетям, которые считают грязными VLAN. Те статические маршруты указывают к чистому (доверяемому) интерфейсу сервера Cisco NAC как следующий переход.

Рисунок 8 – ***потоки маршрутизации***

Первый переход Уровня 3 на недоверяемой или грязной стороне устройства Cisco NAC перераспределяет маршрут по умолчанию в процесс маршрутизации, который указывает к устройству Cisco NAC. Первый переход Уровня 3 на доверяемой или чистой стороне устройства Cisco NAC перераспределяет статический маршрут для подсети (подсетей), которые принадлежат грязной VLAN в уровне доступа (в этом случае 172.26.123.0/26).

Примечание: Первый переход Уровня 3 на противоположных сторонах устройства Cisco

NAC может быть на том же физическом устройстве, но в других VRF.

Примечание: В то время как доверяемая или чистая сторона устройства Cisco NAC остается в таблице глобальной маршрутизации, в топологии, используемой для этого документа, недоверяемая или грязная сторона сервера Cisco NAC находится в VRF. Однако оба интерфейса связаны с тем же коммутатором для ЦОД.

Уровень 3 NAC Cisco OOB облегченный VRF пример конфигурации

Для успешного развертывания NAC Cisco решение OOB необходимо настроить компоненты NAC для соответствия с желаемой архитектурой. Рисунком 9 является Уровень 3 NAC Cisco логическая схема сети OOB, которая используется в этом разделе для показа соответствующей конфигурации диспетчера Cisco NAC Manager, сервера Cisco NAC и коммутатора Edge для Уровня 3 NAC OOB с Облегченными VRF развертываниями.

Рисунок 9 – ***уровень 3 NAC Cisco логическая топология OOB***

Выполните шаги в этих разделах для настройки реального IP Уровня 3 VRF OOB развертывания NAC Cisco:

Шаг 1: Настройте коммутатор Edge

Поскольку эти примеры конфигурации показывают, создают еще две VLAN (DIRTY и ГОСТЬ) на коммутаторе Edge.

Существующая производственная VLAN (VLAN 200) используется для всех корпоративных систем. Данный пример создает VLAN, их связанные транзитные сети, и назначает обоих на корректные VRF. Осуществление имеет место в сервере Cisco NAC, таким образом, вы не должны применять ACL к каждой VLAN в коммутаторе.

Неаутентифицированная роль: VLAN 100, грязный пример конфигурации VRF

```
!--- Define the DIRTY VRF. ip vrf DIRTY rd 100:3 !---
Create the SVI for the DIRTY VLAN. interface Vlan100 ip
vrf forwarding DIRTY ip address 172.26.123.1
255.255.255.224 ip helper-address vrf DIRTY 172.26.51.11
!--- Create the SVI for the DIRTY_TRANSIT_NETWORK.
interface Vlan301 ip vrf forwarding DIRTY ip address
172.26.120.50 255.255.255.252 !--- Set the allowed VLAN
on the trunk. interface FastEthernet1/0/48 switchport
trunk allowed vlan add 301 !--- Set up the routing for
the VRF. router eigrp 26 address-family ipv4 vrf DIRTY
network 172.26.0.0 autonomous-system 100 no auto-summary
exit-address-family
```

Роль guest: VLAN 600, ГОСТЕВОЙ пример конфигурации VRF

```
!--- Define the GUEST VRF. ip vrf GUEST rd 600:3 !---
Create the SVI for the GUEST VLAN. interface Vlan600 ip
vrf forwarding GUEST ip address 172.26.123.193
255.255.255.224 !--- Create the SVI for the
DIRTY_TRANSIT_NETWORK. interface Vlan306 ip vrf
```

```
forwarding GUEST ip address 172.26.120.62
255.255.255.252 !--- Set the allowed VLAN on the trunk.
interface FastEthernet1/0/48 switchport trunk allowed
vlan add 306 !--- Set up the routing for the VRF. router
eigrp 26 address-family ipv4 vrf GUEST network
172.26.0.0 autonomous-system 600 no auto-summary exit-
address-family
```

Шаг 2: Настройте основной коммутатор

Примеры конфигурации в этом разделе показывают моделирование сжатой архитектуры с Catalyst 3750-E Коммутатор. В большинстве сред это не коммутатор граничного класса. Однако коммутатор был создан в лабораторной среде, используемой для этого документа.

Создайте еще четыре VLAN для транзитных сетей, два для VLAN DIRTY и два для ГОСТЕВОГО VLAN. (См. рис. 10.).

- ГРЯЗНАЯ VLANVLAN 301 DIRTY от края до ядраVLAN 901 DIRTY от ядра до ЦОД
- ГОСТЕВОЙ VLANГОСТЬ VLAN 306 от края до ядраГОСТЬ VLAN 906 от ядра до ЦОД

Транзитная сеть создается от края до ядра, и секунда для ядра к ЦОД. Транзитные сети должны быть завершены и для DIRTY и для ГОСТЕВЫХ VRF. Если коммутация на основе тэгов включена вместо Облегченного VRF, это не необходимо.

Примечание: Внимание этого документа на Облегченный VRF, и коммутация на основе тэгов считают из области.

Рисунок 10 – ***транзитные сети***
:

VLAN 301 DIRTY от края до ядра; VLAN 901 DIRTY от ядра до примера конфигурации ЦОД

```
!--- This is the core switch. !--- Define the DIRTY VRF.
ip vrf DIRTY rd 100:1 !--- Create the SVI for the DIRTY
VLANs. interface Vlan301 desc This is the Transit
Network between the Edge & Core ip vrf forwarding DIRTY
ip address 172.26.120.49 255.255.255.252 interface
Vlan901 desc This is the Transit Network between the
Core and the DC ip vrf forwarding DIRTY ip address
172.26.120.2 255.255.255.252 !--- Set the allowed VLAN
on the trunks. interface GigabitEthernet1/0/3 switchport
trunk allowed vlan add 301 interface
GigabitEthernet1/0/48 switchport trunk allowed vlan add
901 !--- Set up the routing for the VRF. router eigrp 26
address-family ipv4 vrf DIRTY network 172.26.0.0
autonomous-system 100 no auto-summary exit-address-
family exit-address-family
```

ГОСТЬ VLAN 306 от края до ядра; гость VLAN 906 от ядра до примера конфигурации ЦОД

```
!--- This is the core switch. ! !--- Define the GUEST
VRF. ip vrf GUEST rd 600:1 !--- Create the SVI for the
GUEST VLANS. interface Vlan306 desc This is the transit
network between the Edge & Core ip vrf forwarding GUEST
ip address 172.26.120.61 255.255.255.252 interface
Vlan906 description Transit Network between Core & DC ip
```

```
vrf forwarding GUEST ip address 172.26.120.14
255.255.255.252 !--- Set the allowed VLAN on the trunks.
interface GigabitEthernet1/0/3 switchport trunk allowed
vlan add 306 interface GigabitEthernet1/0/48 switchport
trunk allowed vlan add 906 !--- Set up the routing for
the VRF. router eigrp 26 address-family ipv4 vrf GUEST
network 172.26.0.0 autonomous-system 600 no auto-summary
exit-address-family
```

Шаг 3: Настройте коммутатор для ЦОД

Поскольку пример конфигурации показывает, сервер Cisco NAC имеет оба интерфейса, связанные с теми же 6500 коммутаторами для ЦОД. Доверяемый интерфейс находится в VLAN 60, и ненадежный интерфейс находится в VLAN 160, который находится в VRF DIRTY.

1. Создайте еще четыре VLAN для соединения с ядром:Грязная VLAN (160)Чистая VLAN (60)Грязная транзитная сеть (901)Чистая транзитная сеть (906)Добавьте VLAN DIRTY к VRF DIRTY.Завершите ГОСТЕВОЙ VRF в ГОСТЕВОМ DMZ (999), который использует Межсетевой экран Cisco ASA (из области для этого документа), чтобы подключить гостей с Интернетом и выполнить функции Технологии NAT.
2. Создайте DIRTY и ГОСТЕВЫЕ подчиненные интерфейсы транзита.Команды, показанные в Примере конфигурации Коммутатора для ЦОД, выполняют эти задачи:Определите ГОСТЕВЫЕ VRF и DIRTY.Создайте сети DIRTY и CLEAN для сервера Cisco NAC.

Пример конфигурации коммутатора для ЦОД

```
!--- Define the DIRTY and GUEST VRFs. ip vrf DIRTY rd
100:26 ip vrf GUEST rd 600:26 !--- Create the sub-
interface and switched virtual interface (SVI) !--- for
the DIRTY and GUEST VLANs. interface
FastEthernet1/34.901 desc Transit Network from Core to
DC for DIRTY traffic encapsulation dot1Q 901 ip vrf
forwarding DIRTY ip address 172.26.120.1 255.255.255.252
interface FastEthernet1/34.906 desc Transit Network from
Core to DC for GUEST traffic encapsulation dot1Q 906 ip
vrf forwarding GUEST ip address 172.26.120.13
255.255.255.252 interface Vlan60 desc Trusted (CLEAN)
side of the NAC Server ip address 172.26.60.1
255.255.255.0 interface Vlan160 desc Untrusted (DIRTY)
side of the NAC Server ip vrf forwarding DIRTY ip
address 172.26.160.1 255.255.255.0 interface Vlan999
description GUEST VLAN SVI ip vrf forwarding GUEST ip
address 192.168.26.254 255.255.255.0 !--- Set up the
routing for the VRFs. router eigrp 26 network
172.26.60.0 0.0.0.255 no auto-summary redistribute
static address-family ipv4 vrf DIRTY autonomous-system
100 network 172.26.120.0 0.0.0.3 network 172.26.160.0
0.0.0.255 no auto-summary redistribute static exit-
address-family address-family ipv4 vrf GUEST network
172.26.0.0 network 192.168.26.0 autonomous-system 600 no
auto-summary redistribute static exit-address-family !--
- Set up the static routes for redistribution for the
VRFs. ip route 172.26.123.0 255.255.255.192 172.26.60.2
ip route vrf DIRTY 0.0.0.0 0.0.0.0 172.26.160.2 ip route
vrf GUEST 0.0.0.0 0.0.0.0 192.168.26.1
```

Шаг 4. : 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. Перейдите к Установке Чистого Access Manager и Чистого Сервера доступа для выполнения начальной настройки.

Шаг 5. : 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 получения дополнительной информации о том, как загрузить лицензии, перейдите *к Доступу* раздел *Веба - консоли CAM* Установки Чистого Access Manager и Чистого Сервера доступа.

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.

Шаг 6: 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. 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 *к Потребовать Входу в систему Агента для* раздела *Клиентских компьютеров* устройства Cisco NAC Настройки для Входа в систему Агента и Клиентской Оценки Положения.

Шаг 7: 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 *к Системному времени*

Набора и *Чистым* разделам *Веба - консоли Прямого доступа Сервера доступа* Администрирования CAM.

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

Шаг 8: Настройка сервера Cisco NAC анализа

Большая часть важной вещи для запоминания за успешный дизайн NAC - то, что трафик, классифицированный как грязный, должен течь в недоверяемую сторону Сервера NAC, поскольку рисунок 11 показывает:

Рисунок 11 – ***развертывания сервера Cisco NAC***

Шаг 9: Добавьте сервер Cisco NAC к диспетчеру Cisco NAC Manager

Выполните эти шаги для добавления сервера Cisco NAC к диспетчеру Cisco NAC Manager:

1. Нажмите **CCA Servers** под областью Device Management. (См. рис. 12.).
2. Нажмите Новую вкладку Server.
3. Используйте коробку IP-адреса сервера для добавления IP-адреса доверяемого интерфейса сервера Cisco NAC.
4. В коробке Расположения сервера введите **сервер Cisco NAC OOB** как расположение сервера.
5. Выберите **Out-of-Band Real-IP Gateway** из выпадающего списка Типа сервера.
6. **Нажмите Add чистый сервер доступа**.

Рисунок 12 – ***добавляющий сервер Cisco NAC к диспетчеру Cisco NAC Manager***

Примечание: Диспетчер Cisco NAC Manager и сервер Cisco NAC должны доверять CA друг друга для Менеджера для успешного добавления Сервера.

После добавления сервера Cisco NAC это появляется в списке под вкладкой List of Servers. (См. рис. 13.).

Шаг 10: Настройте сервер Cisco NAC

Выполните эти шаги для настройки сервера Cisco NAC:

1. Нажмите вкладку List of Servers.
2. Нажмите значок Manage для сервера Cisco NAC для продолжения конфигурации.

Рисунок 13 – ***сервер Cisco NAC, управляемый диспетчером Cisco NAC Manager***

После нажатия значка Manage экран, показанный на рисунке 14, появляется.

Шаг 11: Включите поддержку уровня 3

Выполните эти шаги для включения поддержки Уровня 3:

1. Выберите вкладку Network.

2. Проверьте флажок **Enable L3 Support**.
3. Проверьте **Разрешать L3 строгий режим для блокирования устройств NAT с флажком Agent NAC**.
4. **Нажмите кнопку Update (Обновить).**
5. Перезагрузите сервер Cisco NAC, как проинструктировано.

Рисунок 14 – ***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 связывается с ненадежным интерфейсом Сервера для начала процесса NAC, Сервер перенаправляет пользователя к имени хоста сертификата или IP. Если точки сертификата к доверяемому интерфейсу, процесс регистрации в системе не функционирует правильно.

Шаг 12: Настройте статические маршруты

Выполните эти шаги для настройки статических маршрутов:

1. После перезагрузок сервера Cisco NAC возвратитесь к Серверу и продолжите конфигурацию.Сервер Cisco NAC должен использовать ненадежный интерфейс для передачи с оконечная точками на не прошедшей поверку подлинности VLAN.
2. Выберите **Advanced> Static Routes** для добавления маршрутов к не прошедшей поверку подлинности VLAN.
3. Заполните соответствующие подсети для не прошедших поверку подлинности VLAN.
4. **Нажмите Add маршрут**.
5. Выберите **Ненадежный интерфейс [eth1]** для этих маршрутов.

Рисунок 15 – ***добавляет статический маршрут для достижения не прошедшей поверку подлинности пользовательской подсети***

Шаг 13: Установите профили для коммутаторов в диспетчере Cisco NAC Manager

Выполните эти шаги для устанавливания профилей для коммутаторов в диспетчере Cisco NAC Manager:

1. Выберите **OOB Management> Profiles> Device> Edit**.
2. Заполните информацию о Профиле устройства. Используйте рисунок 16 в качестве руководства.Каждый коммутатор привязан к профилю. Добавьте профиль для каждого типа коммутатора Edge, которым будет управлять диспетчер Cisco NAC Manager. В данном примере управляют 3750 коммутаторами.**Рисунок 16 –** ***профиль SNMP, используемый для управления коммутатором***
3. Установите конфигурацию коммутатора для SNMP.Настройте коммутатор Edge для тех же строк имени и пароля чтения-записи SNMP, которые настроены на диспетчере Cisco NAC Manager.
```
snmp-server community Cisco123 RO
snmp-server community Cisco1234 RW
```
4. Выберите **OOB Management> Profiles> Port> New**. Посмотрите рисунок 17.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 Шаг 17: Настройте Роли пользователя. Сопоставления LDAP могут использоваться для сопоставления ролей пользователя в NAC группам LDAP. Для получения дополнительной информации обратитесь к NAC (CCA) 4. x: Пример конфигурации сопоставления пользователей с определенными ролям при помощи LDAP.**Рисунок 17 – *порт профиль для управления портом коммутатора***
Примечание: Можно также определить названия VLAN вместо ID. При определении названий VLAN у вас могут быть ИДЕНТИФИКАТОРЫ VLAN на других коммутаторах через кампус. Однако то же название VLAN присоединено к специальной роли.Дополнительные параметры доступны под профилем порта для IP, освобождают и возобновляют опции. Прокрутите вниз страницу, показанную в том, для наблюдения этих опций.Если пользователь находится позади IP-телефона, снимите флажок **с Сильным ударом порт после того, как VLAN является измененным** флажком. Если это проверено, это может возможно перезагрузить IP-телефон, когда возвращен порт.**Рисунок 18 – *различные варианты, доступные под портом профиль***

Шаг 14: Настройте параметры настройки получателя SNMP

В дополнение к устанавливанию Строки имени и пароля SNMP для Чтения-записи также необходимо 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 определенной оконечная точки Менеджеру, Менеджер в состоянии создать таблицу соответствий внутренне для MAC/IP и порта коммутатора.

1. Выберите **OOB Management> Profiles> SNMP Receiver**.
2. Настройте параметры настройки trap-сообщения SNMP, поскольку эти данные показывают:**Рисунок 19 – *значение получателя SNMP диспетчера Cisco NAC Manager для сбора trap-сообщений SNMP и сообщает***
3. Для настройки параметров коммутатора для trap-сообщений SNMP увеличьте таймер сброса Clean Access Manager (CAM) стандартного коммутатора до 1 часа 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.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 Качество обслуживания (QoS) для SNMP в сетевой среде большого объема трафика.

Шаг 15: Добавьте коммутаторы как устройства в диспетчере Cisco NAC Manager

Выполните эти шаги для добавления коммутаторов как устройств в диспетчере Cisco NAC Manager:

1. Выберите **OOB Management> Devices> Devices> New**.Используйте профиль коммутатора, созданный в Шаге 13 для добавления коммутатора.
2. Под Профилем устройства используйте профиль, который вы создали. Не изменяйте значение Профиля Порта по умолчанию, когда вы добавите коммутатор.**Рисунок 20 –** ***Добавляет Коммутатор Edge в диспетчере Cisco NAC Manager для Управления через SNMP***
3. После того, как Коммутатор добавлен к диспетчеру Cisco NAC Manager, можно выбрать порты, которыми вы хотите управлять.

Шаг 16: Настройте Порты коммутатора для Устройств, которые будут Управляемы NAC

Выполните эти шаги для настройки портов коммутатора для устройств, которые будут управляемы NAC.

1. Выберите **OOB Management> Devices Switch [IP address]> Ports> List** для наблюдения доступных портов коммутатора, которыми можно управлять.**Рисунок 21 –** ***выбор управления портами, доступный для управляемого коммутатора*** **Примечание:** Не оставляйте профиль по умолчанию столь же “неуправляемым”, пока вы не сможете отметить соответствующие интерфейсы статически как “неуправляемый”. После того, как порты каскадного соединения и любые другие релейные порты, которые должны остаться неуправляемыми, установлены; тогда измените по умолчанию на свой профиль управляемого порта. Сбой, чтобы сделать так в этом заказе может привести к меньше, чем выбираемым результатам.
2. Выберите **OOB Management> Devices Switch [IP address]> Ports> Manage** для управления несколькими портами сразу.

Рисунок 22 – ***управляет множественными портами с опцией соединения***

Шаг 17: настройте роли пользователя

В данном примере VLAN, которые соответствуют каждой роли, уже созданы в коммутаторе Edge.

1. Выберите **User Management> User Roles> Edit Role** и создайте роль сотрудника, поскольку эти данные показывают:**Рисунок 23 –** ***создает роль сотрудника и сопоставляет VLAN ДЛЯ ПЕРЕДАЧИ ДАННЫХ***

2. Выберите **User Management> User Roles> Edit Role** и создайте роль guest, поскольку эти данные показывают:**Рисунок 24 –** ***создает роль guest и сопоставляет ГОСТЕВОЙ VLAN***

Шаг 18: 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.

Шаг 19: 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 необходимо загрузить ActiveX или Компонент Java до конца клиент для выполнения этих задач:

- Выберите MAC-адрес клиентского компьютера.
- Выполните выпуск IP-адреса и возобновите.

1. Выберите **Administration> User Pages**.
2. Отредактируйте страницу для включения опций, поскольку эти данные показывают:

Рисунок 25 – ***параметры настройки страницы пользователя для веб-входа в систему***

Шаг 20: настройте агента Cisco NAC для ролей пользователя

Выполните эти шаги для настройки агента Cisco NAC для ролей пользователя:

1. Выберите **Device Management> Clean Access> General Setup> Agent Login**.Можно настроить диспетчера Cisco NAC Manager 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.
2. Проверьте **Потребовать использование флажка Agent**.

Рисунок 26 – ***вход в систему агента, требуемый для роли сотрудника***

Шаг 21: распределите хост обнаружения к агенту Cisco NAC

Распространение программного обеспечения агента Cisco NAC, установка и конфигурация покрыты в, Настраивают устройство Cisco NAC для Входа в систему Агента и Клиентской Оценки Положения. Данный пример настраивает хост обнаружения на диспетчере Cisco NAC Manager.

Выберите **Device Management> Clean Access> Clean Access Agent> Installation**:

Рисунок 27 – ***обнаруживает хост к агенту Cisco NAC***

Если агент Cisco NAC загружен от сервера Cisco NAC, поле Host Обнаружения

предварительно заполнено. (См. рис. 27.).

Примечание: В Уровне 3 OOB с моделью VRF Хост Обнаружения, как правило, собирается быть именем DNS или IP-адресом диспетчера Cisco NAC Manager, который существует в чистой сети. Поскольку весь трафик от “грязных” сетей маршрутизируется по умолчанию через сервер Cisco NAC, Пакеты обнаружения автоматически текут через Сервер. Трафик, описанный здесь, является одним из преимуществ к Методу VRF. Это обеспечивает последовательный, предсказуемый опыт. Посмотрите Потоки процессов NAC Cisco для получения дополнительной информации.

Шаг 22: веб-вход в систему

Выполните эти шаги для входа в систему через сеть:

1. Подключите клиентский компьютер с помощью одного из портов Edge, управляемых диспетчером Cisco NAC Manager.Клиентский компьютер размещен в не прошедшую поверку подлинности VLAN. Удостоверьтесь, что машина получает IP-адрес от не прошедшей поверку подлинности подсети VLAN.
2. Откройте браузер для выполнения входа в систему.Предположение - то, что этому клиентскому компьютеру не установили агента Cisco NAC уже. Если все Записи DNS перенаправлены к ненадежному интерфейсу сервера Cisco NAC, браузер автоматически перенаправляет к странице входа. Если это не делает, переходит к определенному URL, такому как guest.nac.local для выполнения входа в систему:

Рисунок 28 – ***веб-страница для входа***

Шаг 23: вход в систему агента

Можно распределить агента Cisco NAC точно так же, как любое другое программное приложение конечным пользователям, или можно вызвать его 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.

Эти данные показывают экран, который появляется, когда активирован агент:

Рисунок 29 – ***вход в систему агента***

1. Выберите сервер из выпадающего списка Server.
2. Ввести имя пользователя.
3. Ввести пароль.
4. **Щелкните "Регистрация в системе".**Рисунки 30 и 31 показывают экраны это appear:.**Рисунок 30 –** ***агент Cisco NAC, выполняющий IP, освобождает или возобновляет*** **Рисунок 31 –** ***агент Cisco NAC, указывающий на полный доступ к сети после обновления IP***
5. **Нажмите кнопку OK.**

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

Можно настроить диспетчера Cisco NAC Manager 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. Эти 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. Используйте этого сервисного IP 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.
- Чтобы гарантировать, что активный диспетчер Cisco NAC Manager всегда доступен, его доверяемый интерфейс (Eth0) должен быть подключен. Необходимо избежать ситуации, где Менеджер активен, но не доступен через ее доверяемый интерфейс. Если резервный Менеджер получает тактовые контрольные пакеты от активного Менеджера, но сбоев интерфейса Eth0 активного Менеджера, это условие происходит. 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 Высокой доступности Настройки.

Сервер Cisco NAC

Для обеспечивания защиты против единственного уязвимого звена можно настроить сервер Cisco NAC 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.

Эти 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 Высокой доступности Настройки.

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 к Единой точке входа Active Directory Настройки.

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 в Windows GINA канавки. 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 к Windows GPO Scripts и Совместимости NAC Cisco.

Настройте устройство Cisco NAC 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 к устройству Cisco NAC Настройки для Входа в систему Агента и Клиентской Оценки Положения.

Дополнительные сведения

- Страница технической поддержки устройства Cisco NAC
- Cisco Systems – техническая поддержка и документация