Руководство по проектированию уровня 3 NAC вне диапазона с использованием VRF-Lite для изоляции трафика

Содержание

Введение

Примечание: Сведения в этом документе могут измениться без предупреждения. Подтвердите все рекомендации, если это возможно.

Цель этого документа состоит в том, чтобы описать Облегченную VRF базирующуюся реализацию NAC в Уровне 3 Внеполосные (OOB) развертывания, где сервер NAC (CAS) настроен в Реальном IP-шлюзе (Направленный) режим. Внеполосный уровень 3 быстро стал одной из самых популярных методологий развертываний для NAC. Это переключается на нижний регистр, популярность основывается на нескольких движущих силах. Первым является лучшее использование аппаратных ресурсов. Развертываниями NAC в Уровне 3 методология OOB одиночное NAC-устройство может быть сделано 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 эффективен с точки зрения затрат и с точки зрения Капитала и Эксплуатационных расходов. Существует два широко используемых подхода для развертывания NAC в Уровне 3 архитектура OOB.

1. Базирующийся подход хоста обнаружения — Использует свойственную способность в

Агенте NAC для достижения Сервера NAC (CAS). ACL применились на осуществление контрольного трафика коммутатора доступа в сети Dirty. См. Соединение с Сервером NAC (CAS) с помощью протокола SWISS для получения дополнительной информации.

2. VRF базирующийся подход — Использует VRF для маршрутизации не прошедшего поверку подлинности трафика к CAS. Политика трафика, настроенная на сервере NAC (CAS), используется для осуществления в сети Dirty. Этот подход имеет два подподхода. В первом подходе VRF являются распространяющимися всюду по инфраструктуре, в этом случае все приборы слоя 3 участвуют в коммутации на основе тэгов. Второй подход использует Облегченный VRF и Туннели GRE для туннелирования VRF через приборы слоя 3, которые не понимают коммутацию на основе тэгов. Преимущество к второму подходу - то, что изменения минимальной настройки требуются, чтобы ваша центральная инфраструктура.

Примечание: В то время как Уровень 3, OOB является одной из наиболее распространенных методологий развертываний, это не может всегда быть оптимальное решение для каждой среды. Существуют другие опции для выбора из этого, может быть более оптимальное пригодное для конкретных требований. См. Планирование Ваших Развертываний для получения дополнительной информации об этих других проектных решениях NAC.

Предварительные условия

Требования

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

- Основное понимание операции инфраструктуры Уровня 2 и Уровня 3 и конфигурации
- Основное понимание устройства Cisco NAC и различия между различными методологиями внедрения, которые привязаны к нему
- Все развертывания NAC и дизайны должны основываться на ясных потребностях бизнеса. Это предположения потребности бизнеса для этой контрольной настройки:Пользователи должны аутентифицироваться до того чего предостав доступ к сети в целом.Ваш доступ ограничен на основе того, кто пользователи. Эти привилегии сопоставлены с Составом группы в Active Directory. Группы являются Гостями, Подрядчиками и Сотрудниками.На основе AD Состава группы пользователи размещены в VLAN, которая имеет Привилегии Доступа к сети, которые являются соответствующими каждой группе.Трафик Гостя продолжает быть изолированным от остатка сети даже после аутентификации.После того, как пользователя допускают в сеть, NAC-устройство больше не должно быть в пути трафика. Это препятствует тому, чтобы NAC-устройство стало узким местом, и позволяет сети использоваться к ее полному потенциалу проверенными пользователями.
- NAC имеет много возможностей, которые не покрыты этим документом. Цель этого руководства состоит в том, чтобы исследовать и задокументировать руководства по проектированию и конфигурацию, требуемую для Облегченного VRF базирующегося Уровня 3 Внеполосные развертывания NAC. Это руководство не фокусируется на Оценке Положения или Исправлении. Дополнительные сведения о NAC-устройстве и его полной мощности могут быть найдены в www. cisco . com/go/nac (только зарегистрированные клиенты).

Используемые компоненты

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

Условные обозначения

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

Настройка

Конфигурация инфраструктуры

Введение:

При считании Облегченного VRF базирующегося Уровня 3 развертываниями NAC OOB существует несколько принципов проектирования, которые очень важны для рассмотрения. Эти принципы перечислены здесь, и краткое обсуждение их важности включено.

1. **Классификация трафика и Разработка** — ключевое понятие, чтобы понять и помнить за этот тип дизайна NAC - то, что трафик, классифицированный как Грязный*, должен* течь в сторону UnTrusted Сервера NAC (CAS). Всегда поддерживайте эту принципиальную вершину ума во время дизайна реализации NAC. Кроме того, сетям Clean и Dirty нельзя позволить связаться непосредственно друг с другом. В Уровне 3 OOB разрабатывают с VRF, сервер NAC (CAS) действия как точка осуществления или контроллер, который гарантирует сегрегацию и безопасную связь между сетями Clean и Dirty.
2. **Изоляция трафика** — важно быть уверенным, что соответствующий механизм осуществления выбран для обеспечения трафика и изоляции пути для всего трафика, полученного от неаутентифицируемых и несанкционированных хостов. Облегченный VRF используется здесь для достижения полных данных и изоляции уровня управления (VRF).
3. **Централизованное Осуществление** — поскольку Облегченная VRF методология придерживается естественного выбора пути, созданного путем маршрутизации: изменения топологии, требования управления доступом и/или изменения адреса не создают потребность манипулировать ACL через инфраструктуру. При использовании Туннеля GRE в сочетании с Облегченным VRF это дает вам гибкость для отбрасывания грязного трафика прямо перед сервером NAC без потребности настроить множественные переходы. Облегченный VRF в сочетании с GRE только требуют конфигурации на Граничных приборах слоя 3. Это существенно уменьшает количество устройств, которое должно быть затронуто для обеспечения требования изоляции пути.
4. **Трудность** — Трудность реализации, а также постоянного обслуживания. При определении подхода, что вы, вероятно, будете использовать для Уровня 3 NAC OOB в своей сети, важно рассмотреть простоту реализации и продолжающихся эксплуатационных расходов и сложности реализации той технологии, особенно в

динамическом окружении.

Примечание: NAC-устройство не обращает внимания на то, как трафик представлен ему. Другими словами, само Устройство не имеет никакого предпочтения, поступает ли трафик через Туннель GRE или был перенаправлен через конфигурацию Маршрутизации на основе политик, VRF, Направленный и т.д.

Примечание: Для лучшей возможной производительности конечного пользователя не забудьте использовать сертификаты, которым доверяет браузер конечного пользователя. Использование Самогенерируемых сертификатов на Сервере NAC не рекомендуется для производственной среды.

Примечание: Всегда генерируйте сертификат для Сервера NAC с IP-адресом его Ненадежного интерфейса.

Рисунок виртуализации устройства с VRF может быть замечен здесь. Эта методология предоставляет Плоскость Уровня управления и Данных для изоляции пути.

Топология

Эта схема является представительной для топологии, используемой для создания этой бумаги. Внутренняя сеть направляет через Таблицу глобальной маршрутизации и не имеет никакого VRF, привязанного к ней. VRF DIRTY содержит только Dirty_VLAN и связанные транзитные сети, которые требуются, чтобы вынуждать весь источник данных от DIRTY_VLAN течь через Грязную Сторону NAC-устройств. Гостевой VRF содержит GUEST_VLAN и привязанные транзитные сети, требуемые завершать весь источник данных от GUEST_VLAN на отдельном Подчиненном интерфейсе на Межсетевом экране. Каждую из этих трех Виртуальных сетей несут на той же физической инфраструктуре и предоставляет завершенный трафик и соединяет изоляцию каналом соответственно.

Потоки процессов

Этот раздел показывает поток основного процесса того, что требуется, чтобы получать доступ к сети и с, и без агента установил. Эти потоки процессов макроаналитичны по своей природе и содержат только функциональные шаги решения. Они не включают каждую опцию или шаг, который происходит, и не включайте решения об авторизации, которые основываются на критериях оценки оконечной точки.

!--- конфигурацию

Сведения о конфигурации детализируют шаги, требуемые настраивать вашу сеть для изоляции пути с помощью VRF-Lite/GRE и конфигурации, требуемой для вставки NAC-устройства в сеть как Уровень 3 Реальный IP-шлюз OOB.

Примечание: Облегченный VRF функция, которая позволяет вам поддержать две или больше Виртуальных сети. Облегченный VRF также обеспечивает перекрывающиеся IP-адреса среди Виртуальных сетей. Но, 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.

Облегченные VRF входные интерфейсы использования для различения маршрутов для

других Виртуальных сетей и форм действительные таблицы пересылки пакетов путем соединения одного или более Интерфейсов уровня 3 к каждому VRF. Интерфейсы в VRF могут быть любой физическими, такими как Порты Ethernet; или логический, такие как подчиненные интерфейсы, Туннельные интерфейсы или SVI VLAN. Обратите внимание, что Интерфейс уровня 3 не может принадлежать нескольким VRF никогда.

Важные факторы для облегченного VRF

- Облегченный VRF является только локально значительным 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 доменами защиты, и все домены защиты имеют свои собственные уникальные таблицы маршрутизации.
- Облегченный VRF позволяет множественным Доменам защиты совместно использовать то же физическое соединение между сетевыми устройствами. Магистральные порты с несколько интерфейсов VLAN или Туннелями GRE предоставляют изоляцию трафика, которая разделяет пакеты от каждого другого домена защиты.
- Все домены защиты должны иметь свои собственные VLAN.
- Облегченный VRF не поддерживает всю функциональность VRF MPLS: маркируйте обмен, смежность LDP или помеченные пакеты.
- Ресурс TCAM Уровня 3 разделен между всеми VRF. Чтобы гарантировать, что любой VRF имеет достаточное пространство CAM, используйте **команду maximum routes**.
- Коммутатор Catalyst, использующий Облегченный VRF, может поддержать одну глобальную сеть и до 64 VRF. Общее число поддерживаемых маршрутов ограничено размером TCAM.
- Большинство протоколов маршрутизации (BGP, OSPF, EIGRP, RIP и статичная маршрутизация) может использоваться между устройствами, которые работают Облегченный VRF.
- Нет никакой потребности выполнить BGP с Облегченным VRF, пока вы не должны пропускать маршруты между VRF.
- Облегченный VRF не влияет на скорость коммутации пакетов.
- Групповая адресация и Облегченный VRF не может быть настроена на том же Интерфейсе уровня 3 в то же время.
- **Подкоманда capability vrf-lite** под **маршрутизатором ospf** должна использоваться при настройке OSPF как протокола маршрутизации между сетевыми устройствами.

Определение VRF

В Примере проектирования требования предоставляют изоляцию пути для обоих не прошедших поверку подлинности пользователей или пользователей DIRTY, а также ГОСТЕЙ. Всему другому трафику разрешают использовать внутреннюю сеть. Это требует определения двух VRF. Вот конфигурация:

```
!
ip vrf DIRTY
!--- 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
10:1 !--- 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). ! ip vrf GUESTS
description GUESTS_VRF_FOR_VISITORS rd 30:1 !
```

Привяжите VLAN или интерфейс с VRF

После того, как VRF был определен на Коммутаторе 3 уровня или маршрутизаторе, интерфейсы, которые участвуют в Облегченной VRF конфигурации, должны быть привязаны к VRF, которому они принадлежат. Как отмечалось ранее, или физический или виртуальные интерфейсы может быть привязан к VRF. Включенный примеры физического интерфейса, коммутируемого виртуального интерфейса, подчиненного интерфейса и туннельного интерфейса, которые привязаны к VRF.

```
!
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
!
interface FastEthernet3/1.10
encapsulation dot1Q 10
ip vrf forwarding DIRTY
ip address 192.168.10.1 255.255.255.252
!
interface Vlan100
ip vrf forwarding DIRTY
ip address 192.168.100.1 255.255.255.0
!
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 VRF между двумя устройствами

Существует несколько приемлемых методологий для extenion VRF между двумя частями инфраструктуры. Метод, который вы выбираете, должен основываться на этом критерии:

1. Возможности Платформы — В отношении возможностей платформы, весь текущий Уровень 3 Cisco способная Коммутация Предприятия и Облегченная VRF поддержка Платформ маршрутизации. Это включает, но не ограничено Catalyst 6500, 4500, 3750, и 3560 платформ.
2. Любая платформа маршрутизации, которая выполняет соответствующий Cisco IOS®, которые включают, но не ограничены 7600, 3800, 2800, 1800, и ISR серии 800.
3. Количество Переходов Уровня 3 Между Соответствующими Частями Инфраструктуры — Определение количества переходов Уровня 3 важно для хранения развертываний максимально простыми. Например, если было пять переходов Уровня 3 между инфраструктурой, которые размещают устройства CAS и клиентов, она может создать административную служебную информацию.

С неправильным решением:

1. Транкинг уровня 2 создает очень субоптимальную топологию Уровня 2.
2. Подчиненные интерфейсы уровня 3 создают много дополнительных интерфейсов для настройки. В результате это может создать дополнительную служебную информацию управления и потенциальные проблемы IP-адресации. Это проиллюстрировано в схеме. Если вы предполагаете, что нет никакого резервирования в инфраструктуре, каждый Уровень показанной Сети имеют и входной и выходной физический интерфейс. Вычисление для количества подчиненных интерфейсов тогда (2 * количество уровней в сети * (количество VRF)). В данном примере существует два VRF, таким образом, формула ((2*5) *2) или 20 Подчиненных интерфейсов. Как только резервирование добавлено, этот номер более чем удваивается. Сравните это с расширением GRE, где только четыре интерфейса требуются с тем же конечным результатом. Это иллюстрирует явно, как GRE существенно уменьшает влияние конфигурации.

Транкинг уровня 2

Транкинг уровня 2 предпочтен в сценариях, где помещения Уровня 3 не развернуты или где Сетевые устройства не поддерживают GRE или Подчиненные интерфейсы. Нужно обратить внимание, что Catalyst 3560, 3750 и 4500 платформ не поддерживают Подчиненные интерфейсы. Catalyst 3560, и 3750 также не поддерживает GRE. Catalyst 4500 поддерживает GRE в программном обеспечении, и Catalyst 6500 поддерживает GRE в аппаратных средствах.

В модели помещения Уровня 3, где вы подключаете платформу, которая не поддерживает Подчиненные интерфейсы или GRE к платформе, которая делает, это предпочтено, чтобы только использовать транкинг Уровня 2 на одной стороне и использовать Подчиненные интерфейсы с другой стороны. Это позволяет вам поддерживать все преимущества архитектуры помещения Уровня 3, и все еще преодолевать ограничение никакого GRE или поддержки Подчиненного интерфейса на некоторых платформах. Одно из основных преимуществ конфигурации Уровня 2, соединяющего магистралью только на одной стороне ссылки, - то, что Связующее дерево не введено назад в среду Уровня 3. Посмотрите пример, где 3750 Коммутаторов доступа (Никакой GRE или Поддержка Подчиненного интерфейса) связаны с 6500 Коммутаторами распределения, которые действительно поддерживают GRE и Подчиненные интерфейсы.

3750 соответствующих конфигураций:

В этой конфигурации обратите внимание, что на FastEthernet 1/0/1 настройка по умолчанию для СОБСТВЕННОГО VLAN является VLAN 1. Эта конфигурация не была изменена. Вы также замечаете, однако, что VLAN 1 не позволяют быть соединенным магистралью через ссылку. Позволенный VLANs ограничен только VLANS, которые помечены. Поскольку в этой топологии Уровня 3 нет никакой потребности в согласовании магистрали или трафика VTP для движения от коммутатора до коммутатора, нет также никакой потребности в неинкапсулированном трафике для передавания транзитом этой ссылки. Эта конфигурация увеличивает положение безопасности архитектуры начиная с него, doesn не открывают ненужные дыры безопасности уровня 2.

```
!
ip vrf DIRTY
description DIRTY_VRF_FOR_NAC
rd 10:1
!
```

```
ip vrf GUESTS
description GUESTS_VRF_FOR_VISITORS
rd 30:1
!
!
interface FastEthernet1/0/1
description CONNECTION_TO_DISTRIBUTION_6504
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10,20,30
switchport mode trunk
speed 100
duplex full
!
!
interface Vlan10
description DIRTY_VRF_TRANSIT
ip vrf forwarding DIRTY
ip address 192.168.10.2 255.255.255.252
!
interface Vlan20
description CLEAN_TRANSIT
ip address 192.168.20.2 255.255.255.252
!
interface Vlan30
description GUESTS_VRF_TRANSIT
ip vrf forwarding GUESTS
ip address 192.168.30.2 255.255.255.252
!
```

6500 соответствующих конфигураций:

В этой конфигурации обратите внимание, что инкапсуляция dot1q используется, и кадры с VLAN 10, 20 и 30 помечены. При выборе тегов VLAN для использования, вы не можете использовать номер виртуальной локальной сети (VLAN), который уже определен локально в Базе данных VLAN на коммутаторе.

```
!
ip vrf DIRTY
description DIRTY_VRF_FOR_NAC
rd 10:1
!
ip vrf GUESTS
description GUESTS_VRF_FOR_VISITORS
rd 30:1
!
interface FastEthernet3/1
description CONNECTION_TO_3750_ACCESS
no ip address
speed 100
duplex full
!
!
interface FastEthernet3/1.10
description DIRTY_VRF_TRANSIT
encapsulation dot1Q 10
ip vrf forwarding DIRTY
ip address 192.168.10.1 255.255.255.252
!
interface FastEthernet3/1.20
description CLEAN_TRANSIT
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.252
```

```
!
interface FastEthernet3/1.30
description GUESTS_VRF_TRANSIT
encapsulation dot1Q 30
ip vrf forwarding GUESTS
ip address 192.168.30.1 255.255.255.252
!
```

Подчиненные интерфейсы уровня 3

Когда только необходимо расширить VRF по одному Переходу Уровня 3 в сети, подчиненные интерфейсы уровня 3 являются хорошей опцией. Или GRE или Подчиненные интерфейсы могут быть выбраны на основе вашего удобства с каждой конфигурацией. Это - пример конфигурации для Подчиненного интерфейса Уровня 3:

```
!
interface FastEthernet3/1
description CONNECTION_TO_3750_ACCESS
no ip address
speed 100
duplex full
!
!
interface FastEthernet3/1.10
description DIRTY_VRF_TRANSIT
encapsulation dot1Q 10
ip vrf forwarding DIRTY
ip address 192.168.10.1 255.255.255.252
!
```

Туннели GRE

Туннели GRE являются предпочтительным способом для расширения Облегченного VRF VRF, когда там являются многоуровневыми 3 перехода между клиентами, которые должны обратиться к VRF. Этот тип дизайна более распространен с удаленным NAC филиала компании, где удаленные клиенты хотят обратиться к расположенному в центре серверу NAC. Например, в типичном Ядре, Распределении, клиенты модели Доступа к сети непосредственно не связаны с Дистрибутивами или с Ядром. Поэтому нет никакой потребности добавить сложность VRF definition на Распределении или Основных устройствах. GRE может использоваться для простой передачи трафика, который должен быть изолирован к точке в Сети, где связаны серверы NAC. Это - пример Туннельного интерфейса GRE.

```
!
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
!
```

Маршрутизация Настройки для VRF

Как обсуждено ранее в документе, Облегченном VRF BGP поддержек, OSPF и EIGRP. В этом примере конфигурации выбран EIGRP, потому что это, как правило, - Cisco, рекомендуемая протокол маршрутизации, внедренный на Сетях уровня кампуса, где

требуется быстрая конвергенция.

На это нужно обратить внимание, тот OSPF работает одинаково хорошо с Облегченным VRF, как делает BGP.

Нужно также обратить внимание, что, если дизайн требует, чтобы трафик был пропущен между VRF, тогда требуется BGP.

Это - пример конфигурации Маршрутизации для VRF с EIGRP.

```
!
!--- As with any configuration this is base routing
protocol !--- configuration which handles the routing
for the Global Routing Table. router eigrp 1 network
192.168.20.0 0.0.0.3 network 192.168.21.0 network
192.168.22.0 network 192.168.28.0 0.0.0.3 network
192.168.29.0 0.0.0.3 network 192.168.254.1 0.0.0.0 no
auto-summary ! !--- An Address Family must be defined
for each VRF !--- that is to be routing through the
routing protocol. !--- Routing Protocol options such as
auto-summarization, !--- autonomous system number,
router id, and so forth are all !--- configured under
the address family. Note that EIGRP does not !---
neighbor without the autonomous system specified under
!--- the address family. Also note, that this autonomous
system !--- number should be unique for each VRF and
should not be !--- the same as the Global AS number. !
address-family ipv4 vrf GUESTS network 192.168.30.0
0.0.0.3 network 192.168.38.0 0.0.0.3 no auto-summary
autonomous-system 30 exit-address-family ! address-
family ipv4 vrf DIRTY network 192.168.10.0 0.0.0.3
network 192.168.11.0 no auto-summary autonomous-system
10 exit-address-family !
```

Маршрутизация трафика между таблицей глобальной маршрутизации и грязным VRF

Это зависит от требований развертываний NAC, если 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 NAC-устройства. В случае развертываний Единой точки входа Active Directory необходимо передать подмножество трафика к Active Directory для разрешения Интерактивных Входов в систему, Exchange билета Kerberos, и т.д. При любых обстоятельствах очень важно, чтобы Таблица глобальной маршрутизации знала, как достигнуть Грязного VRF, и что VRF DIRTY знает, как достигнуть Таблицы глобальной маршрутизации, если какие-либо данные должны пройти между двумя. Это, как правило, обрабатывается этой методологией.

Грязные настройки по умолчанию VRF к Недоверяемому или Грязному интерфейсу NAC-устройства. Глобальный имеет Статические маршруты *только* к подсетям, которые считают VLAN DIRTY.

Рассмотрите этот рисунок.

Первый переход Уровня 3 на Недоверяемой или Грязной стороне NAC-устройства перераспределяет маршрут по умолчанию в процесс маршрутизации, который указывает к NAC-устройству. Первый переход Уровня 3 на Доверяемой или Чистой стороне NAC-устройства перераспределяет статический маршрут для подсети, которая принадлежит

VLAN 100, который в этом случае является 192.168.100.0/24.

Примечание: Первый переход Уровня 3 на противоположных сторонах NAC-устройства может быть на том же физическом устройстве, но в других VRF. В то время как Доверяемая или Чистая сторона NAC-устройства остается в Таблице глобальной маршрутизации, в следующем примере Недоверяемая или Грязная сторона сервера NAC находится в VRF.

Конфигурация приведена ниже:

```
!
router eigrp 1
 redistribute static
 network 192.168.20.0 0.0.0.3
 network 192.168.21.0
 network 192.168.22.0
 network 192.168.28.0 0.0.0.3
 network 192.168.29.0 0.0.0.3
 network 192.168.254.1 0.0.0.0
 no auto-summary
 !
 address-family ipv4 vrf GUESTS
  network 192.168.30.0 0.0.0.3
  network 192.168.38.0 0.0.0.3
  no auto-summary
  autonomous-system 30
 exit-address-family
 !
 address-family ipv4 vrf DIRTY
  redistribute static
  network 192.168.10.0 0.0.0.3
  network 192.168.11.0
  no default-information out
  no auto-summary
  autonomous-system 10
 exit-address-family
!
ip classless
ip route 192.168.100.0 255.255.255.0 192.168.21.10
ip route vrf DIRTY 0.0.0.0 0.0.0.0 192.168.11.2
!
!!
```

Конфигурация NAC для уровня 3 OOB

Настройка CAS

Помните наш принцип номера один от раздела Введения: Прием к успешному дизайну NAC должен всегда помнить, что трафик, классифицированный как Грязный*, должен* течь в сторону UnTrusted Сервера NAC (CAS).

В первом снимке экрана обратите внимание на настройку Сети сервера NAC. Вы замечаете, что Сервер развернут как Внеполосный Реальный IP-шлюз. Обратите внимание на то, что маршрут по умолчанию Сервера NAC указан ДОВЕРЯЕМОЙ стороне.

Сервер должен быть настроен со Статическими маршрутами для каждого VLANS DIRTY, которые существуют на НЕДОВЕРЯЕМОЙ стороне. См. второй снимок экрана.

Проверка

Найдите задокументированный процесс пользователя `NAC-Employee`, входящим в нашу сеть. Cisco перехватила действие от Коммутатора доступа, рабочей станции, и показывает информацию от таблиц маршрутизации Коммутаторов распределения.

Этот раздел позволяет убедиться, что конфигурация работает правильно.

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

Этап 1 — Вы еще не соединились с сетью, и порт коммутатора на Коммутаторе доступа не работает.

```
! – Catalyst 3750 Access Switch
!--- Note: Client mahcine is off the network at this
point. ! 3750-Access#show int status | i Fa1/0/13
Fa1/0/13 CLIENT_CONNECTION notconnect 100 auto auto
10/100BaseTX ! ! 3750-Access#!Notice it is in the
"notconnect" state. !
```

Этап 2 — Windows - клиент включает сеть, и начальной VLAN на Коммутаторе является VLAN 100 (Грязная VLAN). IP-адрес назначен на хост, как вы видите в этом снимке экрана.

```
! – Catalyst 3750 Access Switch
!--- Note: Client just connected to the network. 2w5d:
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100,
changed state to up 2w5d: %LINK-3-UPDOWN: Interface
FastEthernet1/0/13, changed state to up 2w5d:
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet1/0/13, changed state to up ! ! 3750-
Access#show int status | i Fa1/0/13 Fa1/0/13
CLIENT_CONNECTION connected 100 a-full a-100
10/100BaseTX !
```

Этап 3 — В течение нескольких секунд, Агент NAC начинает его процесс входа в систему. В данном примере настроена Единая точка входа Active Directory, таким образом, вам не предлагают для имени пользователя и пароля. Вместо этого вы видите всплывающее окно, которое описывает, что происходит Единая точка входа.

После того, как Оценка Аутентификации и Положения была завершена, Сообщение об успешном завершении отображено, порт коммутатора перемещен от Грязной VLAN до VLAN Сотрудника и Агента NAC refreshs IP-адрес ПК.

```
! – Catalyst 3750 Access Switch
2w5d: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Vlan100, changed state to down
2w5d: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Vlan200, changed state to up
!
!--- Note: As you can tell from the previous messages,
!--- the switchport was just moved from VLAN 100 to VLAN
200. ! 3750-Access#show int status | i Fa1/0/13 Fa1/0/13
CLIENT_CONNECTION connected 200 a-full a-100
10/100BaseTX ! !
```

Этот снимок экрана показывает Заключительный IP-адрес, который находится в VLAN Сотрудника (VLAN 200).

Этот снимок экрана показывает устройство пользователя Сотрудника NAC, как перечислено в Списке Сертифицированных устройств. Роль назначена на *EMPLOYEES*, и VLAN 200.

Этот снимок экрана показывает список Подключенных пользователей на Менеджере NAC.

Это - Менеджер NAC журнал событий, который показывает успешную регистрацию в системе внеполосного пользователя.

В этом разделе исследованы таблицы маршрутизации Глобальной Таблицы маршрутизации и VRF DIRTY. В первом снимке экрана обратите внимание **на команду show ip route**. Это указывает на наблюдение таблицы маршрутизации для Глобальных Маршрутов.

```
6504-DISTRIBUTION#show ip route Codes: C - connected, S
- static, R - RIP, M - mobile, B - BGP D - EIGRP, EX -
EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF
NSSA external type 1, N2 - OSPF NSSA external type 2 E1
- OSPF external type 1, E2 - OSPF external type 2 i -
IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-
IS level-2 ia - IS-IS inter area, * - candidate default,
U - per-user static route o - ODR, P - periodic
downloaded static route Gateway of last resort is
192.168.28.2 to network 0.0.0.0 192.168.29.0/30 is
subnetted, 1 subnets D 192.168.29.0 [90/30720] via
192.168.28.2, 2w5d, FastEthernet3/48 192.168.28.0/30 is
subnetted, 1 subnets C 192.168.28.0 is directly
connected, FastEthernet3/48 D EX 192.168.31.0/24
[170/30976] via 192.168.28.2, 2w5d, FastEthernet3/48 D
EX 192.168.30.0/24 [170/30976] via 192.168.28.2, 2w5d,
FastEthernet3/48 D 192.168.200.0/24 [90/28416] via
192.168.20.2, 6d19h, FastEthernet3/1.20 D EX
192.168.38.0/24 [170/30976] via 192.168.28.2, 2w5d,
FastEthernet3/48 C 192.168.21.0/24 is directly
connected, Vlan21 D EX 192.168.39.0/24 [170/30976] via
192.168.28.2, 2w5d, FastEthernet3/48 192.168.20.0/30 is
subnetted, 1 subnets C 192.168.20.0 is directly
connected, FastEthernet3/1.20 D EX 192.168.36.0/24
[170/30976] via 192.168.28.2, 2w5d, FastEthernet3/48 C
192.168.22.0/24 is directly connected, Vlan22 D EX
192.168.37.0/24 [170/30976] via 192.168.28.2, 2w5d,
FastEthernet3/48 D EX 192.168.34.0/24 [170/30976] via
192.168.28.2, 2w5d, FastEthernet3/48 192.168.254.0/32 is
subnetted, 3 subnets D 192.168.254.2 [90/156160] via
192.168.20.2, 2w5d, FastEthernet3/1.20 D 192.168.254.3
[90/156160] via 192.168.28.2, 2w5d, FastEthernet3/48 C
192.168.254.1 is directly connected, Loopback0 D EX
192.168.35.0/24 [170/30976] via 192.168.28.2, 2w5d,
FastEthernet3/48 D EX 192.168.32.0/24 [170/30976] via
192.168.28.2, 2w5d, FastEthernet3/48 S 192.168.100.0/24
[1/0] via 192.168.21.10 D EX 192.168.33.0/24 [170/30976]
via 192.168.28.2, 2w5d, FastEthernet3/48 D*EX 0.0.0.0/0
[170/30976] via 192.168.28.2, 2w5d, FastEthernet3/48
```

Примечание: 192.168.100.0/24 сеть (Грязная Сеть) находится в таблице маршрутизации как статический маршрут со следующим переходом, являющимся Доверяемым Интерфейсом Сервера NAC.

Обратите внимание **на команду show ip route vrf DIRTY**. Это указывает на наблюдение таблицы маршрутизации для виртуальной сети DIRTY только.

```
6504-DISTRIBUTION#show ip route vrf DIRTY Routing Table:
DIRTY Codes: C - connected, S - static, R - RIP, M -
mobile, B - BGP D - EIGRP, EX - EIGRP external, O -
OSPF, IA - OSPF inter area N1 - OSPF NSSA external type
1, N2 - OSPF NSSA external type 2 E1 - OSPF external
type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS
summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-
IS inter area, * - candidate default, U - per-user
static route o - ODR, P - periodic downloaded static
route Gateway of last resort is 192.168.11.2 to network
0.0.0.0 192.168.10.0/30 is subnetted, 1 subnets C
192.168.10.0 is directly connected, FastEthernet3/1.10 C
192.168.11.0/24 is directly connected, Vlan11 D
192.168.100.0/24 [90/28416] via 192.168.10.2, 01:03:19,
FastEthernet3/1.10 S* 0.0.0.0/0 [1/0] via 192.168.11.2
```

Примечание: Обратите внимание, что Грязная VLAN Доступа (192.168.100.0/24) изучена в распределении через EIGRP от 3750 Коммутаторов доступа, только в таблице маршрутизации VRF DIRTY. Этот маршрут не существует в Глобальной таблице.

Приложение A: Конфигурации коммутаторов

Рабочая конфигурация коммутатора доступа

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 3750-Access
!
!
no aaa new-model
clock timezone EST -5
clock summer-time EST recurring
switch 1 provision ws-c3750-24ts
ip subnet-zero
ip routing
!
ip vrf DIRTY
 description DIRTY_VRF_FOR_NAC
 rd 10:1
!
ip vrf GUESTS
 description GUESTS_VRF_FOR_VISITORS
 rd 30:1
!
!
!
crypto pki trustpoint TP-self-signed-819048320
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-819048320
 revocation-check none
 rsakeypair TP-self-signed-819048320
!
!
crypto ca certificate chain TP-self-signed-819048320
 certificate self-signed 01
```

```
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface Loopback0
 ip address 192.168.254.2 255.255.255.255
!

!
interface FastEthernet1/0/1
 description CONNECTION_TO_DISTRIBUTION_6504
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
 speed 100
 duplex full
!
interface range FastEthernet1/0/2 - 24
 description CLIENT_CONNECTION
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
!- SNIP -
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 description DIRTY_VRF_TRANSMIT
 ip vrf forwarding DIRTY
 ip address 192.168.10.2 255.255.255.252
!
interface Vlan20
 description CLEAN_TRANSIT
 ip address 192.168.20.2 255.255.255.252
!
interface Vlan30
 description GUESTS_TRANSIT
 ip vrf forwarding GUESTS
 ip address 192.168.30.2 255.255.255.252
!
interface Vlan100
 description DIRTY_VLAN
 ip vrf forwarding DIRTY
 ip address 192.168.100.1 255.255.255.0
 ip helper-address 192.168.22.11
!
interface Vlan200
 description EMPLOYEES_VLAN
 ip address 192.168.200.1 255.255.255.0
 ip helper-address 192.168.22.11
!
interface Vlan210
 description CONTRACTORS_VLAN
 ip address 192.168.210.1 255.255.255.0
 ip helper-address 192.168.22.11
```

```
!

!
interface Vlan300
 description GUESTS
 ip vrf forwarding GUESTS
 ip address 192.168.31.1 255.255.255.0
!
router eigrp 1
 network 192.168.20.0 0.0.0.3
 network 192.168.200.0
 network 192.168.254.2 0.0.0.0
 no auto-summary
 !
 address-family ipv4 vrf GUESTS
 network 192.168.30.0 0.0.0.3
 network 192.168.31.0
 no auto-summary
 autonomous-system 30
 exit-address-family
 !
 address-family ipv4 vrf DIRTY
 network 192.168.10.0 0.0.0.3
 network 192.168.100.0
 no auto-summary
 autonomous-system 10
 exit-address-family
!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.254.3 remote-as 1
 neighbor 192.168.254.3 update-source Loopback0
 no auto-summary
!
ip classless
ip route 192.0.2.1 255.255.255.255 Null0
ip http server
ip http secure-server
!
!
snmp-server community NIC-NAC-PADDYWHACK RW
snmp-server user NIC-NAC-PADDYWHACK NIC-NAC-PADDYWHACK
v1
snmp-server user NIC-NAC-PADDYWHACK NIC-NAC-PADDYWHACK
v2c
snmp-server trap-source Loopback0
snmp-server host 192.168.22.5 version 2c NIC-NAC-
PADDYWHACK
!
!- SNIP
!
ntp clock-period 36028450
ntp source Loopback0
ntp server 192.168.254.1 version 2 prefer
end
```

Рабочая конфигурация коммутатора распределения

```
!– SNIP -
!
hostname 6504-DISTRIBUTION
```

```
!
boot-start-marker
boot system disk0:s72033-advipservicesk9_wan-mz.122-
33.SXH2a.bin
boot-end-marker
!
!
no aaa new-model
clock timezone EST -5
clock summer-time EST recurring
!
!- SNIP -
!
ip vrf DIRTY
 description DIRTY_VRF_FOR_NAC
 rd 10:1
!
ip vrf GUESTS
 description GUESTS_VRF_FOR_VISITORS
 rd 30:1
!
ipv6 mfib hardware-switching replication-mode ingress
vtp domain cmpd
vtp mode transparent
no mls acl tcam share-global
mls netflow interface
no mls flow ip
no mls flow ipv6
mls cef error action freeze
!
!
redundancy
 keepalive-enable
 mode sso
 main-cpu
  auto-sync running-config
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
!
!

!
vlan 11
 name CAS_DIRTY
!
vlan 21
 name CAS_CLEAN
!
vlan 22
 name SERVER_VLAN
!
interface Tunnel0
 ip vrf forwarding GUESTS
 ip address 192.168.38.1 255.255.255.252
 tunnel source Loopback0
 tunnel destination 192.168.254.3
!
```

```
interface Loopback0
 ip address 192.168.254.1 255.255.255.255
!
!- SNIP -
!
interface FastEthernet3/1
 description CONNECTION_TO_3750_ACCESS
 no ip address
 speed 100
 duplex full
!
interface FastEthernet3/1.10
 description DIRTY_VRF_TRANSIT
 encapsulation dot1Q 10
 ip vrf forwarding DIRTY
 ip address 192.168.10.1 255.255.255.252
 ip verify unicast source reachable-via rx allow-default
!
interface FastEthernet3/1.20
 description CLEAN_TRANSIT
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.252
!
interface FastEthernet3/1.30
 description GUESTS_TRANSIT
 encapsulation dot1Q 30
 ip vrf forwarding GUESTS
 ip address 192.168.30.1 255.255.255.252
!
!
!
!

!
interface FastEthernet3/2
 description CAS1_DIRTY
 switchport
 switchport access vlan 11
 switchport mode access
 speed 100
 duplex full
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet3/3
 description CAS2_DIRTY
 switchport
 switchport access vlan 11
 switchport mode access
 speed 100
 duplex full
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet3/4
 description CAS1_CLEAN
 switchport
 switchport access vlan 21
 switchport mode access
 speed 100
 duplex full
 spanning-tree portfast
 spanning-tree bpduguard enable
!
```

```
interface FastEthernet3/5
 description CAS2_CLEAN
 switchport
 switchport access vlan 21
 switchport mode access
 speed 100
 duplex full
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet3/6
 description CAM
 switchport
 switchport access vlan 22
 switchport mode access
 speed 100
 duplex full
 spanning-tree portfast
 spanning-tree bpduguard enable
!
!
!- SNIP -
!
!

!
interface FastEthernet3/48
 description CONNECTION_TO_THE_WORLD
 ip address 192.168.28.1 255.255.255.252
 speed 100
 duplex full
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan11
 description NAC_DIRTY
 ip vrf forwarding DIRTY
 ip address 192.168.11.1 255.255.255.0
!
interface Vlan21
 description NAC_CLEAN
 ip address 192.168.21.1 255.255.255.0
!
interface Vlan22
 description SERVER_VLAN
 ip address 192.168.22.1 255.255.255.0
!
router eigrp 1
 redistribute static
 network 192.168.20.0 0.0.0.3
 network 192.168.21.0
 network 192.168.22.0
 network 192.168.28.0 0.0.0.3
 network 192.168.29.0 0.0.0.3
 network 192.168.254.1 0.0.0.0
 no auto-summary
 !
 address-family ipv4 vrf GUESTS
  network 192.168.30.0 0.0.0.3
  network 192.168.38.0 0.0.0.3
  no auto-summary
  autonomous-system 30
```

```
 exit-address-family
 !
 address-family ipv4 vrf DIRTY
  redistribute static
  network 192.168.10.0 0.0.0.3
  network 192.168.11.0
  no default-information out
  no auto-summary
  autonomous-system 10
 exit-address-family
!
!
!
!
!

!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.254.3 remote-as 1
 neighbor 192.168.254.3 update-source Loopback0
 no auto-summary
!
ip classless
ip route 192.0.2.1 255.255.255.255 Null0
ip route 192.168.100.0 255.255.255.0 192.168.21.10
ip route vrf DIRTY 0.0.0.0 0.0.0.0 192.168.11.2
!
!
!- SNIP -
!
ntp source Loopback0
ntp master 2
!
end
```

Устранение неполадок

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

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация