Содержание

[Введение](#)
[Предварительные условия](#)
[Требования](#)
[Используемые компоненты](#)
[Настройка](#)
[Проверка](#)
[Устранение неполадок](#)
[Дополнительные сведения](#)

Введение

Этот документ описывает подробно, с какими типами трафика совпадают против карт классов по умолчанию, которые являются частью Catalyst 6500 по умолчанию Sup2T / (Контроль уровня управления) конфигурация Catalyst 6880 CoPP, которая автоматически настроена на устройстве. Это настроено для защиты его ЦП от того, чтобы быть перегруженным.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

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.

Настройка

CoPP включают по умолчанию на Catalyst 6500 / SUP2T и Catalyst 6880 переключают и основываются на предварительно сконфигурированном шаблоне. Некоторые конфигурации схемы классов не имеют соответствующих сообщений о совпадении вследствие того, что они перехватывают трафик не на Списке контроля доступа (ACL) MAC/IP, а скорее на

внутренних исключительных ситуациях, которые сообщены механизмом пересылки, когда трафик получен коммутатором и взятым решением по перенаправлению.

Если определенный class-map должен быть добавлен / модифицируемый / удаленный из текущей политики CoPP, затем это должно быть сделанный от режима конфигурации в режиме policy-map. Посмотрите Руководство по конфигурации программного обеспечения Выпуска 15.0SY Catalyst 6500 - Контроль уровня управления (CoPP) для точного синтаксиса.

Классы исключений CoPP по умолчанию имеют эти описания:

CAS E	название class-map	Описание
Сбой Максимального размера передаваемого блока данных (MTU)	class-copp-mtu-fail	Размер пакета превышает максимальный размер передаваемого блока данных исходящего интерфейса. Если не Фрагментирует, укусил, "not set", фрагментация требуется. Если не Фрагментирует, укусил, установлен, Сообщение о недоступности назначения Протокола ICMP указывает, что "необходимый набор фрагментации и DF", как предполагается, генерируется и передается обратно в источник. Ссылка: RFC 791, RFC1191
Сбой Времени жизни (TTL)	class-copp-ttl-fail	Пакетный TTL = 1 (для IPv4), предел перехода = 0 или 1 (для IPv6) От TTL = 0 (для IPv4) можно сбросить в аппаратных средствах сразу же, поскольку предыдущий переход, как предполагается, уничтожает пакет, когда TTL постепенно уменьшен к 0. Предел перехода = 0 (для IPv6) отличается от TTL = 0, потому что это сообщается в RFC 2460, разделите 8.2, что "В отличие от IPv4, узлы IPv6 не требуются, чтобы принуждать срок действия MAXIMUM PACKET. Это - причина, поле IPv4 Time to Live было переименовано Предел Перехода в IPv6". Это означает, что входящий пакет IPv6 с Пределом Перехода = 0 все еще допустим, и сообщение ICMP нужно передать обратно. Ссылка: RFC 791, RFC 2460
Опции	class-copp-options	Пакет с опциями (для IPv4), Заголовок расширения Перехода за переходом (для IPv6). Например, оповещение маршрутизатора RFC 2113, Строгий

		Исходный маршрут, и так далее. Заголовки расширения не исследованы или обработаны любым узлом вдоль пути доставки пакета, пока пакет не достигает узла (или каждый набор узлов в случае ofmulticast) определенный в Поле адреса точки назначения theIPv6 заголовка. Единственным исключением является заголовок Опций Перехода за переходом, который несет информацию, которая должна быть исследована и обработана каждым узлом вдоль пути доставки пакета, который включает источник и узлы - адресатов. Аппаратная обработка на полях параметра не поддерживается, который является программным обеспечением, processing/switching, необходим. Ссылка: RFC 791 / RFC 2460
Сбой Пересылки по обратному пути (RPF) (Индивидуальная рассылка)	class-copp-ucast-rpf-fail	Пакетная Проверка переадресации по обратному пути сбоя фильтруется. Однако из-за ограниченных ресурсов в аппаратных средствах, Проверка переадресации по обратному пути не может быть сделана в аппаратных средствах в определенных случаях (т.е. больше чем 16 интерфейсов RPF, связанных с одним IP). Когда это происходит, пакет передан к программному обеспечению для завершенной Проверки переадресации по обратному пути. Первый RPF отказал, пакет данных (адресованный группе многоадресной рассылки) передается программному обеспечению для независимой от протокола многоадресной передачи (PIM) - утверждают процесс для начала. Как только процесс сделан, выделенный маршрутизатор / средство передачи избран. Если следующий пакет (тот же поток) не прибывает из выделенного маршрутизатора, это инициирует Ошибку переадресации по

		обратному пути, и аппаратные средства могут отбросить его сразу же (для предотвращения Атаки типа отказ в обслуживании (DOS)).
Ошибка переадресации по обратному пути (Групповая адресация)	class-copp-mcast-rpf-fail	Первый RPF отказал, пакет данных (адресованный группе многоадресной рассылки) передается программному обеспечению для PIM - утверждают процесс для начала. Как только процесс сделан, выделенный маршрутизатор / средство передачи избран. Если следующий пакет (тот же поток) не прибывает из выделенного маршрутизатора, это инициирует Ошибку переадресации по обратному пути, и аппаратные средства могут отбросить его сразу же (для предотвращения атаки DoS). Однако, если таблица маршрутизации обновлена, новый выделенный маршрутизатор, возможно, должен был бы быть выбран (через PIM - утверждают), что означает, что RPF отказал, пакет должен достигнуть, программное обеспечение (для PIM - утверждают для начала снова). Чтобы сделать это, периодическая утечка к программному механизму (на поток) для подведенного RPF пакета доступна в аппаратных средствах. Обратите внимание, хотя, если существует огромное количество потоков тогда, периодическая утечка может быть слишком много для программного обеспечения для обработки. Аппаратные средства CoPP все еще требуется для RPF групповой адресации, отказали пакет. Ссылка: RFC 3704, RFC 2362
Аппаратная перезапись пакета, не поддерживаемая	class-copp-unsupp-rewrite	В то время как аппаратные средства могут переписать пакеты в различных случаях, некоторые случаи просто не могут быть сделаны в текущей схеме оборудования. И для тех, аппаратные средства передают пакет к программному обеспечению.
Никакой маршрут ICMP Acl-drop ICMP	class-copp-icmp-redirect-unreachable	Пакеты, переданные к программному обеспечению для генерации сообщений ICMP. Такой как

Переадресация ICMP		переадресация ICMP, недостижимое назначение ICMP (например. недостижимый узел или административно запрещенный). Ссылка: RFC 792 / RFC 2463
Технология CEF получает (IP - адрес назначения является IP маршрутизатора),	class-copp-receive	Если IP - адрес назначения пакета будет одним из IP-адресов маршрутизатора (то совершит нападки, CEF получают смежность), то программное обеспечение, как предполагается, обрабатывает содержание.
Glean CEF (IP - адрес назначения принадлежит одной из сети маршрутизатора),	class-copp-glean	Если IP - адрес назначения пакета будет принадлежать одной из сети маршрутизатора, но это не решено (т.е. никакое соответствие в таблице Базы данных переадресации (FIB)), то это поразит подобранную смежность CEF, будучи переданным программному обеспечению, где процедура разрешения начнет работу. Для IPv4 тот же поток продолжает поражать glean CEF, пока не решен адрес. Для IPv6, временная запись FIB, которая совпадает с IP - адресом назначения (и указывает для отбрасывания смежности вместо этого) установлен во время разрешения. Если это не может быть решено в указанной продолжительности, запись FIB удалена (т.е. тот же поток начинает поражать glean CEF снова).
Пакет, предназначенный к IP-адресу групповой адресации 224.0.0.0/4	class-copp-mcast-ip-control	Управляющий пакет должен быть обработан программным обеспечением.
Пакет, предназначенный к FF IP-адреса групповой адресации::/8	class-copp-mcast-ipv6-control	Управляющий пакет должен быть обработан программным обеспечением.
Пакет групповой адресации, который должен быть скопирован к программному обеспечению	class-copp-mcast-copy	В некоторых случаях пакет групповой адресации должен быть скопирован к программному обеспечению для обновления состояния (пакет является все еще аппаратными средствами, соединенными на той же VLAN). Например, (*, Гр/м) соответствие для записи плотного режима, двойного-

Пакет групповой адресации, получающий мисс в Таблице FIB	class-copp-mcast-punt	rpf переключателя SPT. IP - адрес назначения (IP-адрес групповой адресации) является мисс в Таблице FIB. Пакет плывется на плоскодонке к программному обеспечению.
Непосредственно связанный источник (IPv4)	class-copp-ip-connected	Многоадресный трафик из непосредственно связанных источников передается программному обеспечению, где состояние групповой адресации может быть создано (и установлено в аппаратных средствах).
Непосредственно связанный источник (IPv6)	class-copp-ipv6-connected	Многоадресный трафик из непосредственно связанных источников передается программному обеспечению, где состояние групповой адресации может быть создано (и установлено в аппаратных средствах).
Транслируемый пакет	class-copp-broadcast	Транслируемые пакеты (например, IP/не-IP с широковещательным DMAC и одноадресный IP - трафик с DMAC Групповой адресации) пропущены к программному обеспечению.
Неизвестный протокол к (т.е. неподдерживаемый) с точки зрения аппаратной коммутации	class-copp-unknown-protocol	Протокол не-IP, такой как Межсетевой пакетный обмен (IPX) и так далее, не будет коммутированными аппаратными средствами. Они передаются программному обеспечению и переданы там.
Многоадресный трафик данных, прибывающий на пути маршрутизируемый порт, где отключен PIM	class-copp-mcast-v4-data-on-routedPort	Многоадресный трафик данных, который входит через маршрутизируемый порт (где PIM отключен) пропущен к программному обеспечению. Однако необязательно, чтобы передать им к программному обеспечению, таким образом, они отброшены.
Многоадресный трафик данных, прибывающий на пути маршрутизируемый порт, где отключен PIM	class-copp-mcast-v6-data-on-routedPort	Многоадресный трафик данных, который входит через маршрутизируемый порт (где PIM отключен) пропущен к программному обеспечению. Однако необязательно, чтобы передать им к программному обеспечению, таким образом, они отброшены.
Входное перенаправление ACL для мостового соединения пакета	class-copp-ucast-ingress-acl-bridged	Аппаратные средства имеют 8 связанных с ACL исключений, установленных программным обеспечением через

		перенаправление ACL. Этот касается одноадресных пакетов, соединенных к, ЦП ACL для Ternary Content Addressable Memory (TCAM) отнесся причины.
Выходное перенаправление ACL для мостового соединения пакета	class-copp-ucast-egress-acl-bridged	Аппаратные средства имеют 8 связанных с ACL исключений, установленных программным обеспечением через перенаправление ACL. Этот касается одноадресных пакетов, соединенных к, ЦП ACL для Ternary Content Addressable Memory (TCAM) отнесся причины.
ACL mcast перенаправляет к передачам пакета по мосту к ЦП	class-copp-mcast-acl-bridged	Аппаратные средства имеют 8 связанных с ACL исключений, установленных программным обеспечением через перенаправление ACL. Этот относится для групповой адресации обработки.
Мост ACL к ЦП для обработки Распределения нагрузки сервера	class-copp-slb	Аппаратные средства имеют 8 связанных с ACL исключений, установленных программным обеспечением через перенаправление ACL. Этот касается аппаратного перенаправления для решения Распределения нагрузки сервера (SLB).
VACL ACL регистрирует перенаправление	class-copp-vacl-log	Аппаратные средства имеют 8 связанных с ACL исключений, установленных программным обеспечением через перенаправление ACL. Этот касается перенаправления пакетов ACL Списка контроля доступом VLAN (VACL) к ЦП для Cisco IOS регистрация целей.
Отслеживание DHCP	class-copp-dhcp-snooping	DHCP snooping, пакеты перенаправлены к ЦП для Обработки DHCP
Политика MAC базирующаяся передача	class-copp-mac-pbf	Базирующаяся Передача политики должна быть сделана в ЦП, так как аппаратные средства не способны к передачам пакетов в этом случае.
Контроль доступа к сети ip admission	class-copp-ip-admission	Для обеспечения доступа к сети на основе антивирусных учетных данных хоста существует подтверждение состояния через одну из этих опций: (1) интерфейс L2 будет использовать IP Порта LAN (локальной сети) (LPIP), где пакеты

		Протокола ARP перенаправлены к ЦП, (2), L3 интерфейс использует IP шлюза (GWIP). После проверки существует аутентификация (*). Поскольку L2 взаимодействует, это - WebAuth, который выполняет перехват пакета HTTP и мог бы также выполнить перенаправление URL (*). Для L3 интерфейса это - AuthProxy.
Динамическая проверка ARP	class-copp-arp-snooping	Для предотвращения ARP, отравляющего (man-in-the-middle) атака, динамическая проверка ARP (также известный как Динамическая проверка ARP (DAI)) проверяет запросы/ответы ARP тем, когда это перехватывает и затем обрабатывает их в ЦП против одного из них: (1) настраиваемые ACL ARP (для статически настроенных хостов), (2) MAC-адрес к связываниям IP-адреса, сохраненным в доверяемой базе данных (т.е. связываниям DHCP). Только допустимые пакеты ARP используются для обновления локального кэша ARP или передаются. Процесс проверки данных требует участия ЦП пакетов ARP, что означает аппаратные средства, CoPP необходим для предотвращения атаки DoS.
Перенаправление ACL к ЦП для WCCP	class-copp-wccp	Используемый в случае, если пакет/поток должен быть перенаправлен к ЦП для решения по перенаправлению протокола WCCP.
Перенаправление ACL к ЦП для Сервисной архитектуры вставки (SIA)	class-copp-service-insertion	Используемый в случае, если пакет/поток должен быть перенаправлен к ЦП для решения SIA.
Обнаружение сети IPv6	class-copp-nd	Для перенаправления пакета Обнаружения сети IPv6 к ЦП для обработки далее. Ссылка: RFC4861

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Чтобы проверить, был ли трафик, наблюдаемый в каких-либо из настроенных карт классов CoPP, введите **команду show policy-map control-plane**.

Устранение неполадок

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

Дополнительные сведения

- Защищая коммутаторы Cisco Catalyst серии 6500 Использование контроля уровня управления, аппаратного ограничения скорости и списков управления доступом
- Руководство по конфигурации программного обеспечения выпуска 15.0SY Catalyst 6500 - контроль уровня управления (CoPP)
- Cisco Systems – техническая поддержка и документация