سياسة مستوى التحكم الافتراضي على Catalyst 6500/Sup2T و Catalyst 6880 مثال تكوين

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
التكوين
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
معلومات ذات صلة

المقدمة

يصف هذا المستند بالتفصيل أنواع حركة المرور التي يتم مطابقتها مقابل مخططات الفئة الافتراضية، والتي تعد جزءا من تكوين CoPP Catalyst 6880 / Catalyst 6500 Sup2T (تنظيم مستوى التحكم) الافتراضي الذي يتم تكوينه تلقائيا على الجهاز. تم تكوين هذا الأمر لحماية وحدة المعالجة المركزية (CPU) الخاصة بها من التحميل الزائد.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

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

التكوين

يتم تمكين CoPP بشكل افتراضي على محولات Catalyst 6500 / SUP2T و Catalyst 6880 ويبني على قالب تم تكوينه مسبقا. لا تحتوي بعض تكوينات خريطة الفئة على عبارات تطابق متطابقة بسبب حقيقة أنها على حركة مرور البيانات غير الموجودة في قائمة التحكم في الوصول إلى (ACL MAC/IP)، ولكن بدلا من ذلك على الاستثناءات الداخلية التي يتم الإشارة إليها بواسطة محرك إعادة التوجيه عند إستلام حركة المرور بواسطة المحول واتخاذ قرار إعادة التوجيه.

إذا كانت هناك حاجة لإضافة / تعديل / إزالة خريطة فئة معينة من سياسة CoPP الحالية، فيجب القيام بذلك من وضع التكوين في وضع خريطة السياسة. راجع دليل تكوين البرنامج Catalyst 6500 الإصدار 15.0SY Software - تنظيم مستوى التحكم (CoPP) للحصول على الصياغة الدقيقة.

تحتوي فئات إستثناء CoPP الافتراضية على هذه الأوصاف:

ظرف	اسم خريطة الفئة	الوصف
فشل الحد الأقصى لوحدة الإرسال (MTU)	class-coPP-MTU-fail	يتجاوز حجم الحزمة حجم MTU للواجهة الصادرة. إذا لم يتم تعيين وحدة بت عدم التجزئة، فإنه يلزم إجراء التجزئة. إذا تم تعيين بت عدم التجزئة، فإن وجهة بروتوكول رسائل التحكم في الإنترنت (ICMP) التي يتعذر الوصول إليها تشير إلى أنه من المفترض إنشاء "التجزئة المطلوبة ومجموعة DF" وإرسالها مرة أخرى إلى المصدر. المرجع: RFC-791، RFC-1191
فشل مدة البقاء (TTL)	class-coPP-ttl-fail	Packet TTL = 1 (لـ IPv4)، حد الخطوة = 0 أو 1 (لـ IPv6) يمكن تجاهل TTL = 0 (لـ IPv4) في الجهاز على

الخيارات	خيارات Class-CoPP	الفور حيث من المفترض أن تقوم الخطوة السابقة بتدمير الحزمة عندما يتم تقليل TTL إلى 0. حد الخطوة = 0 (ل IPv6) مختلف عن TTL = 0 لأنه مذكور في RFC-2460، القسم 8.2 أنه على عكس IPv4، لا تكون عقد IPv6 مطلوبة لفرض الحد الأقصى من عمر الحزمة. وهذا هو السبب في إعادة تسمية حقل "الوقت إلى الحياة" ل IPv4 إلى "حد الخطوات" في IPv6. وهذا يعني أن حزمة IPv6 الواردة ذات حد الخطوة ((Hop 0 = لا تزال صالحة، ويجب إرسال رسالة ICMP مرة أخرى. المرجع: RFC-791، RFC-2460 حزمة مع خيارات (ل IPv4)، رأس ملحق خطوة بخطوة (ل IPv6). على سبيل المثال، تنبيه الموجه RFC-2113، مسار المصدر المقيد، وما إلى ذلك. لا يتم فحص

فشل إعادة توجيه المسار العكسي (RPF) (البث الأحادي)	class-coPP-UCAST-RPF-fail	رؤوس الملحقات أو معالجتها بواسطة أي عقدة على مسار تسليم الحزمة، حتى تصل الحزمة إلى العقدة (أو كل من مجموعة العقد في حالة البث المتعدد) المحددة في حقل عنوان الوجهة لرأس IPv6. الاستثناء الوحيد هو رأس خيارات الخطوة-بالخطوة، والذي يحمل معلومات يجب فحصها ومعالجتها بواسطة كل عقدة على مسار تسليم الحزمة، والذي يتضمن عقد المصدر والوجهة. معالجة الأجهزة في حقول الخيارات غير مدعومة، مما يعني أن معالجة/تحويل البرامج مطلوب. المرجع: RFC-791 / RFC-2460 تمت تصفية الحزمة التي فشلت في إعادة توجيه المسار العكسي (RPF). ومع ذلك، بسبب الموارد المحدودة في

الجهاز، لا يمكن إجراء فحص إعادة توجيه المسار العكسي (RPF) في الأجهزة في حالات معينة (أي أكثر من 16 واجهة إعادة توجيه المسار العكسي (RPF) مرتبطة ببروتوكول واحد). عندما يحدث ذلك، يتم إرسال الحزمة إلى البرنامج للتحقق من إعادة توجيه المسار العكسي (RPF) بالكامل.

يتم إرسال حزمة بيانات فشل إعادة توجيه المسار العكسي (RPF) الأولى (الموجهة إلى مجموعة البث المتعدد) إلى البرنامج لبدء عملية التأكيد على البث المتعدد المستقل للبروتوكول (PIM). بمجرد إتمام العملية، يتم إختيار موجه/مرسل محدد. إذا لم تأت الحزمة التالية (نفس التدفق) من الموجه المعين، فإنها تشعل فشل إعادة توجيه

فشل RPF (البث المتعدد)	class-coPP-mcast-rpf-fail	المسار العكسي (RPF)، ويمكن للأجهزة إسقاطه على الفور (لمنع هجوم رفض الخدمة (DoS)). يتم إرسال حزمة بيانات فشل إعادة توجيه المسار العكسي (RPF) الأولى (الموجهة إلى مجموعة البث المتعدد) إلى البرنامج لبدء عملية تأكيد PIM. بمجرد إتمام العملية، يتم إختيار موجه/مرسل محدد. إذا لم تأت الحزمة التالية (نفس التدفق) من الموجه المعين، فإنها تشعل فشل RPF، ويمكن أن يقوم الجهاز بإسقاطه فورا (لمنع هجوم رفض الخدمة (DoS). ومع ذلك، إذا تم تحديث جدول التوجيه، فقد يلزم إختيار موجه جديد محدد (عبر تأكيد PIM)، مما يعني أن حزمة إعادة توجيه المسار العكسي (RPF) التي فشلت يلزم الوصول إلي البرنامج (لتأكيد

		PIM للبدء من جديد). للقيام بذلك، يتوفر تسرب دوري إلى آلية البرامج (لكل تدفق) للحزمة التي فشلت في إعادة توجيه المسار العكسي (RPF) في الجهاز. ومع ذلك، إذا كان هناك كمية كبيرة من التدفقات، فقد يكون التسرب الدوري أكبر من أن يتمكن البرنامج من التعامل معه. لا يزال CoPP الجهاز مطلوبا للحزمة الفاشلة لإعادة توجيه المسار العكسي (RPF) للبث المتعدد. المرجع: RFC-3704، RFC-2362
إعادة كتابة حزمة الأجهزة غير مدعومة	class-coPP-unsupp-rewrite	وعلى الرغم من إمكانية قيام الأجهزة بإعادة كتابة الحزم في حالات مختلفة، إلا أنه لا يمكن القيام ببعض الحالات في التصميم الحالي للأجهزة. ولهؤلاء، يرسل الجهاز الحزمة إلى البرنامج. الحزم المرسلة إلى البرامج لإنشاء رسائل ICMP. مثل إعادة توجيه
عدم توجيه ICMP إسقاط قائمة التحكم في الوصول ل ICMP إعادة توجيه ICMP	class-coPP-icmp-redirect-unreachable	

إستقبال إعادة التوجيه السريع (CEF) من Cisco (عنوان IP للوجهة هو عنوان IP للموجه)	class-coPP-receive	ICMP، يتعذر الوصول إلى وجهة ICMP (على سبيل المثال، المضيف الذي يتعذر الوصول إليه أو الممنوع إداريا). المرجع: -RFC 792 / RFC-2463 إذا كان عنوان IP لوجهة الحزمة هو أحد عناوين IP للموجه (سيضرب إستقبال CEF)، فمن المفترض أن يعالج البرنامج المحتوى. إذا كان عنوان IP لوجهة الحزمة ينتمي إلى إحدى شبكة الموجه، ولكنه لم يتم حله (أي عدم الوصول إلى جدول قاعدة معلومات إعادة التوجيه (FIB))، فسوف يضرب تجاور CEF، ويتم إرساله إلى البرنامج حيث سيتم بدء إجراء الحل. بالنسبة ل IPv4، يستمر التدفق نفسه في الوصول إلى مجموعة إعادة التوجيه السريع (CEF) حتى يتم حل العنوان. بالنسبة ل IPv6، يتم تثبيت إدخال
CEF glean (ينتمي عنوان IP للوجهة إلى شبكة أحد الموجهات)	طراز-CoPP-glean	

الحزمة الموجهة إلى 224.0.0.0/4 IP للبث المتعدد	class-coPP-mcast-ip-control	يجب معالجة حزمة التحكم بواسطة البرنامج.
الحزمة الموجهة إلى IP FF متعدد البث::/8	class-coPP-mcast-IPv6-control	يجب معالجة حزمة التحكم بواسطة البرنامج.
حزمة البث المتعدد التي يلزم نسخها إلى البرنامج	class-coPP-mcast-copy	في بعض الحالات، يلزم نسخ حزمة البث المتعدد إلى البرنامج لتحديث الحالة (لا تزال الحزمة مترابطة مع الأجهزة على شبكة VLAN نفسها). على سبيل المثال، تم الوصول إلى (*،G/m) لإدخال الوضع الكثيف والتبديل عبر SPT ذي إعادة توجيه المسار العكسي (RPF). الوجهة IP (multicast IP) خطأ في جدول FIB. يتم ضرب الحزمة على البرنامج. يتم إرسال
حزمة البث المتعدد تحصل على خطأ في جدول FIB	class-coPP-mcast-Punt	
مصدر متصل مباشرة (IPv4)	class-coPP-ip-connected	

FIB مؤقت يطابق IP للوجهة (ونقاط إسقاط التجاور بدلا من ذلك) أثناء الحل. إذا تعذر حلها خلال المدة المحددة، تتم إزالة إدخال FIB (أي، يبدأ نفس التدفق في الوصول إلى مجموعة CEF مرة أخرى).

مصدر متصل مباشرة (IPv6)	الفئة-coPP-IPv6 المتصلة	حركة مرور البث المتعدد من المصادر المتصلة مباشرة إلى البرنامج حيث يمكن إنشاء حالة بث متعدد (وتثبيتها في الجهاز). يتم إرسال حركة مرور البث المتعدد من المصادر المتصلة مباشرة إلى البرنامج حيث يمكن إنشاء حالة بث متعدد (وتثبيتها في الجهاز).
حزمة البث	class-coPP-broadcast	يتم تسريب حزم البث (على سبيل المثال، IP/بخلاف IP مع بث DMAC و IP Unicast مع DMAC للبث المتعدد) إلى البرنامج.
بروتوكول غير معروف إلى (وذلك، غير مدعوم من قبل) من حيث تحويل الأجهزة	بروتوكول class-coPP-unknown	لن يتم تحويل البروتوكول غير الخاص ب IP، مثل تبادل حزم الشبكة البينية (IPX) وما إلى ذلك، للأجهزة. يتم إرسالها إلى البرنامج وإعادة توجيهها إلى هناك.
حركة مرور بيانات البث المتعدد الواردة عبر المنفذ الموجه حيث يتم تعطيل PIM	class-coPP-mcast-v4-data-on-routedPort	multicast معطيات حركة مرور أن يأتي من خلال يوجه ميناء (حيث PIM معأق) يسرب إلى البرمجية. ومع ذلك، ليس من الضروري إرسالها إلى

حركة مرور بيانات البث المتعدد الواردة عبر المنفذ الموجه حيث يتم تعطيل PIM	class-coPP-mcast-v6-data-on-routedPort	البرامج حتى يتم إسقاطها. يتم تسريب حركة مرور بيانات البث المتعدد التي تأتي من خلال منفذ موجه (حيث يتم تعطيل PIM) إلى البرنامج. ومع ذلك، ليس من الضروري إرسالها إلى البرامج حتى يتم إسقاطها.
إعادة توجيه قائمة التحكم في الوصول (ACL) إلى المدخل لربط الحزمة	class-coPP-UCAST-ingress-ACL-bridged	يحتوي الجهاز على 8 إستثناءات متعلقة بقائمة التحكم في الوصول (ACL) تم تعيينها بواسطة البرنامج من خلال إعادة توجيه قائمة التحكم في الوصول (ACL). يتعلق هذا الأمر بحزم البث الأحادي التي يتم ربطها بوحدة المعالجة المركزية (CPU) بواسطة قائمة التحكم في الوصول للأسباب المتعلقة بالذاكرة القابلة للتوجيه (TCAM) للمحتوى الثالث.
إعادة توجيه قائمة التحكم في الوصول (ACL) إلى المخرج لجسر الحزمة	class-coPP-ucast-egress-acl-bridged	يحتوي الجهاز على 8 إستثناءات متعلقة بقائمة التحكم في الوصول

		(ACL) تم تعيينها بواسطة البرنامج من خلال إعادة توجيه قائمة التحكم في الوصول (ACL). يتعلق هذا الأمر بحزم البث الأحادي التي يتم ربطها بوحدة المعالجة المركزية (CPU) بواسطة قائمة التحكم في الوصول للأسباب المتعلقة بالذاكرة القابلة للتوجيه (TCAM) للمحتوى الثالث. يحتوي الجهاز على 8 إستثناءات متعلقة بقائمة التحكم في الوصول (ACL) تم تعيينها بواسطة البرنامج من خلال إعادة توجيه قائمة التحكم في الوصول (ACL). يتعلق هذا الأمر بمعالجة البث المتعدد. يحتوي الجهاز على 8 إستثناءات متعلقة بقائمة التحكم في الوصول (ACL) تم تعيينها بواسطة البرنامج من خلال إعادة توجيه قائمة
إعادة توجيه قائمة التحكم في الوصول (ACL) للبث إلى توصيل الحزم إلى وحدة المعالجة المركزية	class-coPP-mcast-acl-bridged	
جسر قائمة التحكم في الوصول (ACL) إلى وحدة المعالجة المركزية (CPU) لمعالجة موازنة حمل الخادم	class-coPP-SLB	

إعادة توجيه سجل ACL VACL	class-coPP-vacl-log	التحكم في الوصول (ACL). يتعلق هذا الأمر بإعادة توجيه الأجهزة لاتخاذ قرار موازنة حمل الخادم (SLB). يحتوي الجهاز على 8 إستثناءات متعلقة بقائمة التحكم في الوصول (ACL) تم تعيينها بواسطة البرنامج من خلال إعادة توجيه قائمة التحكم في الوصول (ACL). يتعلق هذا الأمر بإعادة توجيه الحزمة بواسطة قائمة التحكم في الوصول إلى شبكة VLAN (VACL) ACL إلى وحدة المعالجة المركزية لأغراض Cisco IOS؟ التسجيل.
التطفل على بروتوكول DHCP	class-coPP-dhcp-snooping	تتم إعادة توجيه حزم DHCP التي تم التطفل عليها إلى وحدة المعالجة المركزية لمعالجة DHCP
إعادة توجيه تستند إلى سياسة MAC	class-coPP-mac-pbf	ستتم إعادة التوجيه المستندة إلى السياسة في وحدة المعالجة المركزية (CPU) نظرا

التحكم في الدخول إلى شبكة IP	دخول الفئة-CoPP-IP	لأن الجهاز غير قادر على إعادة توجيه الحزم في هذه الحالة. لتوفير الوصول إلى الشبكة استنادا إلى مسوغات مكافحة الفيروسات الخاصة بالمضيف، هناك التحقق من صحة الموقف عبر أحد هذه الخيارات: (1) ستستخدم واجهة L2 بروتوكول LAN Port IP (LPIP))، حيث يتم إعادة توجيه حزم بروتوكول تحليل العنوان (ARP) إلى وحدة المعالجة المركزية، (2) تستخدم واجهة L3 بروتوكول Gateway IP (GWIP)). بعد التحقق من الصحة، توجد المصادقة (*). بالنسبة لواجهة L2، فإنها WebAuth، التي تقوم بتنفيذ اعتراض حزمة HTTP وقد تقوم أيضا بإعادة توجيه URL (*). بالنسبة لواجهة L3، فإنها AuthProxy.
فحص ARP (بروتوكول تحليل العناوين) الديناميكي	التطفل على بروتوكول Class-CoPP-ARP	لمنع هجوم تسميم ARP (الدخيل)، يتحقق الفحص

الديناميكي ل ARP (المعروف أيضا باسم الفحص الديناميكي ل ARP (DAI) من طلبات/استجابات ARP عندما يعترض ويعالجها بعد ذلك في وحدة المعالجة المركزية مقابل واحدة من هذه: (1) قوائم التحكم في الوصول ل ARP التي قام المستخدم بتكوينها (للمضيفين الذين تم تكوينهم بشكل ثابت)، (2) عنوان MAC إلى روابط عنوان IP المخزنة في قاعدة البيانات الموثوق بها (أي روابط DHCP). يتم إستخدام حزم ARP الصالحة فقط لتحديث ذاكرة التخزين المؤقت ل ARP المحلي أو إعادة توجيهها للخارج. تتطلب عملية التحقق من الصحة مشاركة وحدة المعالجة المركزية لحزم ARP، مما يعني أن حماية مستوى التحكم في الأجهزة مطلوبة لمنع هجوم رفض

إعادة توجيه قائمة التحكم في الوصول (ACL) إلى وحدة المعالجة المركزية (CPU) ل WCCP	class-copp-wccp	الخدمة (DoS). يستخدم في حالة الحاجة إلى إعادة توجيه الحزمة/التدفق إلى وحدة المعالجة المركزية لقرار إعادة توجيه بروتوكول إتصالات ذاكرة التخزين المؤقت للويب (WCCP).
إعادة توجيه قائمة التحكم في الوصول (ACL) إلى وحدة المعالجة المركزية (CPU) لبنية إدخال الخدمة (SIA)	إدخال الخدمة من الفئة CoPP	يستخدم في حالة الحاجة إلى إعادة توجيه الحزمة/التدفق إلى وحدة المعالجة المركزية (CPU) لاتخاذ قرار SIA.
اكتشاف شبكة IPv6	صنف-CoPP-ND	لإعادة توجيه حزمة اكتشاف شبكة IPv6 إلى وحدة المعالجة المركزية (CPU) لمزيد من المعالجة. المرجع: RFC4861

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

للتحقق من ما إذا كانت هناك حركة مرور ملاحظ في أي من مخططات فئة CoPP التي تم تكوينها، أدخل الأمر **show policy-map control-plane**.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- حماية المحولات Cisco Catalyst 6500 Series Switches باستخدام تنظيم مستوى التحكم وتحديد معدل الأجهزة وقوائم التحكم في الوصول
- دليل تكوين البرنامج Catalyst 6500 الإصدار 15.0SY Software - تنظيم مستوى التحكم (CoPP)
- الدعم التقني والمستندات - Cisco Systems

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).