VACL Capture для детального анализа трафика с помощью Cisco Catalyst 6000/6500 под управлением программного обеспечения CatOS

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Родственные продукты
Условные обозначения
Общие сведения
SPAN на основе VLAN
ACL VLAN
Преимущества использования VACL по использованию VSPAN
Настройка
Схема сети
Конфигурация с SPAN на основе VLAN
Конфигурация с VACL
Проверка
Устранение неполадок
Дополнительные сведения

Введение

Этот документ предоставляет пример конфигурации для использования Списка контроля доступом VLAN (ACL) (VACL) функция порта Перехвата анализа сетевого трафика более гранулированным способом. Этот документ также сообщает преимущество использования портов перехвата VACL в противоположность Коммутируемому анализатору для портов (SPAN) на основе VLAN (VSPAN) использование.

Для настройки функции порта VACL Capture на Cisco Catalyst 6000/6500, который выполняет программное обеспечение Cisco IOS, обратитесь к VACL Capture для Детального анализа трафика с Cisco Catalyst 6000/6500 Рабочее программное обеспечение Cisco IOS.

Предварительные условия

Требования

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

- Виртуальная локальная сеть — см. Виртуальные локальные сети / протокол VTP - Введение для получения дополнительной информации.
- Списки доступа — см. Управление доступом Настройки для получения дополнительной информации.

Используемые компоненты

Сведения в этом документе основываются на Cisco Catalyst Коммутатор серии 6506, который выполняет Релиз операционной системы Catalyst 8.1 (2).

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.

Родственные продукты

Эта конфигурация может также использоваться с Cisco Catalyst 6000 / коммутаторы серии "6500", которые выполняют Релиз операционной системы Catalyst 6.3 и позже.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Общие сведения

SPAN на основе VLAN

SPAN копирует трафик с одного или более исходных портов в любой VLAN или от одной или более VLAN до порта назначения для анализа. Локальный анализатор SPAN поддерживает исходные порты, исходные VLAN и порты назначения на том же Коммутаторе серии Catalyst 6500.

Исходный порт является портом, проверенным для анализа сетевого трафика. Исходная VLAN является VLAN, проверенной для анализа сетевого трафика. SPAN на основе VLAN (VSPAN) является анализом сетевого трафика в одной или более VLAN. Можно настроить VSPAN как SPAN для внешнего доступа, выходной диапазон или обоих. Все порты в исходных VLAN становятся в рабочем состоянии исходными портами для сеанса VSPAN. Порты назначения, если они принадлежат какой-либо из VLAN административного источника, исключены из в рабочем состоянии источника. Если вы добавляете или удаляете порты из VLAN административного источника, в рабочем состоянии источники модифицируются соответственно.

Рекомендации для сеансов VSPAN:

- Магистральные порты включены как исходные порты для сеансов VSPAN, но только

VLAN, которые находятся в списке Административного источника, проверены, если эти VLAN активны для транка.
- Для сеансов VSPAN и с входом и с настроенным выходным диапазоном, система работает на основе типа Supervisor Engine, который вы имеете:Если пакеты включены та же VLAN, WS-X6K-SUP1A-PFC, WS-X6K-SUP1A-MSFC, WS-X6K-S1A-MSFC2, WS-X6K-S2-PFC2, WS-X6K-S1A-MSFC2, WS-SUP720, WS-SUP32-GE-3B — Два пакета переданы портом назначения SPAN.WS-X6K-SUP1-2GE, WS-X6K-SUP1A-2GE — Только один пакет передан портом назначения SPAN.
- Порт для внутренней полосы связи не включен как Действующий источник для сеансов VSPAN.
- Когда VLAN очищена, она удалена из списка источников для сеансов VSPAN.
- Если список VLAN Административного источника пуст, сеанс VSPAN отключен.
- Неактивные VLAN не позволены для конфигурации VSPAN.
- Если какая-либо из исходных VLAN становится VLAN RSPAN, сеанс VSPAN сделан неактивным.

См. Характеристики Исходной VLAN для получения дополнительной информации об исходных VLAN.

ACL VLAN

VACL могут управление доступом весь трафик. Можно настроить VACL на коммутаторе для применения ко всем пакетам, которые маршрутизируются в или из VLAN или соединены в VLAN. VACL строго для трафика фильтрации пакетов и перенаправления безопасности к определенным портам физического коммутатора. В отличие от ACL Cisco IOS, VACL не определены направлением (ввод или вывод).

Можно настроить VACL на адресах Уровня 3 для IP и IPX. Все другие протоколы являются доступом, управляемым через MAC-адреса и EtherType с помощью VACL MAC. IP - трафик и трафик IPX не являются доступом, управляемым VACL MAC. Все другие типы трафика (AppleTalk, DECnet, и так далее) классифицированы как трафик MAC. VACL MAC используются к управлению доступом этот трафик.

ACE, поддерживаемые в VACL

VACL содержит упорядоченный список записей управления доступом (ACE). Каждый VACL может содержать ACE только одного типа. Каждый ACE содержит много полей, с которыми совпадают против содержания пакета. Каждое поле может иметь связанную битную маску для указания, какие биты релевантны. Действие привязано к каждому ACE, который описывает то, что система должна сделать с пакетом, когда происходит соответствие. Действие является зависимым функции. Коммутаторы серии Catalyst 6500 поддерживают три типа ACE в аппаратных средствах:

- ACE IP
- ACE IPX
- ACE Ethernet

Эта таблица приводит параметры, которые привязаны к каждому первоклассному типу:

Первоклассный тип	TCP или UDP	ICMP	Другой IP	IPX	Ethernet

Параметры уровня 4	Исходный порт	-	-	-	-
	Оператор исходного порта	-	-	-	-
	Номер порта	-	-	-	-
	Оператор порта назначения	КОД ICMP	-	-	-
	Н/Д	Тип ICMP	Н/Д	-	-
Параметры уровня 3	Байт ToS IP	Байт ToS IP	Байт ToS IP	-	-
	IP - адрес источника	IP - адрес источника	IP - адрес источника	Исходная сеть IPX	-
	IP - адрес назначения (DA)	IP - адрес назначения (DA)	IP - адрес назначения (DA)	Сеть IP - адреса назначения	-
	-	-	-	Узел IP - адреса назначения	-
	TCP или UDP	ICMP	Другой протокол	Тип пакета IPX	-
Параметры уровня 2	-	-	-	-	Ether Type
	-	-	-	-	Адрес источника Ethernet
	-	-	-	-	Адрес назначения (DA) Ethernet

Преимущества использования VACL по использованию VSPAN

Существует несколько ограничений использования VSPAN для анализа трафика:

- Весь трафик Уровня 2, который течет в VLAN, перехвачен. Это увеличивает объем данных, который будет проанализирован.
- Количество Сессий SPAN, которые могут быть настроены на Коммутаторах серии Catalyst 6500, ограничено. См. Сводку характеристик и Ограничения для получения дополнительной информации.
- Порт назначения получает копии отправленного и полученного трафика со всех отслеживаемых портов-источников. Если лимит порта назначения превышен, он может быть перегружен. Такая перегрузка может повлиять на передачу трафика на один или более одного порта-источника.

Функция порта VACL Capture может помочь преодолевать некоторые из этих ограничений. VACL прежде всего не разработаны для мониторинга трафика. Однако с широким диапазоном возможности классифицировать трафик, функция порта Перехвата была представлена так, чтобы анализ сетевого трафика мог стать намного более простым. Это преимущества Использования портов VACL Capture по VSPAN:

- Детальный анализ трафикаVACL могут совпасть на основе IP - адреса источника, IP - адреса назначения, типа протокола Уровня 4, источника и уровня назначения 4 порта и другая информация. Эта возможность делает VACL очень полезными для гранулированной идентификации трафика и фильтрации.
- Количество сеансовVACL принуждены в аппаратных средствах. Количество ACE, которые могут быть созданы, зависит от TCAM, доступного в коммутаторах.
- Превышение подписки порта назначенияГранулированная идентификация трафика сокращает количество кадров, которые будут переданы порту назначения и таким образом минимизирует вероятность их превышения подписки.
- ПроизводительностьVACL принуждены в аппаратных средствах. Нет никакого снижения производительности для приложения VACL к VLAN на коммутаторах Cisco Catalyst серии 6500.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

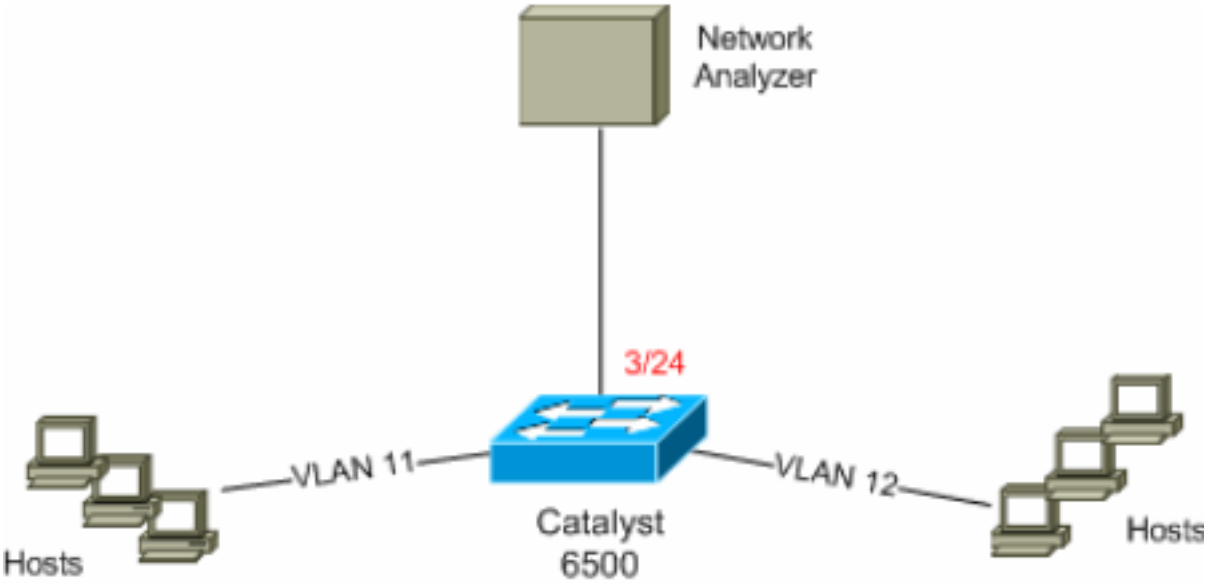
Эти конфигурации используются в данном документе:

- Конфигурация с SPAN на основе VLAN
- Конфигурация с VACL

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схема сети

В настоящем документе используется следующая схема сети:



Конфигурация с SPAN на основе VLAN

Этот пример конфигурации перечисляет шаги, требуемые перехватывать весь трафик Уровня 2, который течет в VLAN 11 и VLAN 12, и передайте им к устройству Анализатора сети.

1. Задайте представляющий интерес трафик.В данном примере это - трафик, который течет в VLAN 100 и VLAN 200.`6K-CatOS> (enable) **set span** *11-12 3/24 !--- where **11-12** specifies the range of source VLANs and **3/24** specify the destination port.* 2007 Jul 12 21:45:43 %SYS-5-SPAN_CFGSTATECHG:local span session inactive for des tination port 3/24 Destination : Port 3/24 Admin Source : VLAN 11-12 Oper Source : Port 3/11-12,16/1 Direction : transmit/receive Incoming Packets: disabled Learning : enabled Multicast : enabled Filter : - Status : active 6K-CatOS> (enable) 2007 Jul 12 21:45:43 %SYS-5-SPAN_CFGSTATECHG:local span sessi on active for destination port 3/24` С этим весь трафик Уровня 2, который принадлежит VLAN 11 и VLAN 12, скопирован и передан порту 3/24.
2. Проверьте свою Конфигурацию SPAN с **командой show span all**.`6K-CatOS> (enable) **show span all** Destination : Port 3/24 Admin Source : VLAN 11-12 Oper Source : Port 3/11-12,16/1 Direction : transmit/receive Incoming Packets: disabled Learning : enabled Multicast : enabled Filter : - Status : active Total local span sessions: 1 No remote span session configured 6K-CatOS> (enable)`

Конфигурация с VACL

В этом примере конфигурации от администратора сети существуют множественные требования:

- Трафик HTTP из диапазона хостов (10.12.12.128/25) в VLAN 12 к определенному серверу (10.11.11.100) в VLAN 11 должен быть перехвачен.
- Протокол передачи дэйтаграмм Многоадресного пользователя (UDP) трафик в направлении передачи предназначил для группового адреса 239.0.0.100 потребности, которые будут перехвачены от VLAN 11.

1. Определите представляющий интерес трафик с помощью Списков управления доступом. Не забудьте упоминать **перехват** ключевого слова для всех определенных ACE.`6K-CatOS> (enable) **set security acl ip** *HttpUdp_Acl* **permit tcp** *10.12.12.128 0.0.0.127* **host** *10.11.11.100* **eq** *www* **capture** *!--- Command wrapped to the second line.* HttpUdp_Acl editbuffer modified. Use 'commit' command to apply changes. 6K-CatOS> (enable) **set security**`

acl ip *HttpUdp_Acl* **permit udp any host** *239.0.0.100* **capture** HttpUdp_Acl editbuffer modified. Use 'commit' command to apply changes.

2. Проверьте, корректна ли первоклассная конфигурация и в надлежащем заказе.6K-CatOS> (enable) **show security acl info** *HttpUdp_Acl* **editbuffer** set security acl ip HttpUdp_Acl ---------- 1. permit tcp 10.12.12.128 0.0.0.127 host 10.11.11.100 eq 80 capture 2. permit udp any host 239.0.0.100 capture ACL HttpUdp_Acl Status: **Not Committed** 6K-CatOS> (enable)
3. Передайте ACL аппаратным средствам.6K-CatOS> (enable) **commit security acl** *HttpUdp_Acl* ACL commit in progress. ACL 'HttpUdp_Acl' successfully committed. 6K-CatOS> (enable)
4. Проверьте статус ACL.6K-CatOS> (enable) **show security acl info** *HttpUdp_Acl* **editbuffer** set security acl ip HttpUdp_Acl ---------- 1. permit tcp 10.12.12.128 0.0.0.127 host 10.11.11.100 eq 80 capture 2. permit udp any host 239.0.0.100 capture ACL HttpUdp_Acl Status: **Committed** 6K-CatOS> (enable)
5. Примените карту доступа VLAN к соответствующим VLAN.6K-CatOS> (enable) **set security acl map** *HttpUdp_Acl* **?** <vlans> Vlan(s) to be mapped to ACL 6K-CatOS> (enable) **set security acl map** *HttpUdp_Acl 11* Mapping in progress. ACL HttpUdp_Acl successfully mapped to VLAN 11. 6K-CatOS> (enable)
6. Проверьте ACL к сопоставлению VLAN.6K-CatOS> (enable) **show security acl map** *HttpUdp_Acl* ACL HttpUdp_Acl is mapped to VLANs: 11 6K-CatOS> (enable)
7. Настройте порт перехвата.6K-CatOS> (enable) **set vlan** *11 3/24* VLAN Mod/Ports ---- ---------- 11 3/11,3/24 6K-CatOS> (enable) 6K-CatOS> (enable) **set security acl capture-ports** *3/24* Successfully set 3/24 to capture ACL traffic. 6K-CatOS> (enable)
   Примечание: Если ACL сопоставлен с несколько интерфейсов VLAN, то порт перехвата должен быть настроен ко всем тем VLAN. Чтобы заставить порт перехвата позволить несколько интерфейсов VLAN, настроить порт как транк и позволить только VLAN, сопоставленные с ACL. Например, если ACL сопоставлен с VLAN 11 и 12, то завершите конфигурацию.6K-CatOS> (enable) **clear trunk** *3/24 1-10,13-1005,1025-4094* 6K-CatOS> (enable) **set trunk** *3/24 on dot1q 11-12* 6K-CatOS> (enable) **set security acl capture-ports** *3/24*
8. Проверьте конфигурацию порта перехвата.6K-CatOS> (enable) **show security acl capture-ports** ACL Capture Ports: 3/24 6K-CatOS> (enable)

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

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

- **покажите, что информация ACL безопасности** — Отображает содержание VACL, которое в настоящее время настраивается или в последний раз предается NVRAM и аппаратным средствам.6K-CatOS> (enable) **show security acl info** *HttpUdp_Acl* set security acl ip HttpUdp_Acl ---------- 1. permit tcp 10.12.12.128 0.0.0.127 host 10.11.11.100 eq 80 capture 2. permit udp any host 239.0.0.100 capture 6K-CatOS> (enable)
- **покажите, что карта ACL безопасности** — Отображает ACL К VLAN или ACL К СОПОСТАВЛЕНИЮ ПОРТОВ для определенного ACL, порта или VLAN.6K-CatOS> (enable) **show security acl map all** ACL Name Type Vlans ---------- ---------- HttpUdp_Acl IP 11 6K-CatOS> (enable)
- **покажите, что порты перехвата ACL безопасности** — Отображают список портов перехвата.6K-CatOS> (enable) **show security acl capture-ports** ACL Capture Ports: 3/24 6K-CatOS> (enable)

Устранение неполадок

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

Дополнительные сведения

- VACL Capture для детального анализа трафика с помощью Cisco Catalyst 6000/6500 под управлением программного обеспечения Cisco IOS
- Управление доступом Настройки - руководство по конфигурации программного обеспечения серии Catalyst 6500, 8.6
- Страницы поддержки продуктов LAN
- Страница поддержки коммутационных решений для локальной сети
- Cisco Systems – техническая поддержка и документация