Руководство по настройке прифилировщика NAC и системы сбора данных NAC SERVER в уровне 3 вне диапазона

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Условные обозначения
Обзор профилировщика NAC
Обзор NAC
Обзор руководства по развертыванию
!--- конфигурацию
Настройте профилировщика NAC в уровне 3 топология OOB
Настройте модули коллектора NAC на сервере NAC
Настройте Коммутатор Удаленного доступа для передачи Trap-сообщений SNMP к Коллектору NAC
Настройте удаленный доступ, включают профилировщика для сбора сведений SNMP
Настройте маршрутизатор удаленного доступа на профилировщике для сбора сведений SNMP
Настройте Коллекторы NAC для Получения Трафика SPAN на их Локальных коммутаторах
Настройте маршрутизатор удаленного доступа для передачи данных NetFlow к коллектору в центральном узле
Проверка
Устранение неполадок
Процедура устранения неполадок
Дополнительные сведения

Введение

Этот документ описывает, как внедрить Профилировщика NAC и Коллекторы СЕРВЕРА NAC в Уровне 3 Внеполосные развертывания. Если вы развертываете Сервер NAC в Высокой доступности (HA), то только один Коллектор активен, и другой находится в состоянии готовности. Если вы не делаете HA, можно добавить каждый Коллектор в Профилировщике отдельно и иметь оба Сервера NAC, выполненные как Коллекторы. Это руководство размышляет над Размещением сервера HA.

Предварительные условия

Требования

Требования этого руководства - то, что вы настроили своего Менеджера NAC, Сервер NAC, Профилировщика NAC и Инфраструктуру сети согласно установке и руководствам по конфигурации для каждого продукта.

Используемые компоненты

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

- Менеджер NAC
- Сервер NAC
- Профилировщик NAC
- 3750 коммутаторов распределения
- 3750 удаленных коммутаторов доступа узла
- 2800 маршрутизаторов удаленного сайта
- 3800 маршрутизаторов распределения

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

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

Обзор профилировщика NAC

Cisco NAC Profiler позволяет администраторам сети эффективно развернуть и управлять Network Admission Control (NAC) в корпоративных сетях переменного масштаба и сложности с идентификацией, местоположением и определением возможностей всех оконечных точек подключенной сети, независимо от типа устройства, чтобы гарантировать и поддержать соответствующий доступ к сети. Cisco NAC Profiler является бессубъектной системой, которая обнаруживает, каталоги, и представляет все оконечные точки, связанные с сетью.

Обзор NAC

Система контроля доступа к сети Cisco NAC (NAC) Устройство, которое также известно как Cisco Clean Access, является мощным, простым в использовании контролем доступа и решением для осуществления соответствия. С функциями универсальной безопасности, внутриполосными или внеполосными параметрами развертывания, программными средствами проверки подлинности пользователя, и пропускной способностью и средствами управления за фильтрацией трафика, устройство Cisco NAC является полным решением контроля и защищенных сетей. Как центральная точка управления доступом для вашей сети, устройство Cisco NAC позволяет вам внедрить безопасность, доступ и политику соответствия в одном месте вместо потребности распространиться политику всюду по сети на многих устройствах.

Обзор руководства по развертыванию

На рисунке 1 существуют простые удаленные развертывания узла с центральными Серверами NAC HA, которые действуют как точка осуществления для Уровня 3 Внеполосные устройства. Профилировщик NAC и Менеджер NAC находятся на той же сети управления и передают и получают информацию от Серверов и Коллекторов. Существует также отдельный сборщик, который захватывает существенные сведения DHCP об устройствах через SPAN в ЦОД или магистральном уровне. Существует несколько способов обнаружить удаленные оконечные точки, и это руководство может помочь вам в ваших развертываниях. Это не предназначено, чтобы быть обязательным руководством, но показывает вам, как каждый модуль на коллекторах может использоваться и как данные оконечной точки, как замечает Профилировщик, принимают Копировальные решения для вас.

Список обязательных и дополнительных программных средств, что предоставлено использование Коллекторов Сервера NAC.

Обязательные модули коллектора

NetTrap — Этот модуль прислушивается к trap-сообщениям SNMP, передаваемым коммутаторами за уведомлением нового Mac или Соединением / Выключенные уведомления. Этот модуль передает все новые MAC-адреса Профилировщику для профилирования. Эта функция определена на, включают линию команды настройки SNMP-Server на Cisco IOS®.

NetMap — Этот модуль находится на Коллекторе и ответственен за то, что сделал Последовательный опрос SNMP устройств в удаленном ответвлении во временных интервалах. В схеме рисунка 1 SNMP Коллектора CAS1a опрашивает удаленный коммутатор и маршрутизатор для определенной информации MIB с доступом для чтения к коммутатору. Этот опрос предоставляет вещи как mac-address к сведениям о портах, интерфейсам, статусу соединения, информации о dot1x, сведения о системе и т.д.

NetWatch (SPAN) — Модуль NetWatch может слушать на Порте SPAN коммутатора и передать поглощенную информацию о потоке данных обратно Профилировщику. Сервер NAC требует, чтобы дополнительный интерфейс на каждом СЕРВЕРЕ NAC собрал данные. Это важно, потому что Профилировщик базируется прежде всего на сведениях DHCP, которые передают устройства и некоторое другое соответствие трафика приложения.

Дополнительные модули коллектора

Можно использовать SPAN или Netflow. Это до развертываний и требований заказчиков, но каждому только рекомендуют на Сервере NAC на сумму трафика, который передается Модулям Коллектора и другой функциональности NAC, которую должен выполнить Сервер NAC. Вы также теряете более жизненные информационные части об устройствах с Netflow как информация поставщика DHCP, назначения URL, информация Web - клиента, информация Web-сервера и т.д.

NetRelay — (Netflow) настроен на каждом маршрутизаторе на на интерфейсное основание, и назначение является управлением IP-адресами СЕРВЕРА NAC. Агент Netflow находится на СЕРВЕРЕ NAC и анализирует Данные NetFlow на основе ваших правил передачи трафика и сетей, настроенных на Профилировщике.

NetInquiry — Это - пассивный и активный механизм на основе ваших вещей как Открытые порты TCP. Например, СЕРВЕР NAC делает SYN/ACK и затем отбрасывает соединение для опроса диапазона конкретной подсети или диапазонов для открытых портов TCP. Если существует ответ, он передает информацию Профилировщику с IP-адресом и опрошенным портом TCP.

Примечание: Для NetInquiry только добавьте определенные подсети или хосты, которые не могут быть достигнуты или замечены с Netflow или NetWatch. NetInquiry может перегрузить ваш Сервер NAC с дополнительной обработкой и аппаратными ресурсами как память и загрузка ЦПУ если не настроенный должным образом. Используйте эту функцию как последнее прибежище.

Примечание: Если у вас есть отдельный сборщик, можно включить и Netflow и SPAN на том же устройстве, но удостовериться, что не превысили намеченную сумму Коллектора.

Рисунок 1

!--- конфигурацию

Настройте профилировщика NAC в уровне 3 топология OOB

- Серверы NAC должны быть настроены через обычный NAC, HA устанавливают.
- Коллектор NAC использует Виртуальный IP - адрес сервера NAC для передачи с Профилировщиком.
- Коллектор NAC HA пара добавлена как одиночная запись в Профилировщике и связывается с виртуальным IP - адресом CAS.

Рис. 2

Настройка конфигурации

Выполните следующие действия:

1. Профилировщику нужно *Клиентское соединение* для новых Коллекторов NAC.
2. Профилировщику нужно *Подключение к серверу* для отдельного устройства, которое находится близко к distribution|data center|services уровень в схеме сети.
3. Выберите **Configuration> NAC Profiler Modules – Модули Профилировщика NAC Списка** и затем нажмите **вкладку Server**.Перейдите к концу страницы и **нажмите Add Соединение**.**Рис. 3**
4. Введите IP-адрес сервиса и информацию о секретном ключе Коллектора HA и **нажмите Add Соединение**.**Рис. 4**
5. **Нажмите Add соединение** снова.**Рис. 5 Рис. 6**
6. Введите **IP-адрес** для настройки *Подключения к серверу*, с которым соединяется Отдельный сборщик.
7. Нажмите **Edit Connection**, когда вы сделаны для возвращения к странице Конфигурации сервера.
8. Нажмите **Update Server** на странице Конфигурации сервера.**Рисунок 7**

Добавьте два новых Коллектора к Профилировщику. Выполните следующие действия:

1. Выберите **Configuration> NAC Profiler Modules> Add Collector**.**Рис. 8**

2. Добавьте новое название Коллектора для Сервера NAC HA Пара. Это может быть чем-либо, что вы хотите, но должны совпасть на Конфигурации Коллектора.Название коллектора — CAS-OOB-Pair1IP-адрес (Виртуальный адрес Сервера NAC)Соединение — Выход это как **NONE** на данный момент. Можно изменить это в более позднее время к Подключению к серверу, которое находится в режиме прослушивания.
3. **Нажмите Add кнопку коллектора**.**Рис. 9**
4. Настройте свои Сервисные модули Коллектора. Оставьте в покое NetMap и NetTrap.**Рис. 10**
5. Добавьте интерфейс NetWatch (eth3), который связан с Портом SPAN на коммутаторе распределения.**Рис. 1-1**
6. Добавьте Блок подсети для модуля NetInquiry для прислушиваний к представляющему интерес трафику, который прибывает из доступов к сети. Будьте определенными в сетях относительно не, облагают налогом сервер NAC излишне. В этой лабораторной установке это может быть целые 192.168.0.0 личного пространства.**Рисунок 12**
Примечание: Развернутая проверка доступности адресата (ping sweep) выхода и набор DNS отключены. Используйте это как последнее прибежище. Набор развернутая проверки доступности адресата (ping sweep) и DNS инициирует эхо-запросы и nslookup на диапазоне IP-подсетей, вы вставляете Сетевой раздел Блоков. Это не рекомендуется и редко используется.
7. Настройте Средство передачи для прослушивания на IP-адресе 192.168.97.10 (VIP) и порт TCP 31416. Это позволяет Коллектору действовать как сервер и прислушиваться к соединению от Профилировщика к определенному порту TCP. Это размышляет над первыми несколькими шагами для Конфигурации сервера.
8. Включите Netflow для пары коллектора. ДополнительноМожно сделать это здесь, так как Netflow передают от удаленного маршрутизатора ни из-за какого удаленного коллектора.
9. Введите блоки IP-адреса для удаленного узла, как изображено. В данном примере использовано целые 192.168.0.0 личного пространства.**Рисунок 13**
10. Нажмите **Save Collector** для сохранения конфигурации.

Добавьте дополнительный отдельный сборщик к профилировщику

Выполните следующие действия:

1. **Нажмите Add коллектор**.**Рисунок 14**
2. Название коллектора может быть чем-либо, что вы хотите. В данном примере это - CAS2.
3. IP-адрес Средства передачи самостоятельно. IP-адрес eth0 для управления.В данном примере это 192.168.97.12.Соединением должен быть IP-адрес Профилировщика. В этом случае это 192.168.96.21.
4. **Нажмите Add коллектор**.**Рисунок 15**
5. После этого вы принесены к странице конфигурации Коллектора. Завершенные шаги 5 - 9 в предыдущий раздел. Это позволяет вам модифицировать и добавлять уникальные IP - адреса и параметры конфигурации отдельного сборщика.
6. Одна уникальная установка для Отдельного сборщика является способностью добавить несколько интерфейсов к конфигурации NetWatch. Здесь можно добавить несколько интерфейсов, таким образом, вы видите трафик для DHCP, DNS и IP-телефонии от удаленных оконечных точек.

7. Настройте интерфейсы NetWatch для своей настройки. В данном примере три интерфейса были добавлены к трафику SPAN на отдельном сборщике.**Рисунок 16**
8. **Примечание:** Выберите **Конфигурация> Применяют Изменения> Модули Обновления** для сохранения настроек.

Настройте модули коллектора NAC на сервере NAC

Примечание: Эта конфигурация должна быть выполнена на всех Коллекторах.

Эта конфигурация позволяет Профилировщику и Коллекторам передавать и устанавливать безопасные соединения для получения информации об устройствах, чтобы начать течь. Выполните следующие действия:

1. SSH или консоль к Коллектору и входу в систему как **root** от консоли или **маяк** от Сеанса SSH.
2. Введите **команду service collector config**.
3. Пробегите сценарий конфигурации для устанавливания части Коллектора NAC.**HA пример коллектора**Коллектор является настройкой как типом *Подключения к серверу*:`[root@cas1 ~]#`**`service collector config`** `Enable the NAC Collector (y/n) [y]: Configure NAC Collector (y/n) [y]: Enter the name for this remote collector. Please note that if this collector exists on a HA pair that this name must match its pair’s name for proper operation. (24 char max) [cas1]: CAS-OOB-Pair1 Network configuration to connect to a NAC Profiler Server Connection type (server/client) [server]: Listen on IP [192.168.97.10]:`
   Вас просят ввести IP-адрес (IP-адреса) NPS. Это необходимо для настройки списка контроля доступа, используемого этим коллектором. Если NPS является частью пары HA, то необходимо включать реальный IP - адрес каждого независимого NPS и виртуального IP для обеспечения правильного подключения в случае аварийного переключения. Введите IP-адрес (IP-адреса) Профилировщика NAC.
   ```
   (Finish by typing ‘done’) [127.0.0.1]: 192.168.96.20  (Real IP address of  NAC Server1)
   Enter the IP address(es) of the NAC Profiler.
   (Finish by typing ‘done’) [192.168.96.20]: 192.168.96.21 (Virtual IP of NAC Server)
   Enter the IP address(es) of the NAC Profiler.
   (Finish by typing ‘done’) [done]: 192.168.96.22 (Real IP of NAC Server2)
   Enter the IP address(es) of the NAC Profiler.
   (Finish by typing ‘done’) [done]: done
   Port number [31416]:
   Encryption type (AES, blowfish, none) [none]: AES
   Shared secret []: cisco123
   •Configured CAS-OOB-Pair1-fw
   •Configured CAS-OOB-Pair1-nm
   •Configured CAS-OOB-Pair1-nt
   •Configured CAS-OOB-Pair1-nw
   •Configured CAS-OOB-Pair1-ni
   •Configured CAS-OOB-Pair1-nr

   NAC Collector has been configured.
   ```
4. Запустите сервисы коллектора.`[root@cas1 ~]#`**`service collector start`** **Одинокий пример Коллектора**`[root@cas2 ~]#`**`service collector config`** `Enable the NAC Collector (y/n) [y]: Configure NAC Collector (y/n) [y]: Enter the name for this remote collector. Please note that if this collector exists on a HA pair that this name must match its pair's name for proper operation. (24 char max) [cas2]: Network configuration to connect to a NAC Profiler Server Connection type (server/client) [client]: Connect to IP [192.168.96.21]: Port number [31416]: Encryption type (AES, blowfish, none) [none]: Shared secret []: -- Configured cas2-fw -- Configured cas2-nm -- Configured cas2-nt -- Configured cas2-nw -- Configured cas2-ni -- Configured cas2-nr NAC Collector has been configured. [root@cas2 ~]#`**`service collector start`**

Настройте Коммутатор Удаленного доступа для передачи Trap-сообщений SNMP к Коллектору NAC

Эта конфигурация позволяет Профилировщику динамично получать все новые устройства, соединяющиеся с портом коммутатора через trap-сообщения уведомления Mac. Это особенно важно с тех пор в топологии существует IP-телефон и ПК, связанный с тем же портом.

Консоль или Telnet в коммутатор `(nac-3750-access#)`.

```
snmp-server community cleanaccess RW snmp-server community profiler RO snmp-server enable traps mac-notification snmp-server host 192.168.96.10 version 2c cleanaccess snmp-server host 192.168.97.10 version 1 profiler
```

Настройте удаленный доступ, включают профилировщика для сбора сведений SNMP

Выполните следующие действия:

1. Выберите **Profiler GUI> Configuration>, Сетевые устройства> Добавляют Устройство**.**Рисунок 18**
2. Добавьте имя хоста и управление IP-адресами коммутатора.
3. Также введите строки snmp только для чтения, настроенные в коммутатор. Удостоверьтесь, что выбрали модуль сопоставления Коллектора NAC, таким образом, Коллектор выбран к SNMP, опрашивают коммутатор доступа каждый час и передают информацию Профилировщику.
4. **Нажмите Add Устройство** и **Примените Изменения** для обновления Модулей от левой области GUI.**Рисунок 19**

Настройте маршрутизатор удаленного доступа на профилировщике для сбора сведений SNMP

Это позволяет IP-адрес Уровня 3 привязке MAC в базе данных Профилировщика.

1. Выберите **Profiler GUI> Configuration>, Сетевые устройства> Добавляют Устройство**.**Рис. 20** Посмотрите рисунок 21.
2. Добавьте имя хоста и управление IP-адресами маршрутизатора.
3. Также введите строки snmp только для чтения, настроенные в маршрутизатор. Удостоверьтесь, что выбрали модуль сопоставления Коллектора NAC, таким образом, Коллектор выбран к SNMP, опрашивают коммутатор доступа каждый час и передают информацию Профилировщику.
4. **Нажмите Add Устройство** и **Примените Изменения** для обновления Модулей от левой области GUI.**Рис. 21**

Настройте Коллекторы NAC для Получения Трафика SPAN на их Локальных коммутаторах

Примечание: Это позволяет Модулю NetWatch начинать прислушиваться к трафику в сети и передавать информацию Профилировщику. Удостоверьтесь, что вы не превышаете

намеченную сумму интерфейса Коллектора NAC. Это имеет ограничение 1 Гбайт/с. Можно получить интерфейсы или vlans коммутатора, и это зависит от модели коммутатора и версии кода.

Примечание: Минимально вы хотите видеть запросы DHCP и предложения от оконечных точек на ваших коммутаторах доступа. Если это не возможно, попытайтесь включить Коллектор NAC или около серверов DHCP в вашей сети. Это сделано в этом руководстве по конфигурации.

Выполните следующие действия:

1. Настройте сеанс монитора на коммутаторе распределения #1 для удаленного входящего и исходящего трафика узла:`monitor session 1 source interface F0/0`
   `monitor session 1 destination interface Gi1/0/44`
2. Настройте двойной сеанс монитора на коммутаторе распределения #2 для удаленного входящего и исходящего трафика узла:`monitor session 1 source interface F0/0`
   `monitor session 1 destination interface Gi1/0/44`
3. Настройте другой сеанс монитора для Отдельного сборщика. Данный пример контролирует несколько интерфейсов, связанных с основным коммутатором, которые имеют значение. Это DHCP, DNS и Cisco CallManager server для этой лабораторной установки.`monitor session 1 source interface G1/0/7-9`
   `monitor session 1 destination interface G1/0/48`

Настройте маршрутизатор удаленного доступа для передачи данных NetFlow к коллектору в центральном узле

Выполните следующие действия:

1. Telnet к удаленному маршрутизатору.
2. Включите Netflow глобально.`ip flow-export version 5`
   `ip flow-export destination 192.168.97.12 2055`**Примечание:** Коллекторы слушают на порту 2055 UDP для Netflow. IP-адрес для передачи Netflow всегда является управлением IP-адресами Коллекторов.
3. Включите Netflow на интерфейсах.`interface FastEthernet0/1`
   `ip address 192.168.121.1 255.255.255.0`
   `ip flow ingress`
   `ip route-cache flow`

Проверка

Посмотрите раздел Процедуры устранения проблем, чтобы подтвердить, что ваша конфигурация работает должным образом.

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

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

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

Процедура устранения неполадок

Выполните следующие шаги для устранения неполадки в вашей настройке.

1. Удостоверьтесь, что Профилировщик и Коллектор связываются и работают. Если они не, то вы не видите информации об устройствах в вашей сети. Если существуют проблемы, не продолжайтесь, пока всеми Модулями Коллектора и Сервером не является `Running`.На Профилировщике выберите **Configuration> NAC Profiler Modules> List NAC Profiler Modules**.
2. Проверьте, что коммутатор доступа передает trap-сообщения уведомления нового Mac к Коллектору. Будьте осторожны, когда вы включаете отладку, и необходимо знать ее опасности.`nac-3750-access#`**`debug snmp packet`** `nac-3750-access#`**`debug snmp header`**
3. Проверьте, что Коллектор имеет SNMP, опросил коммутатор:Посмотрите на столбец Last Scan.
4. Debug SNMP снова на коммутаторе.
5. От Профилировщика выберите **Configuration> Network Devices**. Примите решение перечислить **Сетевые устройства** и затем выбрать **Device**.
6. Нажмите **Query**.
7. Наблюдайте, что выходные данные отладки на Коммутаторе для Коллектора к SNMP опрашивают коммутатор:`*Mar 30 23:09:24: SNMP: Packet` **`received via UDP from 192.168.97.11`** `on Vlan100 *Mar 30 23:09:24: SNMP: Get-next request, reqid 1347517983, errstat 0, erridx 0 ifType = NULL TYPE/VALUE *Mar 30 23:09:24: SNMP: Response, reqid 1347517983, errstat 0, erridx 0 ifType.1 = 53 *Mar 30 23:09:24: SNMP: Packet` **`sent via UDP to 192.168.97.11`**
8. Включите свой IP-телефон на коммутаторе или выполните **команду shut then no shut** на интерфейсе:
```
15w4d: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/4, changed state to down
15w4d: %ILPOWER-5-POWER_GRANTED: Interface Gi1/0/4: Power granted
15w4d: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/4, changed state to up
15w4d: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/4, changed state
to up
15w4d: SNMP: Queuing packet to 192.168.97.12
15w4d: Outgoing SNMP packet
15w4d: v2c packet
15w4d: community string: profiler
15w4d: SNMP: V2 Trap, reqid 14430, errstat 0, erridx 0
 sysUpTime.0 = 949829672
 snmpTrapOID.0 = cmnMacChangedNotification
 cmnHistMacChangedMsg.0 =
01 00 79 00 07 50 C6 82 27 00 04 00
```
9. Проверьте, что Коллектор отправляет новый запрос trap-сообщения для полученного MAC-адреса:
```
15w4d: SNMP: Packet received via UDP from 192.168.97.11 on Vlan120
15w4d: SNMP: Get request, reqid 1576567642, errstat 0, erridx 0
 system.1.0 = NULL TYPE/VALUE
 ifIndex.10104 = NULL TYPE/VALUE
 ifDescr.10104 = NULL TYPE/VALUE
 ifType.10104 = NULL TYPE/VALUE
 ifSpeed.10104 = NULL TYPE/VALUE
 ifPhysAddress.10104 = NULL TYPE/VALUE
 ifAdminStatus.10104 = NULL TYPE/VALUE
 ifOperStatus.10104 = NULL TYPE/VALUE
 ifName.10104 = NULL TYPE/VALUE
 dot1xAuthAuthControlledPortStatus.10104 = NULL TYPE/VALUE
```

```
 dot1xAuthAuthControlledPortControl.10104 = NULL TYPE/VALUE
paeMIBObjects.2.4.1.9.10104 = NULL TYPE/VALUE

-------snip ----------
ifIndex.10104 = 10104
 ifDescr.10104 = GigabitEthernet1/0/4
 ifType.10104 = 6
 ifSpeed.10104 = 100000000
 ifPhysAddress.10104 = 00 14 A8 2E A5 04
 ifAdminStatus.10104 = 1
 ifOperStatus.10104 = 1
 ifName.10104 = Gi1/0/4
 dot1xAuthAuthControlledPortStatus.10104 = 1
 dot1xAuthAuthControlledPortControl.10104 = 3
15w4d: SNMP: Packet sent via UDP to 192.168.97.11
```

10. Проверьте, что Профилировщик получил новый MAC-адрес IP-телефона от Коллектора:Выберите **Endpoint Console> View/Manage Endpoints> Display Endpoints портами устройства> разгруппированный> Таблица Устройств** и затем выберите свой коммутатор.
11. Проверьте, что SPAN работает на коммутатор, и Коллектор получает трафик.`SSH to the NAC Profiler :`
    `Type : tcpdump –i eth3`

    ```
    16:54:36.432218 IP cas2.nacelab2.cisco.com.9308 > elab2-dns-
    dhcp.nacelab2.cisco.com.domain:  48871+ PTR? 68.39.168.192.in-addr.arpa. (44)
    ```

    Наблюдайте выходные данные на экране. Если вы обеспокоены суммой выходных данных, можно передать выходные данные по каналу к файлу на Коллекторе NAC. Посмотрите оперативные страницы руководства в Linux о том, как выполнить это.
12. Проверьте, чтобы видеть, был ли трафик DHCP об оконечной точке IP-телефона замечен через Порт SPAN и передан до Профилировщика.Выберите **Endpoint Console> View/Manage Endpoints> Display Endpoints портами устройства> разгруппированный> Таблица Устройств** и затем выберите свой коммутатор.Затем выберите **MAC-адрес** своих устройств.Нажмите **View Profile Data**.Необходимо видеть информацию о Классе поставщика DHCP от устройств, перехваченных от трафика NetWatch/SPAN на Коллекторе. Эта информация может прибыть из Сервера DHCP или Предложения DHCP на Порте SPAN назад клиенту, который зависит от вашей маршрутизации и среды.
13. Проверьте, что Netflow передают от удаленного маршрутизатора до интерфейса управления Коллектора.`NAC-2800-Remote#`**`show ip flow export`** `Flow export v5 is enabled for main cache Exporting flows to 192.168.97.12 (2055) Exporting using source IP address 10.0.0.2 Version 5 flow records 2602429 flows exported in 554968 udp datagrams 0 flows failed due to lack of export packet NAC-2800-Remote#`**`show ip flow top 10 aggregate source-address`** Существует четыре главных говорящих:`IPV4 SRC-ADDR  bytes  pkts flows`

    ```
    ===============  ==========  ==========  ==========
    192.168.122.60           44           1           1
    192.168.122.59           88           2           2
    192.168.121.90          367           3           3
    10.0.0.1              19320         322           1
    ```

14. Проверьте, что Профилировщик от Коллекторов получает Netflow. Выберите свой удаленный MAC или IP Оконечной точки и посмотрите на Представленные Данные:Выберите **Endpoint Console> View/Manage Endpoints> Display Endpoints портами устройства> разгруппированный> Таблица Устройств** и затем выберите свой коммутатор.Затем выберите MAC-адрес своих устройств.Нажмите **View Profile Data**.В выходных данных вы видите целевой трафик к IP 192.168.70.50 и порту назначения

2000. Это - IP-адрес Cisco CallManager и порта назначения, 2000 используется для контрольного трафика SCCP.

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация