CoPP على سلسلة مبدلات Nexus 7000

المحتويات

المقدمة

يصف هذا وثيقة ماذا، كيف، ولماذا يتم إستخدام تنظيم مستوى التحكم (CoPP) على محولات Nexus 7000 Series Switches، والتي تتضمن الوحدات النمطية من السلسلة M1، F1، F2، و M2 وبطاقات الخط (LCs). كما يتضمن سياسات أفضل الممارسات، فضلا عن كيفية تخصيص سياسة CoPP.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة ب CLI لنظام تشغيل Nexus.

المكونات المستخدمة

أسست المعلومة في هذا وثيقة على ال nexus 7000 sery مفتاح مع مشرف 1 وحدة نمطية.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

نظرة عامة على المحول CoPP على السلسلة Nexus 7000 Series Switch

يعد CoPP أمرا بالغ الأهمية لتشغيل الشبكة. عادة ما يتضمن هجوم رفض الخدمة (DoS) على مستوى التحكم/الإدارة، والذي يمكن تنفيذه إما بشكل غير مقصود أو بشكل غير مقصود، معدلات مرور مرتفعة مما يؤدي إلى الاستخدام المفرط لوحدة المعالجة المركزية. تنفق وحدة المشرف مقدار مفرط من الوقت معالجة الحزم.

الأمثلة على مثل هذه الهجمات تشمل:

- طلبات صدى بروتوكول رسائل التحكم في الإنترنت (ICMP).
- الحزم المرسلة مع مجموعة **خيارات IP**.

ويمكن أن يؤدي ذلك إلى ما يلي:

- فقدان رسائل الاحتفاظ بالحياة وتحديثات بروتوكول التوجيه.
- تعبئة قوائم انتظار الحزم، مما يؤدي إلى حالات إسقاط عشوائي.
- جلسات تفاعلية بطيئة أو غير مستجيبة.

يمكن أن تؤثر الهجمات على إستقرار الشبكة وتوافرها وتؤدي إلى حالات انقطاع عن الشبكة تؤثر على الشركات.

CoPP هي ميزة قائمة على الأجهزة تحمي المشرف من هجمات رفض الخدمة (DoS). وهو يتحكم في معدل السماح للحزم بالوصول إلى المشرف. يتم تكوين ميزة CoPP مثل سياسة جودة الخدمة الخاصة بالإدخال المرفقة بالواجهة الخاصة التي تسمى **مستوى التحكم**. ومع ذلك، فإن CoPP هو ميزة أمان وليس جزءا من جودة الخدمة. لحماية المشرف، يفصل CoPP حزم مستوى البيانات من حزم مستوى التحكم (منطق الاستثناء). وهو يحدد حزم هجوم رفض الخدمة (DoS) من الحزم الصالحة (التصنيف). يسمح CoPP بتصنيف هذه الحزم:

- إستقبال الحزم
- حزم البث المتعدد
- حزم الاستثناء
- إعادة توجيه الحزم
- حزم Broadcast MAC + غير IP
- حزم Broadcast MAC + IP (راجع معرف تصحيح الأخطاء من CSCub47533 Cisco - الحزم في شبكة L2 VLAN (لا SVI) التي تصل CoPP)
- حزم MAC + IP للبث
- MAC للموجه + حزم غير خاصة ب IP
- حزم ARP

بعد تصنيف الحزمة، يمكن أيضا تمييز الحزمة واستخدامها لتعيين أولويات مختلفة استنادا إلى نوع الحزم. يمكن تعيين مطابقة الإجراءات وتجاوزها وانتهاكها (الإرسال والإفلات ووضع علامة للأسفل). إذا لم يتم إرفاق أي منظم بفئة، تتم إضافة منظم افتراضي يكون إجراء التوافق الخاص به هو الإسقاط. يتم تنظيم حزم GLEAN باستخدام الفئة الافتراضية. بمعدل واحد، لونين، بمعدل إثنين، ثلاثة تنسيق ألوان مدعومة.

يمكن لحركة المرور التي تصل إلى وحدة المعالجة المركزية (CPU) على الوحدة النمطية "المشرف" أن تأتي من خلال أربعة مسارات:

1. واجهات داخل النطاق (منفذ اللوحة الأمامية) لحركة المرور التي يتم إرسالها بواسطة بطاقات الخط.

2. واجهة الإدارة (mgmt0) المستخدمة لحركة مرور الإدارة.

3. واجهة معالج التحكم والمراقبة (CMP) المستخدمة لوحدة التحكم.

4. قناة النطاق الخارجي للإيثرنت (EOBC) المحولة للتحكم في بطاقات الخط من الوحدة النمطية للمشرف ورسائل حالة التبادل.

تخضع حركة المرور المرسلة من خلال واجهة النطاق الداخلي إلى CoPP، لأن هذه هي حركة المرور الوحيدة التي تصل إلى الوحدة النمطية للمشرف من خلال محركات إعادة التوجيه (FEs) على بطاقات الخط. يكون تنفيذ محول Nexus 7000 Series Switch ل CoPP مستند إلى الأجهزة فقط، مما يعني أن CoPP لا يتم تنفيذها في البرنامج بواسطة الوحدة النمطية للمشرف. يتم تنفيذ وظائف CoPP (تنظيم) على كل FE بشكل مستقل. عند تكوين مختلف المعدلات لخريطة سياسات CoPP، يجب الأخذ بعين الاعتبار عدد بطاقات الخط في النظام.

يبلغ إجمالي حركة المرور التي يتلقاها المشرف X × n، حيث يمثل N عدد رسائل التحكم في الوصول إلى البنية الأساسية (FE) على نظام Nexus 7000، ويمثل X المعدل المسموح به للفئة المحددة. يتم تطبيق قيم واضع السياسات التي تم تكوينها على أساس كل حالة وصول إلى الخادم (FE)، وتمثل حركة مرور البيانات المجمعة المعرضة للوصول إلى وحدة المعالجة المركزية (CPU) مجموع حركة المرور المتزامنة والمنقولة على جميع شبكات FE. وبمعنى آخر، فإن حركة المرور التي تصل إلى وحدة المعالجة المركزية تساوي معدل التوافق الذي تم تكوينه مضروبا في عدد رسائل التحكم في الوصول إلى النقل (FEs).

- N7K-M148GT-11/L LC به 1 FE
- N7K-M148GS-11/L LC به 1 FE
- N7K-M132XP-12/L LC به 1 FE
- N7K-M108X2-12L LC به 2 FE
- N7K-F248XP-15 LC تحتوي على 12 SOC) FE)
- N7K-M235XP-23L LC به 2 FE
- N7K-M206FQ-23L LC به 2 FE
- N7K-M202CF-23L LC به 2 FE

يتم تنفيذ تكوين CoPP فقط في سياق الجهاز الظاهري الافتراضي (VDC)، ومع ذلك، فإن سياسات CoPP قابلة للتطبيق على جميع VDCs. يتم تطبيق نفس السياسة العامة على جميع بطاقات الخط. يطبق CoPP مشاركة الموارد بين VDCs إن ينتسب ميناء من ال نفسه FEs إلى VDCs مختلف (M1 Series أو M2 Series LC). على سبيل المثال، تعد المنافذ الخاصة ب FE واحد، حتى في نقاط VDC المختلفة، مقابل نفس العتبة ل CoPP.

إن ال نفسه FE يكون شاركت بين VDCs مختلف وفئة معطاة من التحكم مستوى حركة مرور يتجاوز الحد، هذا يؤثر كل VDCs على ال نفسه FE. يوصى بتخصيص FE واحد لكل VDC لعزل تنفيذ CoPP، إن أمكن.

عند ظهور المحول لأول مرة، يجب برمجة السياسة الافتراضية لحماية **مستوى التحكم**. يوفر CoPP السياسات الافتراضية، والتي يتم تطبيقها على **مستوى التحكم** كجزء من تسلسل بدء التشغيل الأولي.

لماذا CoPP على محول Nexus 7000 Series Switch

يتم نشر المحول من السلسلة Nexus 7000 كمحول تجميع أو محول أساسي. وبالتالي، فهي أذن ودماغ الشبكة. وهو يعالج الحد الأقصى للتحميل في الشبكة. ويجب أن يعالج الطلبات المتكررة والمفاجئة. وتتضمن بعض الطلبات ما يلي:

- **معالجة وحدة بيانات بروتوكول الجسر للشجرة المتفرعة (BPDU)** - بشكل افتراضي كل ثانيتين.

- **تكرار الخطوة الأولى** - يتضمن هذا بروتوكول موجه الاستعداد السريع (HSRP) وبروتوكول تكرار الموجه الظاهري (VRRP) وبروتوكول موازنة حمل العبارة (GLBP) - يكون الإعداد الافتراضي كل ثلاث ثوان.

- **تحليل العنوان** - يتضمن هذا بروتوكول تحليل العنوان/اكتشاف الجوار (ARP/ND)، تكوين قاعدة معلومات إعادة التوجيه (FIB) - ما يصل إلى طلب واحد في الثانية، لكل مضيف، مثل تكوين فريق وحدة تحكم واجهة الشبكة (NIC).

- **بروتوكول التحكم في المضيف الديناميكي (DHCP)** - طلب DHCP، ترحيل - ما يصل إلى طلب واحد في الثانية، لكل مضيف.

- **بروتوكولات التوجيه** للطبقة 3 (L3).

- Data Center Interconnect - المحاكاة الظاهرية للنقل الفرعي (OTV)، تحويل التسمية متعدد البروتوكولات (MPLS)، وخدمة شبكة المنطقة المحلية الخاصة الظاهرية (VPLS).

يعد CoPP ضروريا لحماية وحدة المعالجة المركزية (CPU) من الخوادم التي تم تكوينها بشكل غير صحيح أو هجمات رفض الخدمة (DoS) المحتملة، مما يسمح لوحدة المعالجة المركزية بامتلاك دورة كافية لمعالجة رسائل مستوى التحكم الهامة.

معالجة مستوى التحكم على المحول Nexus 7000 Series Switch

يأخذ المحول من السلسلة Nexus 7000 نهج مستوى التحكم الموزع. كما يحتوي على متعدد المراكز على كل وحدة إدخال/إخراج، بالإضافة إلى متعدد المراكز لمستوى التحكم في المحول على الوحدة النمطية Supervisor. فهو يقوم بإلغاء تحميل المهام المكثفة إلى وحدة المعالجة المركزية (CPU) لوحدة الإدخال/الإخراج الخاصة بقوائم التحكم في الوصول (ACL) وبرامج FIB. وهو يعمل على زيادة سعة مستوى التحكم باستخدام عدد بطاقات الخط. ويتجنب هذا الأمر حدوث إختناق مع المشرف على وحدة المعالجة المركزية (CPU)، والذي يظهر من خلال النهج المركزي. تقوم أدوات تحديد معدل الأجهزة و CoPP المستندة إلى الأجهزة بحماية مستوى التحكم من الأنشطة الضارة أو الضارة.

سياسة أفضل الممارسات ل CoPP

تم تقديم سياسة أفضل الممارسات (BPP) ل Cisco NX-OS، الإصدار 5.2. لا يعرض إخراج الأمر **show running-config** محتوى CoPP. يعرض أمر **show run all** محتوى CoPP.

```
----------------------------------------SNIP-----------------------------------
SITE1-AGG1# show run copp

Command: show running-config copp !!
    Time: Mon Nov 5 22:21:04 2012 !!

                                    (version 5.2(7
                                copp profile strict


SITE1-AGG1# show run copp all

Command: show running-config copp all !!
        Time: Mon Nov 5 22:21:15 2012 !!

                                    (version 5.2(7
---------------------SNIP-------------------------------
                                    control-plane
                            service-policy input copp-system-p-policy-strict
                                copp profile strict
```

يوفر CoPP أربعة خيارات للمستخدم للنهج الافتراضية:

- صارم
- متوسط
- متساهل
- الكثافة (مقدمة في الإصدار 6.0(1))

في حالة عدم تحديد أي خيار أو في حالة تخطي الإعداد، يتم تطبيق تنظيم صارم. تستخدم كل هذه الخيارات نفس فئات وخرائط الفئة، لكن قيم معدل المعلومات الإلزامية (CIR) المختلفة وعدد الاندفاع (BC) للتنظيم. في إصدارات Cisco NX-OS الأقدم من 5.2.1، تم إستخدام أمر **الإعداد** لتغيير الخيار. أدخل Cisco NX-OS، الإصدار 5.2.1 تحسين على CoPP حتى يمكن تغيير الخيار دون أمر **الإعداد**؛ أستخدم الأمر **coPP profile**.

```
SITE1-AGG1# conf t
.Enter configuration commands, one per line. End with CNTL/Z
? SITE1-AGG1(config)# copp profile
  dense The Dense Profile
  lenient The Lenient Profile
  moderate The Moderate Profile
  strict The Strict Profile
SITE1-AGG1(config)# copp profile strict
SITE1-AGG1(config)# exit
```

أستخدم الأمر **show coPP profile <profile-type>**لعرض تكوين CoPP الافتراضي. أستخدم الأمر **show coPP status** للتحقق من تطبيق سياسة CoPP بشكل صحيح.

```
SITE1-AGG1# show copp status
Last Config Operation: copp profile strict
Last Config Operation Timestamp: 20:40:27 PST Nov 5 2012
Last Config Operation Status: Success
Policy-map attached to the control-plane: copp-system-p-policy-strict
```

لعرض الفرق بين حزمتي CoPP BPP، أستخدم الأمر **show copp diff profile <profile-type 1> profile <<profile-type 2**:

```
SITE1-AGG1# show copp diff profile strict profile moderate
A '+' represents a line that has been added and
.a '-' represents a line that has been removed
policy-map type control-plane copp-system-p-policy-strict-
                class copp-system-p-class-critical -
                    set cos 7 -
  police cir 39600 kbps bc 250 ms conform transmit violate drop -
                class copp-system-p-class-important -
                    set cos 6 -
  police cir 1060 kbps bc 1000 ms conform transmit violate drop -
---------------------------------------SNIP----------------------
    policy-map type control-plane copp-system-p-policy-moderate+
                class copp-system-p-class-critical +
                    set cos 7 +
  police cir 39600 kbps bc 310 ms conform transmit violate drop +
                class copp-system-p-class-important +
                    set cos 6 +
  police cir 1060 kbps bc 1250 ms conform transmit violate drop +
---------------------------------------SNIP----------------------
```

كيفية تخصيص سياسة CoPP

يمكن للمستخدمين إنشاء سياسة CoPP مخصصة. قم باستنساخ بروتوكول CoPP الافتراضي، وألصقه بواجهة

التحكم-plane لأن CoPP هو للقراءة فقط.

```
SITE2-AGG1(config)# policy-map type control-plane copp-system-p-policy-strict
                                                                           ^
String is invalid, 'copp-system-p-policy-strict' is not an allowed string at %
.marker '^'
```

يقوم الأمر **[CoPP copy profile <profile-type> <prefix> <suffix]** بإنشاء نسخة من CoPP BPP. ويتم إستخدام هذا الأمر لتعديل التكوينات الافتراضية. الأمر **coPP copy profile** هو أمر وضع **exec**. يمكن للمستخدم إختيار بادئة أو لاحقة لاسم قائمة الوصول ومخططات الفئة وخرائط السياسة. على سبيل المثال، يتم تغيير **CoPP-system-p-policy-strict** إلى **[prefix]CoPP-policy-strict[suffix]**. يتم التعامل مع التكوينات المستنسخة كتكوينات مستخدم ويتم تضمينها في إخراج **show run**.

```
SITE1-AGG1# copp copy profile ?
  dense The Dense Profile
  lenient The Lenient Profile
  moderate The Moderate Profile
  strict The Strict Profile
SITE1-AGG1# copp copy profile strict ?
  prefix Prefix for the copied policy
  suffix Suffix for the copied policy
SITE1-AGG1# copp copy profile strict suffix ?
  WORD Enter prefix/suffix for the copied policy (Max Size 20)
SITE1-AGG1# copp copy profile strict suffix CUSTOMIZED-COPP
SITE1-AGG1# show run copp | grep policy-map
policy-map type control-plane copp-policy-strict-CUSTOMIZED-COPP
SITE1-AGG1#
```

من الممكن تعليم حركة المرور التي تتجاوز وتتنهك معدل المعلومات المسموح به المحدد (PIR) باستخدام الأوامر التالية:

```
SITE1-AGG1(config)# policy-map type
control-plane copp-policy-strict-CUSTOMIZED-COPP
SITE1-AGG1(config-pmap)# class copp-class-critical-CUSTOMIZED-COPP
SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms
?
  <CR>
  conform Specify a conform action
  pir Specify peak information rate

SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms pir
?
  Peak Information Rate in bps/kbps/mbps/gbps <1-80000000000>

SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms pir 100 mbps
?
  <CR>
  Peak Burst Size in bytes/kbytes/mbytes/packets/ms/us <1-512000000>
  be Specify extended burst
  conform Specify a conform action

SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms pir 100 mbps conform
?
  drop Drop the packet
  set-cos-transmit Set conform action cos val
  set-dscp-transmit Set conform action dscp val
  set-prec-transmit Set conform action precedence val
  transmit Transmit the packet

SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms pir 100 mbps conform
set-dscp-transmit ef exceed set dscp1 dscp2 table cir-markdown-map violate
set1 dscp3 dscp4 table1 pir-markdown-map
#(SITE1-AGG1(config-pmap-c
```

تطبيق سياسة CoPP المخصصة على **مستوى تحكم** الواجهة العامة. أستخدم الأمر **show coPP status** للتحقق من تطبيق سياسة CoPP بشكل صحيح.

```
SITE1-AGG1# conf t
.Enter configuration commands, one per line. End with CNTL/Z
SITE1-AGG1(config)# control-plane
? SITE1-AGG1(config-cp)# service-policy input
copp-policy-strict-CUSTOMIZED-COPP

SITE1-AGG1(config-cp)# service-policy input copp-policy-strict-CUSTOMIZED-COPP
SITE1-AGG1(config-cp)# exit
SITE1-AGG1# sh copp status
Last Config Operation: service-policy input copp-policy-strict-CUSTOMIZED-COPP
Last Config Operation Timestamp: 18:04:03 UTC May 15 2012
Last Config Operation Status: Success
Policy-map attached to the control-plane: copp-policy-strict-CUSTOMIZED-COPP
```

دراسة حالة لسياسة CoPP المخصصة

يصف هذا القسم مثالا حقيقيا يتطلب فيه العميل أجهزة مراقبة متعددة من أجل إختبار الاتصال للواجهات المحلية بشكل متكرر. تمت مواجهة صعوبة في هذا السيناريو عندما يريد العميل تعديل سياسة CoPP من أجل:

- قم بزيادة CIR حتى يمكن لهذه العناوين المحددة إختبار اتصال الجهاز المحلي وعدم انتهاك السياسة.
- السماح لعناوين IP الأخرى بالحفاظ على القدرة على إختبار اتصال الجهاز المحلي، ولكن في محرك CIR أقل لأغراض أستكشاف الأخطاء وإصلاحها.

يتم عرض الحل في المثال التالي، وهو إنشاء سياسة مخصصة باستخدام خريطة فئة منفصلة. تحتوي خريطة الفئة المنفصلة على عناوين IP المحددة لأجهزة المراقبة وتحتوي خريطة الفئة على عنوان CIR أعلى. وهذا يؤدي أيضا إلى ترك *مراقبة* خريطة الفئة الأصلية، والتي على قبض حركة مرور ICMP لجميع عناوين IP الأخرى في معرف فئة مورد (CIR) أقل.

```
F340.13.19-Nexus7000-1#
F340.13.19-Nexus7000-1#
F340.13.19-Nexus7000-1# conf t
.Enter configuration commands, one per line. End with CNTL/Z
F340.13.19-Nexus7000-1(config)# copp copy profile strict prefix TAC_CHANGE
#(F340.13.19-Nexus7000-1(config
#(F340.13.19-Nexus7000-1(config
F340.13.19-Nexus7000-1(config)# ip access-list TAC_CHANGE-copp-acl-specific-icmp
#(F340.13.19-Nexus7000-1(config-acl
F340.13.19-Nexus7000-1(config-acl)# permit icmp host 1.1.1.1 host 2.2.2.2 echo
F340.13.19-Nexus7000-1(config-acl)# permit icmp host 1.1.1.1 host 2.2.2.2 echo-reply
#(F340.13.19-Nexus7000-1(config-acl
F340.13.19-Nexus7000-1(config-acl)# exit
-F340.13.19-Nexus7000-1(config)# sho ip access-lists TAC_CHANGE-copp-acl-specific
icmp IP access list TAC_CHANGE-copp-acl-specific-icmp
permit icmp 1.1.1.1/32 2.2.2.2/32 echo 10
permit icmp 1.1.1.1/32 2.2.2.2/32 echo-reply 20
#(F340.13.19-Nexus7000-1(config
#(F340.13.19-Nexus7000-1(config
F340.13.19-Nexus7000-1(config)# class-map type control-plane match-any
TAC_CHANGE-copp-class-specific-icmp
F340.13.19-Nexus7000-1(config-cmap)# match access-group name TAC_CHANGE-copp
acl-specific-icmp-
F340.13.19-Nexus7000-1(config-cmap)#exit
#(F340.13.19-Nexus7000-1(config
```

```
-F340.13.19-Nexus7000-1(config)#policy-map type control-plane TAC_CHANGE-copp
                                                                policy-strict
F340.13.19-Nexus7000-1(config-pmap)# class TAC_CHANGE-copp-class-specific-icmp
                                                                insert-before
                                                  TAC_CHANGE-copp-class-monitoring
                                               F340.13.19-Nexus7000-1(config-pmap-c)# set cos 7
F340.13.19-Nexus7000-1(config-pmap-c)# police cir 5000 kbps bc 250 ms conform transmit
                                                                violate drop
                                             F340.13.19-Nexus7000-1(config-pmap-c)# exit
                                                    #(F340.13.19-Nexus7000-1(config-pmap
                                                    #(F340.13.19-Nexus7000-1(config-pmap
                                                    #(F340.13.19-Nexus7000-1(config-pmap
                                                    #(F340.13.19-Nexus7000-1(config-pmap
                                               F340.13.19-Nexus7000-1(config-pmap)# exit
                                                        #(F340.13.19-Nexus7000-1(config
                                                        #(F340.13.19-Nexus7000-1(config
                                             F340.13.19-Nexus7000-1(config)# control-plane
 F340.13.19-Nexus7000-1(config-cp)# service-policy input TAC_CHANGE-copp-policy-strict
                                                 F340.13.19-Nexus7000-1(config-cp)# end
                                                                F340.13.19-Nexus7000-1#
                                 F340.13.19-Nexus7000-1# sho policy-map interface control-plane
                                                                Control Plane
                                                 service-policy input TAC_CHANGE-copp-policy-strict
                                                                <abbreviated output>
                                          (class-map TAC_CHANGE-copp-class-specific-icmp (match-any
                                         match access-group name TAC_CHANGE-copp-acl-specific-icmp
                                                                set cos 7
                                                       police cir 5000 kbps bc 250 ms
                                                             conform action: transmit
                                                                 violate action: drop
                                                                          :module 4
                                                                    ,conformed 0 bytes
                                                       5-min offered rate 0 bytes/sec
                                                                peak rate 0 bytes/sec
                                                                    ,violated 0 bytes
                                                       5-min violate rate 0 bytes/sec
                                                                peak rate 0 bytes/sec
                                                                          :module 7
                                                                    ,conformed 0 bytes
                                                       5-min offered rate 0 bytes/sec
                                                                peak rate 0 bytes/sec
                                                                    ,violated 0 bytes
                                                       5-min violate rate 0 bytes/sec
                  (peak rate 0 bytes/secclass-map TAC_CHANGE-copp-class-monitoring (match-any
                                                 match access-group name TAC_CHANGE-copp-acl-icmp
                                                match access-group name TAC_CHANGE-copp-acl-icmp6
                                              match access-group name TAC_CHANGE-copp-acl-mpls-oam
                                            match access-group name TAC_CHANGE-copp-acl-traceroute
                                          match access-group name TAC_CHANGE-copp-acl-http-response
                                          match access-group name TAC_CHANGE-copp-acl-smtp-response
                                        match access-group name TAC_CHANGE-copp-acl-http6-response
                                        match access-group name TAC_CHANGE-copp-acl-smtp6-response
                                                                set cos 1
                                                       police cir 130 kbps bc 1000 ms
                                                             conform action: transmit
                                                                 violate action: drop
                                                                          :module 4
                                                                    ,conformed 0 bytes
                                                       5-min offered rate 0 bytes/sec
                                                                peak rate 0 bytes/sec
                                                                    ,violated 0 bytes
                                                       5-min violate rate 0 bytes/sec
                                                                peak rate 0 bytes/sec
                                                                          :module 7
```

```
,conformed 0 bytes
5-min offered rate 0 bytes/sec
peak rate 0 bytes/sec
,violated 0 bytes
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
<abbreviated output>
```

بنية بيانات CoPP

يتم إنشاء بنية بيانات CoPP BPP على النحو التالي:

- **تكوين قائمة التحكم في الوصول (ACL)**: قوائم التحكم في الوصول (ACL) إلى IP و MAC.
- **تكوين المصنف**: قائمة التحكم في الوصول (ACL) أو MAC المطابقة لبروتوكول IP على خريطة الفئة.
- **تكوين واضع السياسات**: تعيين CIR و BC ومطابقة الإجراء وانتهاك الإجراء. الشرطى له معدلان (CIR و BC)، ولونان (مطابقة ومخالفة).

```
mac access-list copp-system-p-acl-mac-fabricpath-isis
permit any 0180.c200.0015 0000.0000.0000
permit any 0180.c200.0014 0000.0000.0000

ip access-list copp-system-p-acl-bgp
permit tcp any gt 1024 any eq bgp
permit tcp any eq bgp any gt 1024

class-map type control-plane match-any copp-system-p-class-critical
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-pim
<snip>
match access-group name copp-system-p-acl-mac-fabricpath-isis
policy-map type control-plane copp-system-p-policy-dense
class copp-system-p-class-critical
set cos 7
police cir 5000 kbps bc 250 ms conform transmit violate drop
```

عامل مقياس CoPP

يتم إستخدام تكوين عامل النطاق الذي تم تقديمه في الإصدار 6.0 من Cisco NX-OS لقياس معدل الشرطي لسياسة CoPP المطبقة لبطاقة خط معينة. يؤدي ذلك إلى زيادة أو تقليل معدل المنظم لبطاقة خط معينة، ولكنه لا يغير سياسة CoPP الحالية. تسري التغييرات فورا، ولا حاجة إلى إعادة تطبيق سياسة CoPP.

```
:scale factor option configured within control-plane interface
<Scale-factor <scale factor value> module <module number
scale factor value>: from 0.10 to 2.00>
Scale factor is recommended when a chassis is loaded with both F2 and M
.Series modules
SITE1-AGG1# conf t
.Enter configuration commands, one per line. End with CNTL/Z
SITE1-AGG1(config)# control-plane
? SITE1-AGG1(config-cp)# scale-factor
whole>.<decimal> Specify scale factor value from 0.10 to 2.00>

? SITE1-AGG1(config-cp)# scale-factor 1.0
```

```
module Module

? SITE1-AGG1(config-cp)# scale-factor 1.0 module
Specify module number <1-10>

SITE1-AGG1(config-cp)# scale-factor 1.0 module 4
SITE1-AGG1# show system internal copp info
<snip>
:Linecard Configuration
----------------------
Scale Factors
Module 1: 1.00
Module 2: 1.00
Module 3: 1.00
Module 4: 1.00
Module 5: 1.00
Module 6: 1.00
Module 7: 1.00
Module 8: 1.00
Module 9: 1.00
Module 10: 1.00
```

إدارة ومراقبة CoPP

باستخدام الإصدار 5.1 من Cisco NX-OS، من الممكن تكوين حد إسقاط لكل اسم فئة CoPP الذي يشغل رسالة syslog في حالة تجاوز الحد. الأمر هو **حد تسجيل الإسقاط <عدد البايت المسقط> مستوى <logging level>**.

```
SITE1-AGG1(config)# policy-map type control-plane
copp-policy-strict-CUSTOMIZED-COPP
SITE1-AGG1(config-pmap)# class copp-class-critical-CUSTOMIZED-COPP
? SITE1-AGG1(config-pmap-c)# logging
drop Logging for dropped packets

? SITE1-AGG1(config-pmap-c)# logging drop
threshold Threshold value for dropped packets

? SITE1-AGG1(config-pmap-c)# logging drop threshold
<CR>
Dropped byte count <1-80000000000>

? SITE1-AGG1(config-pmap-c)# logging drop threshold 100
<CR>
level Syslog level

? SITE1-AGG1(config-pmap-c)# logging drop threshold 100 level
Specify the logging level between 1-7 <1-7>

SITE1-AGG1(config-pmap-c)# logging drop threshold 100 level 7
```

هنا مثال من syslog رسالة:

```
:COPP-5-COPP_DROPS5: CoPP drops exceed threshold in class%
,copp-system-class-critical
.check show policy-map interface control-plane for more info
```

عدادات CoPP

يدعم CoPP نفس إحصائيات جودة الخدمة مثل أي واجهة أخرى. وهو يعرض إحصائيات الفئات التي تشكل سياسة

الخدمة لكل وحدة إدخال/إخراج تدعم CoPP. أستخدم الأمر **show policy-map interface control-plane** لعرض إحصائيات CoPP.

ملاحظة: يجب مراقبة جميع الفئات من حيث الحزم المنتهكة.

```
SITE1-AGG1# show policy-map interface control-plane
Control Plane

service-policy input: copp-policy-strict-CUSTOMIZED-COPP

(class-map copp-class-critical-CUSTOMIZED-COPP (match-any
match access-group name copp-acl-bgp-CUSTOMIZED-COPP
match access-group name copp-acl-bgp6-CUSTOMIZED-COPP
match access-group name copp-acl-eigrp-CUSTOMIZED-COPP
match access-group name copp-acl-igmp-CUSTOMIZED-COPP
match access-group name copp-acl-msdp-CUSTOMIZED-COPP
match access-group name copp-acl-ospf-CUSTOMIZED-COPP
match access-group name copp-acl-ospf6-CUSTOMIZED-COPP
match access-group name copp-acl-pim-CUSTOMIZED-COPP
match access-group name copp-acl-pim6-CUSTOMIZED-COPP
match access-group name copp-acl-rip-CUSTOMIZED-COPP
match access-group name copp-acl-rip6-CUSTOMIZED-COPP
match access-group name copp-acl-vpc-CUSTOMIZED-COPP
match access-group name copp-acl-eigrp6-CUSTOMIZED-COPP
match access-group name copp-acl-mac-l2pt-CUSTOMIZED-COPP
match access-group name copp-acl-mpls-ldp-CUSTOMIZED-COPP
match access-group name copp-acl-mpls-oam-CUSTOMIZED-COPP
match access-group name copp-acl-mpls-rsvp-CUSTOMIZED-COPP
match access-group name copp-acl-otv-as-CUSTOMIZED-COPP
match access-group name copp-acl-mac-otv-isis-CUSTOMIZED-COPP
match access-group name copp-acl-mac-fabricpath-isis-CUSTOMIZED-COPP
match protocol mpls router-alert
match protocol mpls exp 6
set cos 7
threshold: 100, level: 7
police cir 39600 kbps , bc 250 ms
: module 1
conformed 22454 bytes; action: transmit
violated 0 bytes; action: drop

: module 2
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop

: module 3
conformed 19319 bytes; action: transmit
violated 0 bytes; action: drop

: module 4
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
```

للحصول على طريقة عرض إجمالية للعدادات المتوافقة والمخالفة لجميع وحدات الإدخال/الإخراج وخرائط الفئة، أستخدم **مستوى التحكم في الواجهة** | **show policy-map** الأمر **"class|compatible|violation"**.

```
"SITE1-AGG1# show policy-map interface control-plane | i "class|conform|violated
(class-map copp-class-critical-CUSTOMIZED-COPP (match-any
conformed 123126534 bytes; action: transmit
violated 0 bytes; action: drop
```

```
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
conformed 107272597 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
(class-map copp-class-important-CUSTOMIZED-COPP (match-any
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
```

يجب مراقبة **الفئة CoPP-class-l2-default والفئة-default** لضمان عدم وجود زيادات عالية، حتى للعدادات المتوافقة. من الناحية المثالية، يجب أن يكون لهذين الصنفين قيم منخفضة للعداد المتزامن وعدم حدوث زيادة عداد منتهكة على الأقل.

عدادات ACL

لا يتم دعم الأمر **statistics per-entry** لقائمة التحكم بالوصول إلى IP أو قائمة التحكم بالوصول إلى MAC المستخدمة في خريطة فئة CoPP، وليس له تأثير عند تطبيقه على قائمة التحكم بالوصول إلى IP الخاصة ب CoPP أو قائمة التحكم بالوصول الخاصة بالتحكم في الوصول إلى Mac. (لا يوجد فحص CLI تم بواسطة محلل واجهة سطر الأوامر). لعرض مرات وصول قائمة التحكم في الوصول ل CoPP MAC أو قوائم التحكم في الوصول إلى IP على وحدة الإدخال/الإخراج، أستخدم أمر **show system internal access-list input detail**.

فيما يلي مثال:

```
c200.0041 is the destination MAC used for FabricPath IS-IS.0180 !!

SITE1-AGG1# show system internal access-list input entries det | grep 0180.c200.0041
[00fc:00f7:00f7] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [30042]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [29975]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [8965]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [8935]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [58233]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [27689]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[00fc:00f7:00f7] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
```

```
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
```

أفضل ممارسات تكوين CoPP

هذه توصيات بأفضل الممارسات لتكوين CoPP:

- أستخدم وضع CoPP المقيد بشكل افتراضي.
- يوصى بملف تعريف CoPP الكثيف عند تحميل الهيكل بالكامل بوحدات F2 Series أو تحميله بوحدات أكثر من فئة F2 مقارنة بأي وحدات إدخال/إخراج أخرى.
- لا يوصى بتعطيل CoPP. قم بضبط CoPP الافتراضي، حسب الحاجة.
- مراقبة عمليات الإسقاط غير المقصودة، وإضافة سياسة CoPP الافتراضية أو تعديلها وفقا لحركة المرور المتوقعة.
- استنادا إلى عدد وحدات FE في الهيكل، يمكن زيادة أو تقليل إعدادات CIR و BC ل CoPP. وهذا أيضا استنادا إلى دور الأجهزة الموجودة على الشبكة والبروتوكولات قيد التشغيل وما إلى ذلك.
- لأن أنماط حركة المرور تتغير باستمرار في **مركز البيانات**، فإن تخصيص CoPP هو عملية ثابتة.
- CoPP و VDC: يجب أن تنتمي جميع المنافذ التي لها نفس FE إلى نفس VDC، وهو أمر سهل بالنسبة إلى وحدة التحكم LC من السلسلة F2، ولكنه ليس بالسهولة نفسها بالنسبة للفئة M2 أو LC M108. وهذا يرجع لأن مشاركة موارد CoPP بين VDCs إذا كانت المنافذ من نفس FE تنتمي إلى VDCs مختلفة (M1 Series أو M2 Series LC). يعتد الميناء من واحد FE، حتى في VDCs مختلف، ضد ال نفسه عتبة ل CoPP.
- يوصى بتكوين عامل المقياس عند تحميل هيكل بوحدات كل من الفئة F2 والفئة M.

أفضل ممارسات مراقبة CoPP

وهذه توصيات بشأن أفضل الممارسات لرصد البرامج التعاونية:

- قم بتكوين حد رسالة syslog ل CoPP (الإصدار 5.1 من Cisco NX-OS) لمراقبة حالات السقوط التي يتم فرضها بواسطة CoPP.
- يتم إنشاء رسائل syslog إذا تجاوزت عمليات السقوط داخل فئة حركة مرور البيانات الحد الذي قام المستخدم بتكوينه.
- يمكن تخصيص حد التسجيل ومستواه داخل كل فئة من فئات حركة المرور باستخدام الأمر **packet-count>> level <level>**لحد **إسقاط التسجيل**.
- نظرا لأن خيار "إحصائيات لكل إدخال" لقائمة التحكم بالوصول إلى MAC أو قائمة التحكم بالوصول إلى IP ACL)) إلى CoPP غير مدعوم، أستخدم الأمر **show system internal access list input input** لمراقبة عمليات الوصول إلى إدخالات التحكم في الوصول (ACE).
- يجب مراقبة الأمر **class coPP-class-l2-default و**class-default لضمان عدم وجود زيادات عالية، حتى بالنسبة للعدادات المتوافقة.

- يجب مراقبة جميع الفئات فيما يتعلق بالحزم المتهكة.

نظرا لأن **CoPP-Class-Critical** حيوي للغاية ولكن لديه سياسة **إسقاط خاطئة**، فمن الممارسات الجيدة مراقبة معدل الحزم المتوافقة للحصول على إشارة مبكرة عندما يصبح الفصل قريبا من اللحظة التي يبدأ فيها الانتهاك. إذا زاد العداد المخالف لهذه الفئة، لا يعني ذلك بالضرورة تنبيه أحمر. بل يعني أن هذه الحالة يجب التحقيق فيها على المدى القصير.

- أستخدم الأمر **coPP profile strict** بعد كل ترقية لرمز Cisco NX-OS، أو على الأقل بعد كل ترقية لرمز Cisco NX-OS رئيسي؛ إذا تم إكمال تعديل CoPP مسبقا، فيجب إعادة تطبيقه.

الخلاصة

- CoPP هي ميزة قائمة على الأجهزة تحمي المشرف من هجمات رفض الخدمة (DoS).
- تدعم بطاقات LC من السلسلة M1 و F2 و F1 sery LCs. M2 Series CoPP لا يساند CoPP.
- تكوين CoPP مماثل ل MQC (واجهة سطر الأوامر لجودة خدمة الوحدة النمطية).
- يتم إجراء تكوين CoPP ومراقبته فقط في VDC افتراضي.
- يمكن إستخدام CoPP الافتراضي مع الخيارات الصارمة والمعتدلة والمتساهلة والكثيفة.
- إستنساخ CoPP BPP إلى قواعد CoPP المخصصة لمطابقة متطلبات الشبكة المحددة.
- يتم عرض عدادات CoPP (المتطابقة والمخالفة بالبايت لكل فئة-map) باستخدام الأمر **show policy-map interface control-plane**.
- وتساوي حركة المرور التي يتم استقبالها بواسطة وحدة المعالجة المركزية (CPU) للوحدة النمطية للمشرف العدد الإجمالي لأنواع FEs مضروبا في المعدل المسموح به.
- حاولت أن يتحاشى ميناء مشترك من واحد FE عبر مختلف VDCs.
- اتبع أفضل ممارسات CoPP من أجل تنفيذ الميزات ومراقبتها بنجاح.

ميزات غير مدعومة

هذه الميزات غير مدعومة:

- وضع سياسات التجميع الموزع.
- وضع سياسات التدفق الميكروي.
- وضع سياسات إستثناء الخروج.
- دعم CoPP لوحدة بيانات بروتوكول الجسر (BPDU) التي تأتي من منفذ QinQ (dot1q-tunnel): بروتوكول اكتشاف Cisco (CDP)، و DOT1x، وبروتوكول الشجرة المتفرعة (STP)، وبروتوكول خط اتصال الشبكة

المحلية الظاهرية (VTP).

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).